Report on Issues and Activity in the Area of Security for Software Defined Radio

1 September 2002

Executive Summary

This report is the result of the Software Defined Radio Forum's long history of interaction with the United States Federal Communication Commission (FCC) on regulatory issues related to Software Defined Radio (SDR). In the FCC Report and Order on SDR dated September 13, 2001, the Commission declined "to set specific security or authentication requirements at this time because they could hinder the development of the technology used to provide such security and could have the potential to be unduly burdensome on manufacturers." However the Commission stated that "it is possible that we may have to specify more detailed security requirements at a later date as software defined radio technology develops." The Commission noted "the SDR Forum has indicated that it is continuing to develop methods for the security and authentication of radio software and that it will report its findings to the Commission." As anticipated by the FCC, the SDR Forum has prepared this report on industry measures to address these security concerns.

Although this report is relevant to the questions being asked by the United States Federal Communications Commission, the SDR Forum believes that the document may be of interest to other regulatory agencies around the world.

In the review of security issues and activities of a wide variety of external organizations, the SDR Forum has developed the following views:

- There is broad interest in wireless communications and the security aspects of wireless systems by many industry players, some of which are relatively new to wireless systems. This broad industry involvement stems from the continuing merger of communications, computing systems, and content providers. This broad activity in wireless communications systems and security involves not only the traditional wireless players, but also many new players who bring additional expertise in security issues to the wireless community.
- Many of the general security core technologies, including security techniques used for information content (e.g., credit card) and general wireless security techniques, appear to be applicable to the more specific case of security of SDR-based systems.
- There are ample market drivers to provide adequate incentives for the wireless communication industry to deploy security technologies including core technologies that were not initially developed for SDR but which are applicable to SDR..
- The necessary work on security specifically for SDR-capable devices is being done by industry today. Solutions for SDR security are forthcoming from industry and will likely be based on security mechanisms, protocols, and algorithms previously developed for other security applications.
- The SDR Forum will continue to stimulate this industry activity by being a focal point for software download for RF reconfiguration including the security aspects of software download.

This report supports the above views by providing an overview of the security challenge that is followed by a more detailed description of security threats. This is followed by a

description of the ongoing activities in industry to mitigate these threats. In both the discussion of the threats and in the discussion of the mitigating activities, the flow of the information is from the more general to the more specific; i.e., first there is a discussion of general communications security, followed by a discussion of wireless communication security, and then specific SDR security.

One section of the report is dedicated to the topic of market incentives for deployment of security measures for SDR. The SDR Forum is confident that the technology is present to solve the SDR security issues and that there is a strong market incentive to do so.

Finally, the report concludes with a synopsis of future work planned by the SDR Forum, including plans to work with the wireless industry and standards organizations on measures needed to mitigate security threats to SDR-based systems.

Table of Contents

List of Key Acronyms

1G	1st Generation Commercial Mobile Wireless
2G	2nd Generation Commercial Mobile Wireless
3G	3rd Generation Commercial Mobile Wireless
3GPP	Third Generation Partnership Project (based on GSM and UTRA)
3GPP2	Third Generation Partnership Project 2
AES	Advanced Encryption Standard
APCO	Association of Public Safety Communications Officials
ARIB	Association of Radio Industries and Businesses (Japan)
ATIS T1	Alliance for Telecommunication Industry Solutions Committee T1 (Telecommunications)
CWTS	China Wireless Telecommunication Standards Group
ECC	Elliptic Curve Cryptosystem
EDGE	Enhanced Data Rates for the GSM Evolution
ETRI	Electronics and Telecommunications Research Institute (Korea)
ETS	European Telecommunication Standard
ETSI	European Telecommunications Standards Institute
GPRS	General Packed Radio Service
GSM	Global System for Mobile Communication
IMT-2000	International Mobile Telecommunications 2000
IPsec	Internet Protocol Security
ITU	International Telecommunication Untion
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
J2ME	Java 2 Micro Edition
LAN	Local Area Network
MExE	Mobile Execution Environment
MOU	Memorandum of Understanding
NASTD	National Association of State Telecommunications Directors
NIST	National Institute of Standards and Technology
NOI	Notice of Inquiry (of the FCC)
NPRM	Notice of Proposed Rulemaking (of the FCC)
OEM	Original Equipment Manufacturer
OSI	Open System Interconnect Reference Model
PC	Personal Computer
PCS	Person Communications Services
PJava	Personal Java
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PPTP	Point to Point Tunneling Protocol
RF	Radio Frequency
RFI	Request for Information
R&O	Report and Order of the U.S. Federal Communications Commission
RSA	Rivest-Shamir-Adleman Algorithm
SDO	Standards Development Organization

SDR	Software Defined Radio
SDRF	Software Defined Radio Forum
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
TCPA	Trusted Computing Platform Alliance
TETRA	TErrstrial Trunked Radio
TIA	Telecommunications Industry Association
TSG SA	Technical Specification Group Systems Architecture (a 3GPP subgroup)
TTA	Telecommunications Technology Association (Korea)
TTC	Telecommunications Technology Committee (Japan)
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	User Services Identity Module
UTRA	UMTS Terrestrial Radio Access
VPN	Virtual Private Networks
WAP	Wireless Application Protocol
WEP	Wireline Equivalent Privacy
WLAN	Wireless Local Area Network

Report on Issues and Activity in the Area of Security for Software Defined Radio

1 Introduction

This document provides information on the security challenges and security activities from three perspectives: the broad perspective of security for communications systems in general, the more specific perspective of security for wireless communications systems, and the perspective of security for software defined radio (SDR). It is the SDR Forum's position that:

- The wireless communications security threats and more specifically the software defined radio security threats are characterized and understood by industry.
- The wireless and more specifically the software defined radio industries are fully engaged on the many aspects of security in order to mitigate these threats.
- Core security technologies (e.g., Internet security technologies such as Public Key Infrastructure - PKI) that have been developed for other communications security challenges appear to be applicable to the SDR security challenges.
- Private industry, in particular the commercial wireless industry, has tremendous incentive to ensure that SDR products and wireless networks are secure; specifically this includes motivation to apply existing core security technologies to the SDR security challenge.
- Regulatory mandates of specific security methods, techniques, and algorithms are counterproductive. On the other hand, specifying functional or performance requirements for security robustness against defined threats may be appropriate.

These views are supported by the ongoing security activities summarized herein.

This report does not advance solutions to the issues raised. It sets the stage for the solutions by providing a framework document on the SDR security topic. In addition, it is fully recognized that in a complex subject such as security, expertise for developing the solutions lies in organizations dedicated to addressing security issues. The SDR Forum is the focal point for ensuring that security issues associated with software defined radio are identified and are brought to the attention of, and addressed by, those organizations having the recognized security expertise.

1.1 Background

Software Defined Radio (SDR) provides an efficient and comparatively inexpensive mechanism for the design and implementation of multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades, thus addressing many of the most challenging issues confronting the wireless industry. SDR technology provides the building blocks to affordably integrate a wide variety of mobile

Internet applications over multiple air interfaces, using multiple technologies to provide rapid access to advanced wireless networks.

These great benefits of programmability come with the responsibility for diligence in deploying security measures to protect against un-wanted operation. At its meeting on Sept. 13, 2001, the United States Federal Communications Commission (FCC) adopted an Software Defined Radio (SDR) First Report and Order, which removed barriers to entry of SDR products in the marketplace. In the Report and Order, the FCC made clear its view that:

> It is critical "to ensure that software changes cannot be made to a radio that will cause it to operate with parameters outside of those that were approved in order to prevent interference to authorized radio services."

The Commission noted "that industry groups are still in the process of developing security standards." The Commission stated that:

> "We continue to believe that the best approach is to rely on a general requirement that manufacturers take adequate steps to prevent unauthorized changes to the software that drives their equipment. This will allow manufacturers flexibility to develop innovative software defined transmitting equipment while at the same time providing for oversight of the adequacy of such steps through the equipment authorization process."

Accordingly the Commission declined "to set specific security or authentication requirements at this time because they could hinder the development of the technology used to provide such security and could have the potential to be unduly burdensome on manufacturers." **However the Commission stated that "it is possible that we may have to specify more detailed security requirements at a later date as software defined radio technology develops."**

The Commission noted "the SDR Forum has indicated that it is continuing to develop methods for the security and authentication of radio software and that it will report its findings to the Commission." Therefore, the SDR Forum has prepared this report to the FCC on industry measures to address these security concerns. Although this report is relevant to the questions being asked by the United States Federal Communications Commission, the SDR Forum believes that the document may be of interest to other regulatory agencies around the world.

Fortunately the solutions for the security of radio software will be able to draw on the enormous amount of activity currently devoted to the protection of digital assets. In this report, therefore, the Forum takes a broad survey of industry activities in the area of security measures that may be applied to the SDR security challenge.

This report does not address the security requirements of military systems because the extreme need for security for such systems has led to a sophisticated set of organizations to maintain and refine security measures. Much of the technology developed for military systems is also applicable to personal and mobile communications systems, and can be used to implement commercial security measures. The report does not provide a broad discussion of threats to civil Government communications systems (e.g., aviation, Forest Service, etc.). However, the report does provide information about the security threat to

Public Safety communications systems and the ongoing work to mitigate such threats. Public Safety is considered to a very important class of civil Government systems.

1.2 Related Work in the SDR Forum

In April 2002, the SDR Forum formally submitted to a broad cross section of industry a request for information (RFI) regarding security issues and activities for software defined radio. The RFI may be found in Appendix A. Responses were received from the Intel Corporation, the Third Generation Partnership Project, Mobile Virtual Center of Excellence in Mobile and Personal Communications (Mobile VCE), and the Motorola Corporation. These responses are provided as Appendices B through E respectively.

In addition to the above, the SDR Forum is in the process of developing a series of documents on software download as described in Appendix F. This work includes many aspects of software download including the development of protocols. Security is a major aspect of this work.

The Forum has long been active in many aspects of the application of SDR technology to the defense community. The experience in such highly secure systems provides in depth knowledge of the many technologies that can be brought to bear on addressing the problems associated with commercial wireless security.

1.3 Structure of the Document

The structure of this document is:

- An overview of the security topic.
- A discussion of security threats scenarios.
- Survey of security activity to mitigate the security threat – the survey includes a general discussion of security activity from a broad perspective, general wireless security activity, and then the specific security activity applicable to SDR security challenges.
- Market incentives for the SDR industry to apply the security mechanisms, algorithms, and technologies that have already been developed by the wireless communications community and by the communications community in general.
- Future work.
- Appendices that:
  - provide the SDR Forum Request for Information (RFI) on SDR security issues and responses to this RFI.
  - provide information on Third Generation Partnership Project (3GPP) security threats.
  - provide information on applicable security products and services.

–

1.4 Disclaimer

Inclusion of the responses (Appendices B through E) to the SDR Forum RFI implies no endorsement of these views by the SDR Forum and the viewpoints represented in these responses are not to be construed as SDR Forum approved or official positions. The RFI responders have authorized the SDR Forum to include their submissions in this document.

Information included in Appendices G through M implies no endorsement of these views by the SDR Forum and the viewpoints represented in these responses are not to be construed as SDR Forum approved or official positions.

2 Overview of Security Challenge

The challenges to the security of SDR-capable devices is best viewed by first reviewing the general challenges to the communications and information technology industries, and then reviewing the challenges to wireless communications systems in general. The rationale for this is that many of the counter-measures against these more general security challenges appear to also be applicable to the specific challenges to SDR security.

The digitization of the global economy has led to an enormous amount of financial transactions and services occurring over the Internet. This has naturally resulted in a dramatic increase in criminal activity targeted at this electronic flow of financial assets.

Richard A. Clarke, President Bush's special advisor for cyberspace security within the National Security Council, in his address to the recent RSA Conference stated that:

- businesses spent an estimated $2 billion last November cleaning up damage from the Nimda virus.
- $12 billion was lost in 2001 due to all computer viruses.
- the number, sophistication and costs of such attacks are on the rise.

Continued advances in digital technology offer both great opportunity and challenges. However digital technology also provides the ability to create easily, and redistribute globally, unlimited perfect copies, posing particularly damaging and challenging piracy risks. Fortunately in a market economy the threat also represents an opportunity to solutions providers. This has resulted in industry providing a stream of economically appropriate responses to counter the threats.

The issue of software security spans the breadth and depth of industry today from financial institutions providing secure transactions; to the security measures of enterprises and institutions against network damaging viruses and denial of service attacks; to the entertainment industry protecting valuable music and video content.

The freedom of movement derived from the introduction of wireless systems brought with it a major shift in the security landscape. Security concerns include attempts to access the control structure of the system and disrupt operations, interception of message content, theft of intellectual property, and unpaid use of services.

When the first generation (1G) cellular systems were fielded, the exposure of an unencrypted analog air interface was underestimated. The result was lack of privacy for users, with a number of famous incidents where over-the-air conversations were recorded. There was also considerable loss of revenue by service providers through cloned mobile terminals.

Second generation (2G) system architectures were designed to have substantially better security. But as they were deployed en masse, they encountered increasingly sophisticated attacks. Future generations of systems will need to develop security measures that outpace developments in subversion techniques.

Security architectures for third generation (3G) systems were further refinements from the 2G systems and were designed to meet increased threats. References [1 and 5] document the security aspects of the Third Generation Partnership Project (one of many international entities addressing wireless communications standardization). The impending widespread use of SDR technology brings the added risk that software can be introduced into a device that changes its RF operating characteristics so it is no longer compliant with its regulatory authorization to operate. The software and hardware architecture of systems in which SDR technology is deployed must incorporate security measures to isolate and protect radio-critical system elements from improper changes, whether accidental or intentional.

3 Detailed Discussion of Security Threats

This section provides a general description of telecommunications security challenges followed by more specific security challenges facing the wireless industry. This is followed by a description of the specific challenges to SDR security including the presentation of an SDR security threat model.

3.1 General Telecommunications Challenges

Security requirements can be generically divided into the following six general categories:

1. **Trusted System Operation**: confidence that software will execute in the device exactly as intended.
2. **Authentication**: the ability to validate the origin of received information. For example, an SDR device should be able to ensure that the downloaded software originates from a trusted server, prior to installation. The SDR device should install only authenticated software.
3. **Authorization**: verification that the user is permitted to access the data or to utilize a communications capability.
4. **Integrity**: verification that received information has not been modified or corrupted in transit. Prior to accepting and installing new software, an SDR device should be able to ascertain that, since originating from the trusted server, the downloaded data has not been modified. The SDR unit should only install software that has been checked for its integrity.
5. **Privacy**: Often times referred to as "confidentiality" this category usually refers to the assurance that other parties cannot access a user's personal information. In the case of SDR, however, privacy can apply not only to user data, but also to the executable software, which is the intellectual property of the equipment manufacturer or software developer. Encryption techniques may be used to prevent unauthorized parties from gaining access to private user data, or to proprietary software.
6. **Non-repudiation:** positive verification of a sender or receiver's participation in a transaction.

As noted by Intel (see Appendix B), in the Internet security world, "levels of trust" for "trusted computing" comprises authentication, authorization, privacy, integrity, and non-repudiation. In that sense, the "trusted system operation" category could be viewed as comprising each of the rest of the security categories listed above.

These general security requirements are similar for many different types of communications systems, both wireline and wireless. Industry has worked diligently to find solutions to these requirements for many different communications systems (e.g., the Internet). These activities, which are described briefly in Section 4, appear to be very

applicable to the SDR security challenges. As will be discussed later, solutions such as Public Key Cryptography (PKC) appear applicable to SDR systems.

3.2 Wireless Security Challenges

Inherent in the use of radio interfaces in communications systems is a degree of vulnerability which is greater than in wireline systems. The advantages of mobility provided by wireless systems far outweigh the security problems, but architectural provision to mitigate the threats are essential. References [1 – 7] provide detailed descriptions of the large amount of work in security that has taken place and is continuing to take place in the wireless industry; these references also provide descriptions of security threats.

Wireless networks have already begun to see attacks. For instance, an attack last year in Japan sent a malicious email to 13 million users of i-mode. When the email was opened, the communication device repeatedly dialed 1-1-0 (Japanese equivalent to 911 in the United States) every 20 minutes.

An area of unique sensitivity is that mobile handheld devices can contain a significant amount of personal data. Personal lists containing names, addresses, phone numbers, and other information such as credit card information, passwords and other sensitive data is stored on the terminal. In addition, in the near future in the United States, the location of the user may be available in conjunction with system support for E911 FCC mandates.

3.2.1 A Case Study: 802.11 and WEP

The unique vulnerability of wireless communications systems is due to the fact that a physical wire does not have to be tapped to access the data flow. This "wireless tapping" issue was particularly highlighted when Adam Stubblefield, a 20-year-old undergraduate student from Rice University, was able to crack the wired equivalent privacy (WEP) encryption protocol used in 802.11b wireless local area networks; accomplished by capturing the encrypted data with a standard off the shelf PC card and then extracting the key.

This has led to the phenomenon of "War Driving". Similar to "War Dialing" (the act of using software to quickly and randomly dial phone numbers with the hopes of reaching a modem and then gaining access to the computer or network); hackers now use a laptop with a wireless LAN (WLAN) card and drive around snooping for vulnerable WLANs to attack. This is just one example of why new more robust security algorithms and protocols are being developed and brought to market.

The disadvantages of relying on WEP for network security are widely known. While many of the problems can be traced to user error on installation and configuration, a true problem with WEP exists because of the relatively small size of the initialization vector (IV). The WEP protocol uses a 24-bit public IV with a 40-bit secret key to generate the keystream. Comparing two or more encrypted packets using the same IV allows one to, with some analysis, recover the plaintext of one of the packets. Once the plaintext of one of the packets is known it is trivial to determine the plaintext of the other packets and the

keystream. Once one knows the keystream, all packets encrypted with the same IV can also be decrypted. Over time, one could build a database of keystreams for each IV. Other problems exist as well for the WEP protocol to be a serious WLAN security barrier. The IEEE 802.11i Working Group is expected to come out with an interim solution to the WEP vulnerabilities followed by a long-term solution. However, many wireless equipment vendors are not waiting for the Working Group's solution, they are marketing solutions to compensate for the WEP flaws.

Many companies are turning to the 802.1X protocol to secure access to their wireless LAN. It is well on its way to becoming an industry standard. The basic 802.1X protocol provides effective authentication regardless of whether you implement 802.11 WEP keys or no encryption at all. 802.1X communications begins with an unauthenticated client device attempting to connect with an authenticator such as an 802.11 server. The server responds by enabling a port for passing only EAP (Extensible Authentication Protocol) packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, until the verification of the client's identity is established using an authentication server. Once authenticated, the access point opens the client's port for other types of traffic. The 802.1X protocol does not provide the actual authentication mechanisms; an EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), must be defined for authentication to take place. Wireless LAN implementations of 802.1X fall outside the scope of the 802.11 standard, however, the 802.11i committee is specifying the use of 802.1X to eventually become part of the 802.11 standard.

Other vendors are offering a solution know as dynamic WEP. Under dynamic WEP each user is assigned an encryption key rather then one key for all users. With this system each key is then used less and thus, there is less data available to the potential intruder to determine any one key. However, each vendor has a different protocol for implementing dynamic WEP and there are interoperability issues between vendors. The 802.11i Working Group is considering a dynamic WEP implementation for the next security standard for 802.11.

3.2.2 Wireless Security Threats and Requirements from a 3GPP Perspective

The Third Generation Partnership Project has produced several documents on security [see References 1 and 5 for example]. The 3GPP document, "3G Security: Security Threats and Requirements," [Reference 5] contains an evaluation of perceived threats by 3GPP and produces a list of security requirements to address those threats. This document takes note of the security principles and objectives as set out in Reference [1] which is a 3GPP document that is intended to offer security guidance to those involved in 3GPP systems.

As noted in the 3GPP security threats and requirements document [Reference 5, Section 6], it is possible to classify security threats in many different ways. The 3GPP basically categorizes threats by the point of the attack:

- the radio interface,
- other parts of the network,
- threats on the terminal and universal integrated circuit card/user services identity module (UICC/USIM)

The threats to the radio interface and the network infrastructure are further categorized by:

- unauthorized access to data,
- threats to integrity
- denial of service
- unauthorized access to services
- repudiation (network only)

Appendix G provides a summarization of the wireless threats defined by 3GPP and the categorization of those threats [Reference 5]. Table 3-1 is a brief synopsis of this summarization that provides illustrative examples of how 3GPP categorizes security threats. The table should be viewed as being illustrative of:

1. specific security threats against wireless communications systems, and
2. how those threats are characterized.

The information in Table 3-1 and Appendix G is not specifically related to SDR. However, many aspects considered here as part of prudent wireless system design appear to have extension to SDR specific concerns on security.

Table 3-1: Illustrative Examples of Wireless Threats Defined by 3GPP[1]

Threat Category	Attacks on the Radio Interface	Attacks on Other Parts of the System
Unauthorized access to data	**Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on the radio interface. This may be used to access security management data or other information which may be useful in conducting active attacks on the system.	**Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on any system interface, whether wired or wireless. This may be used to access security management data which may be useful in conducting other attacks on the system.
Threats to integrity	**Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling data or control data on the radio interface. This includes both accidental or deliberate manipulation. Note: Replayed data which cannot be decrypted by an intruder may still be used to conduct attacks against the integrity of user traffic, signalling data or control data.	**Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling or control data on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.
Denial of service	**Physical intervention:** Intruders may prevent user traffic, signalling data and control data from being transmitted on the radio interface by physical means. An example of physical intervention is jamming.	**Physical intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by physical means. An example of physical intervention on a wired interface is wire cutting. An example of physical intervention on a wireless interface is jamming. Physical intervention involving interrupting power supplies to transmission equipment may be conducted on both wired and wireless interfaces. Physical intervention may also be conducted by delaying transmissions on a wired or wireless interface.
Unauthorized access to services	**Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication has been performed.	**Masquerading as a user:** Intruders may impersonate a user to utilize services authorized for that user. The intruder may have received assistance from other entities such as the serving network, the home environment or even the user himself.
Repudiation		**Repudiation of user traffic origin:** A user could deny that he sent user traffic.

[1] From Reference [5]

3.2.3 Other Perspectives of Wireless Security Threats and Requirements

In this report to the FCC, we will not attempt to summarize all of the various threat models or specific threats that have been identified by various organizations. This would be a time consuming task and would make for a very large document. Certainly, there is ongoing security work in many organizations such as:

1. Essentially every standards related organization[2] (e.g., 3GPP2 and the many fora that develop technical specifications) working in wireless telecommunications.
2. Essentially every Standards Development Organization (SDO) responsible for developing standards for wireless communications systems.

There are many different specific threats to wireless communications. An extensive list of specific wireless security threats could be compiled by an examination of various documents on wireless security. Rather than focus on each specific threat, however, the Forum believes that it is important to have an agreed model for characterizing the specific threats. By creating such a model, it will be possible to treat each specific threat as a member of a "class of threats". Techniques to mitigate the threats can be developed for each class of threats, rather than for each specific threat. Since the list of specific threats will grow with time, it will be better to develop mitigation techniques for a "class of threats" which will be effective even against threats that are not yet known.

As a result of the above, the SDR Forum has not attempted to summarize all of the threats and security requirements of the various wireless standards-related and SDOs. Instead, the Forum proposes a model that can be used to classify specific threats to SDR-based communications systems. The model initially proposed by the SDR Forum is presented in Section 3.3.3. Creation of a such a model will help the Forum, relevant standards-related organizations, relevant SDOs, and regulators to focus on the specific security issues related to SDR-capable devices and SDR-based systems.

3.3 Challenge Specific to SDR

As noted in the Introduction of this report, the United States Federal Communications Commission in its first Report and Order (R&O) on SDR declined to set specific security and authentication requirements at the time of the R&O. However, the Commission stated that it may have to specify security requirements at a later date. In response to these statements by the FCC in the R&O, this section briefly discusses the regulatory considerations for SDR and some specific concerns of spectrum users, and then presents a proposed security threat model. It should be noted that work on this model is continuing within the SDR Forum. The section ends with a discussion of practical aspects of the threat to SDR security.

[2] The Partnership Projects (3GPP and 3GPP2) and many technical fora (e.g., Mobile Wireless Internet Forum and the SDR Forum)are not accredited standards development organizations. Many of these standards-related organizations develop technical specifications that are later adopted by accredited SDOs such as TIA, ATIS T1, ETSI, ARIB, TTC, CWTS, ETRI, TTA, etc.

3.3.1 Regulatory Considerations

Figure 3-1 is a regulatory view of the multi-dimensional aspects of software defined radio. Initial regulatory concern will largely be focused on the lowest level and the protection of radio spectrum. This was demonstrated in the United States FCC proceeding history. After investigating a broad range of potential regulatory involvement including interoperability between radio services and spectrum efficiency and sharing, the Commission concluded that at this time only rule changes to the equipment approval process were needed.

The "higher-planes" concerns, however, are seen to become important later on as the level of adoption of SDR technology increases. This is evident in Figure 3-1 which shows that the regulatory concerns related to radio software download can be viewed as an evolving process that focuses for the time being on equipment certification considerations. The concerns are:

- How will type approval be applied to terminals capable of reconfiguration via software developed by independent third parties?
- Must all hardware and software be type approved?
- What controls are in place to ensure that SDR devices are not susceptible to malicious attack?
- Will security mechanisms be deployed by industry that are adequate for ensuring that radio parameters (e.g., frequency, power, and modulation) can not be changed by unauthorized users?

The SDR Forum views that the multi-dimensional aspects of regulatory interest in Figure 3-1 is consistent with the SDR security threat model[3] that is presented in Section 3.3.3.

[3] This model is still a subject of further study within the SDR Forum and will be finalized prior to the next report to the FCC.

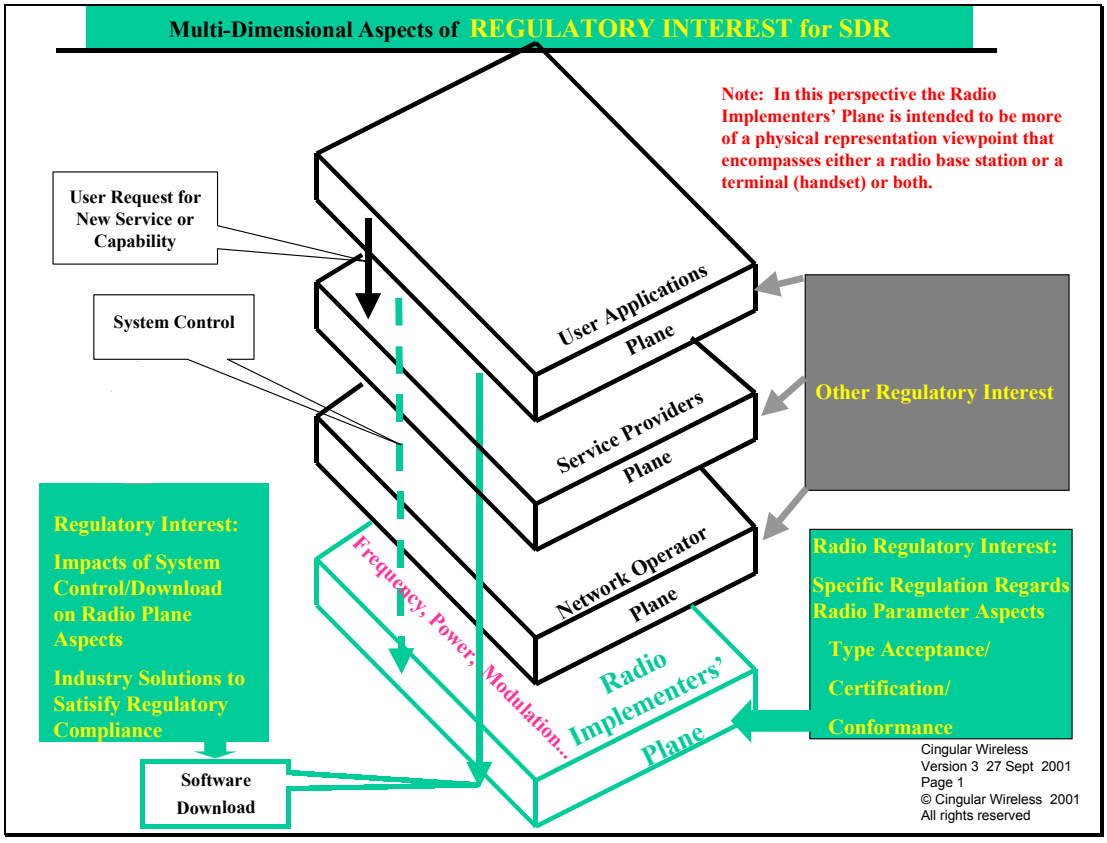


Figure 3-1: Evolution of Regulatory Concerns

3.3.2 Some Specific Concerns of Existing Spectrum Users

As emphasized throughout the FCC's proceeding, the introduction of SDR technology raises significant new implications for regulators and non-traditional concerns for spectrum users. Until recently, wireless regulations and practices were based on a radio device designed, built and operated using hardware (and firmware) that was relatively difficult to modify after it leaves the factory. In the past, changes to a radio required a highly skilled technician, and infrequent problems resulted from mechanical or physical failures of components (plus the rare intentional or malicious act of such an "expert" to make an unauthorized change). The impending widespread use of software changes, whether to add or improve user services or to reconfigure RF parameters of a wireless device, presents substantial new challenges to manufacturers and operators, particularly in the face of a youthful "digital generation" and increasing attacks on the Internet. Furthermore, it raises serious and valid questions among regulators and spectrum users about the potential risks from SDR-based systems.

The FCC itself raised specific questions about the security of SDR operations in its Notice of Inquiry (NOI) and Notice of Proposed Rulemaking (NPRM). These included:

- Should we require anti-tampering or other security features? How would such security features work? Could equipment be designed to prevent it from transmitting in certain designated frequency bands, such as those allocated exclusively for government use, as a safeguard against causing interference? (NOI)
- Ability of SDRs to be reprogrammed to new operating parameters in the field could have far reaching implications for the way the Commission (regulates)… Goal is to ensure that regulatory requirements keep pace with technology development – concerned that technical requirements continue to be met, specifically about ensuring that changes to power levels are consistent with RF exposure rules and ability to ensure that radios are only operated on approved frequency bands. (NPRM)
- Conclusion: a means will be necessary to avoid unauthorized modifications to software that could affect the compliance of a radio . . . The software must not allow the user to operate the transmitter with frequencies, output power, modulation types or other parameters outside of those that were approved. (NPRM)
- FCC . . . declines to set specific security or authentication requirements at this time because they could hinder development of the security technology and could be unduly burdensome on manufacturers. FCC's focus is on the results that security efforts should achieve rather than the means to be used . . . (NPRM)

The National Telecommunications Information Administration (NTIA), regulator for Federal Government wireless systems in the United States, raised similar concerns about the introduction of SDR, including the following:

- SDRs should ensure positive spectrum control . . . There are many Government and non-Government frequency bands that are currently allocated to radio services that support safety-of-life and other sensitive operations.
- NTIA shares the Commission's concern of ". . . maintaining our ability to ensure that radios are only operated on approved frequency bands" and as such, endorses the FCC conclusion that ". . . a means will be necessary to avoid unauthorized modifications to software that could affect the compliance of a radio."

The Forum also notes ongoing effort among European regulators (EC/TCAM) and in Asian countries (e.g., Japan's MPHPT) on comparable questions and studies relating to the appropriate safeguards and security measures for SDR-based systems.

The FCC proceeding produced substantial input from industry and radio user entities, many of which raised specific concerns about risks to their operations and offered recommendations on how to handle potential problems. An illustrative group of comments is provided, as follows:

- Legitimate users of the radio spectrum need protection from both willful use and inadvertent use of unauthorized bands. Inadvertent use of unauthorized bands could occur if software based radio based wireless devices are accidentally put into a mode in which they transmit an unauthorized waveform or unauthorized power level – BellSouth
- In the case of commercial handsets . . . there are a number of possible problems ranging from simple software defects occurring in a small number of cellular

telephones to intentional software virus attacks on all phones operating in an entire cellular network – Motorola

- Over reliance upon software to control frequency selection for public safety communications could impose unacceptable risks of error and failure. In today's environment, a malfunctioning radio will only impact the user of that radio in most instances, whereas a SDR with a software "glitch" could operate on incorrect frequencies and pose serious radio interference problems for many other unsuspecting public safety users – APCO
- To the extent that an SDR allows an individual to program a radio to operate on frequencies and/or in operating modes that have not been appropriately approved through FCC processes and procedures, this increases the possibility that misuse, whether intentionally or unintentionally, may occur . . . and may further increase interference problems and/or unauthorized access to vital public safety radio systems – Public Safety National Coordination Committee
- Given the interference potential of SDRs, the Commission should adopt rules that both deter unauthorized modifications and facilitate the detection of such modifications. . . The prevention of interference is FCC's core function and should be dealt with seriously - Cingular Wireless

The SDR Forum is keenly aware of and acknowledges the valid concerns and questions regarding potential risks to existing spectrum users from new and untried technologies. In this regard, a major objective of the organization – and one vital to future operations and business plans of its membership – is to improve the effective, efficient and interference-free use of the radio spectrum through the promotion of software defined radio. The Forum is firmly committed to the satisfactory handling of SDR security issues and requirements, and is confident that the security threat model described in section 3.3.3 is an effective approach to study and manage identified and future threats.

3.3.3 SDR Threat Scenarios

For SDR-capable devices, security threats can be described using a four-part model, as illustrated in Figure 3.2 This model builds on the model described in Appendix E by incorporating the “point of attack” categorization of 3GPP as described in Section 3.2.2 and summarized in Appendix G (see Reference 5 for full details). The model is responsive to the fact that requests for updates may come from the terminal to the network as well as the requirement that updates may be originated by the network; where the updates originate has an impact on how one should categorize or model the SDR threat scenarios.

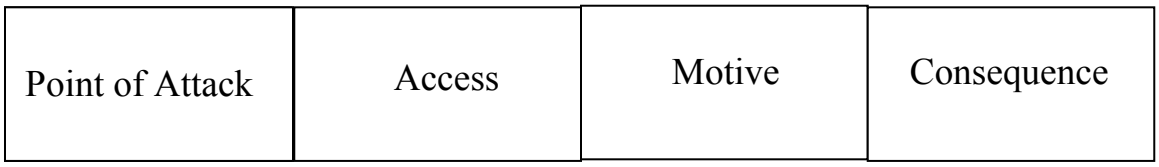


Figure 3.2: Four-part SDR Security Threat Model

Point of Attack[4]: refers to the device or system component within the communication system where the security breach occurs. (Note: the point of attack is not necessarily the same as the target of the attack. For example, the target could be the population of terminals operating within a wireless network, whereas the point of the attack could be the network that provides services to those terminals.) The following points of attack are considered in this model:

- **Terminals and UICC/USIM:** The security breach occurs at the handset or other terminal equipment.
- **Infrastructure**: The security breach occurs within the Radio Access Network or Core Network.

Access: refers to the means by which the perpetrator obtains access to the Point of Attack.

- **Physical**: the threat requires physical control of, or access to, the device or network entity.
- **Remote**: the threat can be perpetrated remotely, by exploiting some external interface to the device or network entity, including wireless interfaces.

Motive: refers to the motivation of the party responsible for the threatening action.

- **Negligent**: accidentally harmful consequences of a legitimate action. (e.g. the download of authenticated software which contains an unintentional software "bug")
- **Unauthorized**: unintentionally harmful consequence of an improper or unauthorized action. (e.g. download of unauthorized black market software which is advertised to "boost" handset performance)
- **Malicious**: deliberate, improper action, specifically intended to cause harmful consequences.

[4] The point of attack categorization is based on the 3GPP categorization of the point of attack for threats against 3G wireless systems [Reference 5]. The threat against SDR-capable devices is expected to be a subset of the to general wireless threat identified by 3GPP. The SDR threat model is still under study by the SDR Forum. The SDR Forum has the view that the general security threat against wireless systems is well understood and that the SDR-capable base stations and terminals may not require any additional security measures in the network infrastructure. Nevertheless, a full understanding of the security threats to SDR-capable devices requires a understanding of the security measures in place in the network infrastructure. Therefore, it is important to include the "point of attack" component in this model.

Consequence: refers to the nature of the harmful consequence resulting from the threatening action.

- **Denial of Service (DoS)**: widespread impairment of the Quality of Service (QoS) for users of the network, on which, the attack was perpetrated.
- **Interference with other Services**: widespread performance impairment of, or improper access to, other networks or services.
- **Digital Rights Violation**: Unauthorized access to, or theft of, digital content and software.

The point of attack, access means, motivation, and consequence are variables in the description of a security threat. There are, therefore:

2 x 2 x 3 x 3 = 36 unique categories of threats.

For each of these categories, there are many variations and permutations, resulting in a boundless array of unique threat scenarios. It is, however, sufficient to focus on the simple four-part security threat model when considering the necessary security counter-measures (as discussed in later sections).

The SDR Forum has the view that the issues, problems, and solutions associated with security aspects of SDR must be addressed from a "systems" perspective. The four-part model described above supports this viewpoint. The following example, supported by Figures 3-3 and 3-4 are provided to illustrate this systems perspective.

For our example, we consider authorization and download of radio software and the mechanisms needed to insert the radio software into a terminal (handset). The SDR software download example is illustrated in Figure 3-3.

The data source for the software download may originate either internal or external to the wireless system as illustrated in Figure 3-3. The information flow may go out over the radio interface and thus come through the core network. It is entirely possible for the data and information to be downloaded to originate outside the radio system and the core network (e.g., from a manufacturer's system) where presumably the network operator and the service provider (who may or may not be the same entity or company) have "reviewed and authorized" the download of the radio software. Then, the security, integrity and threats are many and can occur at numerous points in the entire process.

Thus, at the onset it is a systems view that must be taken. As we move forward into the details of the system and subsystems then more and more specific models and analysis are required to address the details of the issues.

Figure 3-4 depicts the characterization of software download. In this report, we are only concerned with the download of radio software as opposed to the download of non-radio software. In other words, the ellipses in the terminal device and radio access network in Figure 3-3 is the software encircled with the loop in Figure 3-4. Furthermore the following definitions are used for the primary radio software (which is of particular interest to regulators) and the ancillary radio software:

> Primary radio software: Software that affects the radio functionality (e.g., frequency, power, and modulation). The primary software within a wireless device is tightly coupled with the radio hardware to derive the overall radio functionality.
>
> Ancillary radio software: Software that affects the use of the device, but does not affect the radio functionality. Input/output drivers and user interfaces are examples of ancillary radio software download.

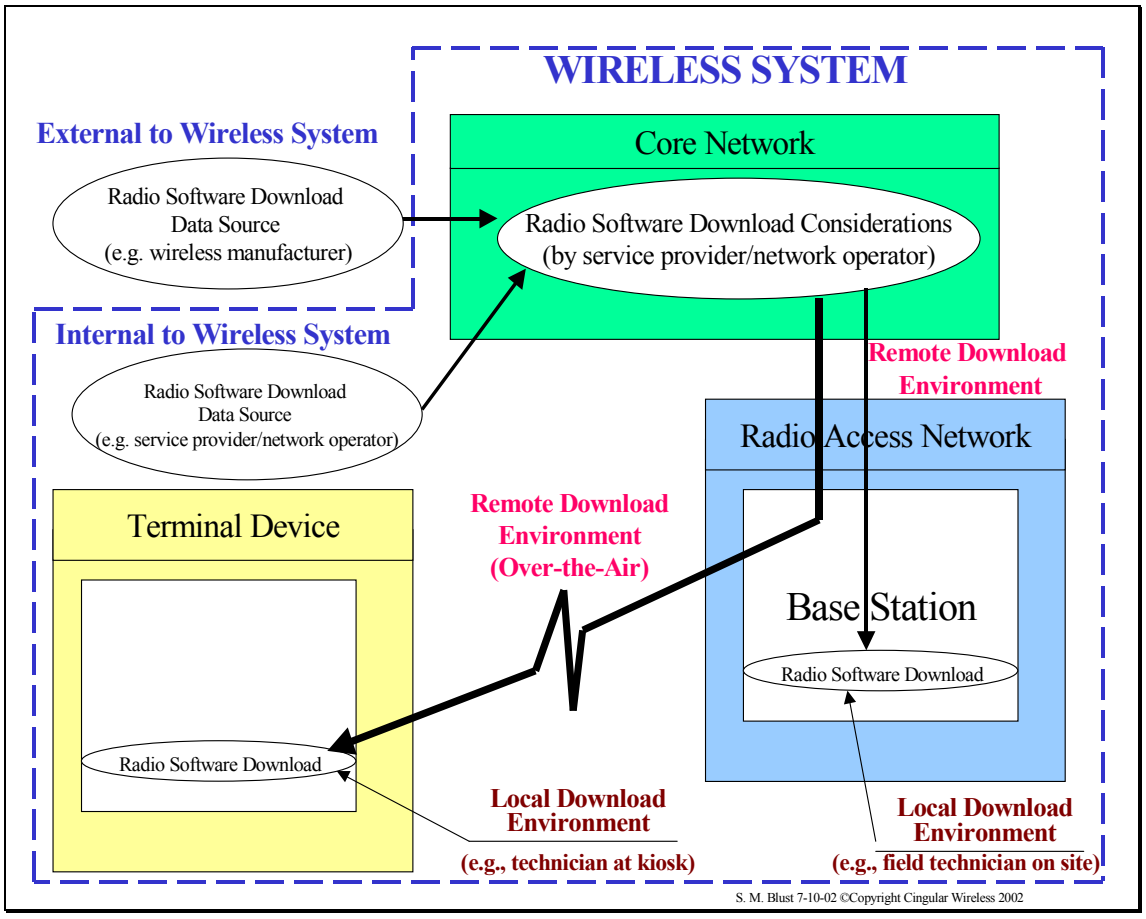


Figure 3-3: Radio Software Download System Flow Example

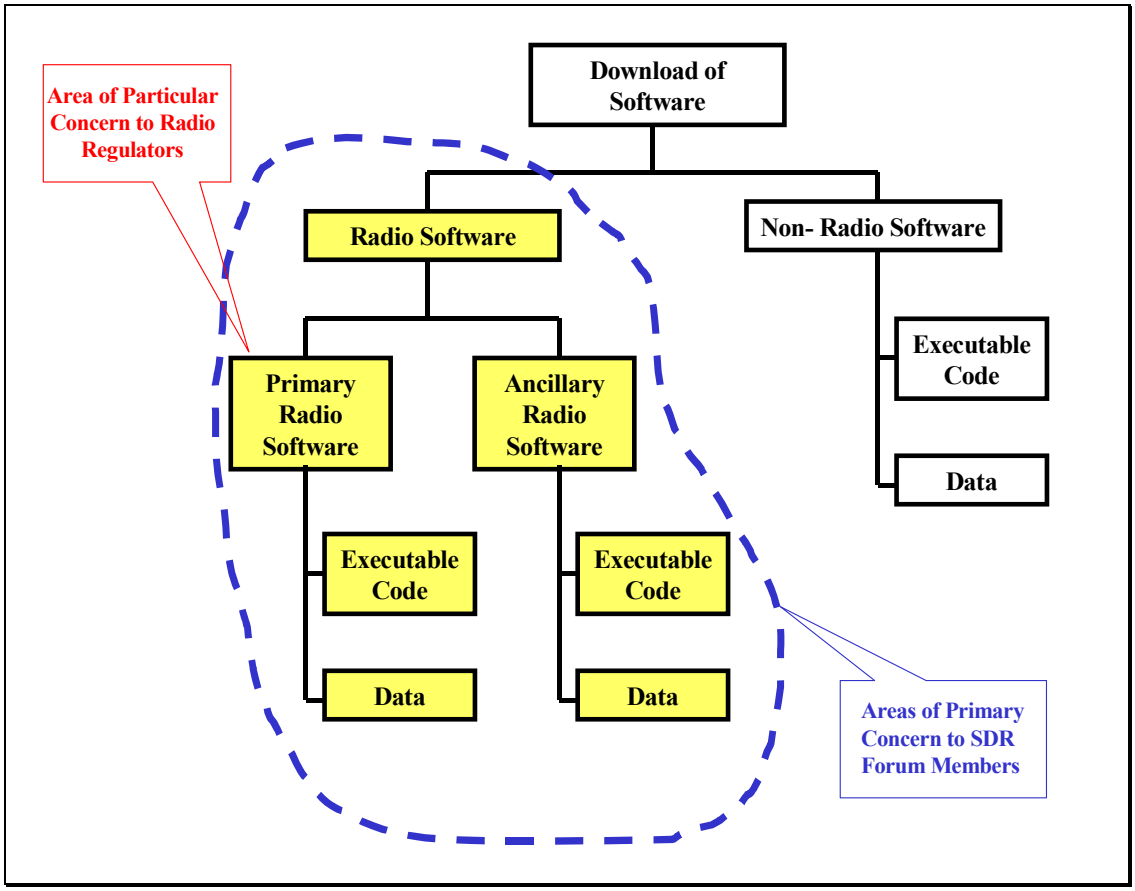


Figure 3-4: Characterizations of Software Download

Table 3-2 contains several example security threats, and also illustrates how the four-part model can be used to classify a given threat.

Table 3-2: Examples of SDR Security Threat Scenarios

	Example Threat Scenario	Point of Attack	Access	Motive	Consequence
1	A sophisticated hacker creates and distributes a virus or malicious application that causes widespread interference **to other communication systems**, such as public safety, emergency, and navigation control communication systems.	Terminal	Remote	Malicious	Interference
2	A sophisticated hacker creates and distributes a virus or malicious application that corrupts the operation of SDR terminals in a manner which causes widespread disruption of service **to the effected communication system**.	Terminal	Remote	Malicious	Denial of Service
3	Manipulation of signaling or control data: Intruders may modify, insert, replay, or delete signaling or control data on any stem interface.	Infrastructure	Remote	Malicious	Denial of Service
4	A black market company creates and distributes a rogue application which causes an SDR terminal to deviate from its normal performance limits, and in so doing, causes widespread disruption of service to the effected communication system. (As an example: an application that causes the terminal transmitter to always transmit at maximum power, ostensibly allowing the user to get better performance, yet actually degrading the overall performance of the system).	Terminal	Remote	Unauthorized	Denial of Service
5	An unethical company takes in old model phones, illegally reprograms and resells the devices as "new" on the black market. The hardware/software combination of the modified phones is unreliable, and causes the devices to eventually "crash" (i.e. suffer an unrecoverable failure)	Terminal	Physical	Unauthorized	Denial of Service
6	A new release of software inadvertently contains a "bug" and is distributed to users in the network. The bug causes terminals to reset unexpectedly, causing widespread denial of service.	Terminal	Remote	Negligent	Denial of Service
7	An unethical company intercepts software downloaded to phones operating in the network, and illegally re-uses the software to build and sell black market devices.	Terminal	Remote	Malicious	Digital rights

8	An unethical company modifies the electronic identifier information on phones intended for sale in one country, and profitably resells the phones in another country where the sale is not legal. (As an example: low cost phones with reduced spectral emission specifications may be legal in one country, but illegal in another country).	Terminal	Physical	Unauthorized	Interference
9	Disreputable parties modify device software, causing them to transmit and/or receive on different frequencies, thus enabling covert communications or eavesdropping.	Terminal	Physical	Malicious	Interference

A wireless base station or handset, employing SDR technologies, should be protected against the threats described above. Achieving robust security must be accomplished through a combination of inherent limitations in the programmability of the unit (as discussed in Appendix E, Section 8), and the addition of specific security features (such as those discussed in Appendix E, Section 9).

3.4 Unique Concerns of Public Safety Organizations

How does the emergence of SDR technology affect Public Safety and what should public safety, with its unique structure, mission and protocols, be concerned with in the implementation of this new technology?

First, the evolution of radio technology is such that in a few years, all radio offerings to public safety will be software defined radios in some form. Second, there are a number of key issues that are currently being considered by both SDR developers and regulatory agencies. For example:

> **Control**. Robust control methods are essential to ensure that SDR technology does not compromise safety and interference controls. Control is ultimately the responsibility of equipment manufacturers to ensure that their products are reliable and tamper-proof. With the emergence of SDR technologies, it will become increasingly common for the software to be loaded in the field (note that this is the norm for current generation cellular base stations). However, there need be no compromise to any of the quality assurance steps: design, verification and configuration control. **The user verification is particularly important to the public safety agency.** Quality should not be compromised as a result of SDR. A central requirement to achieve this quality control is that interfaces within a radio, particularly those which affect emissions and safety, must remain under tight control of the equipment manufacturer, and must be protected through robust security measures.

Third Party Software. SDR technology will allow radio functionality to be implemented in software not necessarily developed by the hardware developer. But there is the potential for significant administrative problems associated with third party software changes. Who would hold the third party accountable for the safe and reliable operation of the revised hardware-software combination? FCC type acceptance procedures and system security are also key issues.

Additional public safety issues include:

- preventing interference from malfunctioning equipment (security)
- ensuring that both hardware and software (OEM and third party) provides protection to Public Safety from illegal use or jamming of public safety channels (security)
- protection from unmanaged use by other public safety users of other land mobile channels. (authorization)
- impersonation of User to the network issues (unauthorized access to the network)
- denial of service (Life threatening issue)
- Impersonation of the network (Life threatening issue) encryption key alteration, encryption suppression
- Threats to system integrity (manipulation to system parameters or mode of operation) Requires robust authentication procedures in base station equipment.
- Eavesdropping on user data (Breach of security, public safety has some experience in this scenario)

Unauthorized interception of radio and/or data communications is of critical concern to public safety users. Interception of such signals could mean death or serious injury to public safety personnel. Sophisticated encryption techniques should be made available to public safety users of SDR technology. AES voice encryption and 128-bit data encryption should be considered minimum standards for public safety SDR devices. Devices can be lost or stolen and, therefore, must be capable of remote revocation of service.

And last but not least, radios currently being considered will need to be priced competitively to be practical for use by public safety. Public safety needs cost effective devices that can access multiple waveforms (public safety and commercial) in durable equipment. This equipment, and the software utilized with it, should be competitively marketed and priced accordingly.

In summary, the development of technology and regulations concerning software defined radios cannot be ignored by public safety. SDR and the increased benefits it brings to public safety will allow public safety agencies to better protect their citizens.

4 Survey of Security Activity

The wireless industry has responded to the security challenges summarized in Section 3 of this report by initiating many research and development programs intended to mitigate the threats of these security challenges. The most significant of these security activities is summarized in this section. The focus is on those security activities that are the most directly applicable to the SDR security challenges.

4.1 General Discussion of Security Activity

The focus of this document is on security for software defined radio including network aspects for systems that incorporate SDR technology. However, core technologies that have been developed for other types of communications systems are applicable to the more specific issue of mitigating any threats to SDR-based communications systems. Appendices H, I, J, K, and L provide information on companies that provide security services or products. The information in these appendices was obtained from the Web[5].

This information is not exhaustive and is presented as indicative of the work in the industry.

4.1.1 Public Key Cryptography

As noted previously, security requirements may be divided into the following categories:

- Trusted system operation
- Authentication
- Authorization
- Integrity
- Privacy
- Non-Repudiation

Realization of the first requirement, "Trusted System Operation", is achieved primarily through product design and development. The last five categories (i.e., authentication, authorization, integrity, privacy, and non-repudiation) require a robust security system framework, such as Public-Key Cryptography (PKC). PKC technologies are well established in other communication industries, and are well suited to address the security issues surrounding SDR. PKC, as it is currently applied to the Internet, has successfully secured billions of dollars of Internet commerce, and can be effectively adapted to address the challenge of securing re-programmable wireless products and systems. A brief overview of PKC may be found in Section 3 of Appendix E.

[5] The inclusion of this information on specific companies and commercial products does not imply endorsement of these companies or products by the SDR Forum. The information provided in these appendices is intended to be illustrative of the large amount of work that has been undertaken by the private sector in addressing security issues. The SDR Forum does not claim that the list of companies and products included is exhaustive.

4.1.2 Trusted Computing

Trusted computing (TC) is a concept for hardening the platform from software-based attacks based on the expected behavior (trust) of the platform and transactions. PC's, Servers, Mobile, Handheld, and Communications devices all play a role in the TC environment. Trusted Computing is an evolutionary sequence of infrastructure and technology ingredients defining "Levels of Trust" that address the 5 critical needs of Internet Transaction Security – Authentication, Authorization, Privacy, Integrity and Non-Repudiation. Features supporting incremental "levels" of Trusted Computing will be developed and added over time.

"Levels of Trust" is a concept of building increasing "levels" of trust benefits and features within the platform as the technology ingredients and the Trusted Computing environment evolves. The features and benefits of these levels are currently being developed in order to define a model and specifications for computing platforms that deliver agreed upon value within each Level of Trust.

The Trusted Computing Platform Alliance (TCPA)[6] was created to address trusted computing issues. The TCPA, formed in 1999 by Compaq, HP, IBM, Intel and Microsoft, originated as the Intel Trusted Computing Initiative within the Intel Architecture Labs (IAL) and the Desktop Architecture Lab (DAL). This initiative was chartered to implement security technologies for the computing platform to enable fundamental criteria for e-business and e-commerce adoption.

Today TCPA has over 160 members, including leading companies in hardware, software, communications, and other technologies. These companies are joined in an open alliance to develop the necessary technology and cooperation to make Trusted Computing a reality.

4.2 Wireless Security Activity

As serious as the security concerns are however, the strength of a market economy is nowhere more evident than in the dramatic proliferation of solutions to wireless security. As documented in a recent Business Week article, “Wireless-Security Outfits Seize the Day”, “Spurred by the meteoric rise of wireless LANs and the arrival of faster data connections over cell-phone networks”… “Players of every size, in software and hardware, are racing to cash in on the need to protect those proliferating untethered networks”… “dozens of software and hardware companies now pitch ways to "lock down" wireless data communications.”

[6] http://www.trustedcomputing.org/tcpaasp4/index.asp

References [1 – 7] provide detailed descriptions of the large amount of work in security that has taken place and is continuing to take place in the wireless industry. Industry's motivation to work on wireless security problems includes the following:

- industry concerns about fraudulent use of the wireless devices which cause a loss of revenue
- user's concerns about privacy
- digital rights

Therefore, the wireless industry will continue to work hard on security issues. Much of this effort is in national and international standards organizations as described later in this report.

4.2.1 Technology Development

There is a vast amount of work by industry in the development of new technologies to mitigate security threats. This technology development addresses threats to all types of communications and information systems. Much of the activity for the wireline communications and information technology systems is also applicable to wireless communications systems. It is beyond the scope of this report to describe all of these technologies. Therefore, only the technologies most relevant to the SDR security challenges are summarized below.

4.2.1.1 Mechanisms and Technologies

The ITU has developed several recommendations on security. For example, References [6 and 7] provide information on security considerations for IMT-2000. Recommendation ITU-R M.1223 [Reference 7] is entitled "Evaluation of Security Mechanisms for IMT-2000". This document defines the following classes of security mechanisms:

- authentication
- anonymity
- confidentiality
- non-cryptographic security mechanisms
- integrity mechanisms
- non-repudiation mechanisms
- security management

This classification of mechanisms may be appropriate, at least in part, for classification of mechanisms for mitigating the SDR security threat as well.

The wireless industry has developed numerous mechanisms for thwarting the threats to wireless communications summarized in Section 3. The detailed descriptions of these mechanisms may be found in the appropriate 3GPP and 3GPP2 technical specifications and associated standards based on these technical specifications and published by the

regional and national standards development organizations. These documents are further referenced in ITU-R Recommendations[7].

The following security mechanisms were not developed specifically for wireless communications systems, but appear to have applicability to wireless systems that employ SDR-capable devices.

- Public Key Cryptography
- Virtual Private Networks
- Firewalls
- Biometric Technologies

Public Key Cryptography is described in Appendix E, Section 5. The other mechanisms also appear applicable to mitigation of the wireless security threats and are described in Appendix M.

4.2.1.2 Security Algorithms

As with specific technologies, it is beyond the scope of this document to provide a detailed description or even a summary of the many security algorithms that have been developed. Instead, a summary listing of security documents developed by 3GPP and 3GPP2 are provided. This is followed by a brief description of examples of commercial implementation of security algorithms.

[7] ITU-R Recommendation M.1457, "Detailed Specifications of the Radio Interfaces of International Mobile Telecommunicatons-2000 (IMT-2000)". This Recommendation provides detailed references to all of the technical standards published by the regional and national mobile telecommunications standards development organizations (SDOs).

Table 4-1 provides a list of security documents developed by 3GPP including algorithms. The documents listed in Table 4-1 may be downloaded from:

http://www.3gpp.org/specs/specs.htm

Table 4-1: 3GPP Security Documents

3GPP Document Number	Document Title	Document Description
TS 21.133	Security Threats and Requirements	Detailed security requirements.
TS 33.102	Security Architecture	Provides a specification of all security mechanisms and protocols, except algorithms.
TS 33.103	Security Integration Guidelines	
TS 33.105	Cryptographic Algorithm Requirements	Defines requirements for standard cipher and integrity algorithm.
TS 33.106	Lawful Interception Requirements	Defines all requirements for network based lawful interception.
TS 33.120	Security Objectives and Principles	Elaborates on the basic principles underlying the security.
TR 33.901	Criteria for Cryptographic Algorithm Design Process	Describes process used to design cipher and integrity algorithm.
TR 33.902	Formal Analysis of the 3G Authentication Protocol with Modified Sequence Number Management	Formal analysis using BAN and Temporal Logic of authentication mechanism.

Table 4-2 lists documents on algorithms developed by 3GPP2. These documents may be downloaded from:

http://www.3gpp2.org/Public_html/specs/index.cfm

Table 4-2: 3GPP2 Security Documents

3GPP2 Document Number	Document Title
N.S0014	Authentication Enhancements
S.R0032	Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy
S.S0053	Common Cryptographic Algorithms
S.S0054	Interface Specification for Common Cryptographic Algorithms
S.S0055	Enhance Cryptographic Algorithms

Example of Commercial Implementations of Security Algorithms

A real concern for mobile devices is the lack of computing resources available for many encryption algorithms. Ntru has developed a small and fast proprietary algorithm that eliminates the need for a separate cryptographic processor and maintains a strong security. The NTRUEncrypt Public Key Authentication and Cryptosystem (NTRUEncrypt PKCS) is a fast and efficient collection of techniques for public key authentication, digital signatures and encryption, with low memory and processor requirements. Compared to current (large integer) based cryptosystems, the NTRUEncrypt PKCS is (with comparable security) over 100 times the speed. Keys are short and easily generated. Ntru's encryption algorithms have been included in Texas Instruments security library for its DSP-based OMAP processor.

The Elliptic Curve Cryptosystem (ECC) is another algorithm being marketed by vendors, such as Certicom, as a public key encryption scheme able to provide the requisite level of security on devices with limited resources, such as mobile phones, PDAs and Smart Cards. ECC offers significant efficiency savings due to its added strength-per-bit when compared to integer factorization systems (e.g. RSA) or discrete logarithm systems (e.g. DSA).

4.2.1.3 Authentication

Authentication refers to the ability to validate the origin of received information. For example, prior to installing new software an SDR device should be able to verify that downloaded data originates from a trusted server. The SDR device should install only authenticated software.

Public-key cryptography can provide a full solution to the authentication problem. As was described in Section 3 of Appendix E, secure methods to generate and verify digital signatures are available. These basic methods can be combined to create a secure Public-Key Infrastructure (PKI) and establish trust in an SDR system. For example, the manufacturer could have private and public authentication keys. The public key would be stored in each of the manufacturer's radios as a root key and the private key would be used to sign software downloads to those radios. Prior to installing any software, the radio would use the root key to verify the digital signature of the software. Since only the manufacturer possesses the private key, only the manufacturer could have created the digital signature, thus the authenticity of software can be proven. The manufacturer could also delegate trust to other third-party entities using certificates. In this case, the public key of a third party could be put into a certificate that is signed by the manufacturer. Software could then be signed by the third-party. The radio would then check the signature of the software using the third-parties public key. Then, the radio would verify the authenticity of this public key by checking the signature of the third-party's public-key certificate using the manufacturer's root key. Many other extensions to this basic premise are also possible.

4.2.2 Standards Based Activity

Standards activity on security mechanisms, algorithms and protocols is taking place in a plethora of organizations. The most significant wireless security activity is summarized in the following subsections. These activities demonstrate the high degree to which the wireless industry is engaged on the subject of security. The industry is constantly reviewing, enhancing, developing, and applying new security technologies to ensure the protection of wireless subscriber devices and the wireless infrastructure networks.

4.2.2.1 International Telecommunication Union

The International Telecommunication Union (ITU) has security activities in both the Telecommunication Standardization Sector (ITU-T) and the Radiocommunication Sector (ITU-R). In ITU-T, the security standardization is focused in Study Group 17 (Data Networks and Telecommunication Software). Most of this work is focused on wireline data communications networks. In ITU-R, the security work is focused in Study Group 8 (Mobile, Radiodetermination, Amateur, and Related Satellite Services). Within ITU-R SG8, Working Party 8F (International Mobile Telecommunications-2000 and Systems Beyond IMT-2000) is responsible for ITU-R recommendations on mobile security, including:

- ITU-R Recommendation M.1078, "Security Principles for International Mobile Telecommunications-2000 (IMT-2000).
- ITU-R Recommendation M.1223, "Evaluation of Security Mechanisms for IMT-2000"

WP8F plans to update these security documents within the next year and possibly create new security recommendations. WP8F is also in the process of developing a report on technology trends that includes software defined radio. It is expected that future recommendation (s) from WP8F will address global issues associated with software defined radio including circulation and security issues.

4.2.2.2 GSM Association

Founded in 1987, the GSM Association has played a pivotal role in the development of the GSM platform and of the global wireless industry. Members include more than 400 operators in 175 countries/areas of the world. Associate Membership is open to suppliers of the GSM Family of technology platforms (GSM, GPRS, EDGE and UMTS) including application providers, billing systems suppliers, data clearing houses, Financial Clearing Houses , GRX Carrier, Infrastructure Suppliers, Mobile Terminal suppliers, roaming brokers, SIM card suppliers, security systems suppliers, signaling providers, and simulators suppliers.

A Security Group was established to maintain and develop GSM Association algorithms and protocols, technical security aspects of customer apparatus and to examine and recommend infrastructure solutions to combat fraud. The Group consists of technical representatives from Association members who study the security threats to GSM, its

interfacing with 3GSM and converging technologies, and advises members on security issues.

The Security Group has realized two important initiatives over the past 12 months. First, it has introduced a new GSM security algorithm called AS/3. This is a further enhancement of the AS algorithm that ensures security between base station and terminal. This latest improved algorithm will also be deployed as the 3GSM algorithm, which will mean that multi-band terminals will be able to take advantage of advanced third generation security.

The group along with the 3GPP security group also accomplished the second key security advance in cooperation with US standards bodies. The result has been the introduction of a security protocol -known as an authentication key agreement (AKA) - that will be applicable to all mobiles, regardless of whether they have been developed according to 3GPP or 3GPP2 standards

The group has also been addressing the security issues associated with GPRS. GPRS essentially opens up customer terminals and network elements to the Internet world. GPRS backbones are implemented on IP based networks which means the routing and access control issues need to be carefully considered.

In order to maintain the proper level of security with GPRS services there are some requirements for GPRS operators and Inter-PLMN backbone providers. A starting point for focusing on various security aspects of GPRS networks includes:

- security of the subscribers
- security of the GPRS network itself
- security of the various interconnections (GRX, BG, charging…)

Among the security issues the group has identified are: unsolicited data to customers; customer service termination; mobile users running servers or acting as gateways; communication strategy to inform customers of risks; denial of service attacks; uncontrolled terminal equipment; user visibility within the architecture; authentication; end to end security vs link by link security; legal interception; abuse content; monitoring and supervision; reliability of charging data; advices and warnings between GPRS operators; security border separations; reaction in case of compromise; APN provisioning and control for roaming.

These security issues are discussed by clearly identifying the nature of the problem, providing a brief overview of the problem, the likely impact and some solutions/recommendations in the “GPRS Security Focuses**”** [Reference 2].

4.2.2.3 European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) created a security group within the GSM standards effort called SMG10. In conjunction with the Secure Algorithms Group of Experts (SAGE) and the GSM Association Security Group, they developed protocols and algorithms to secure the GSM cellular system. This work is continuing in the Third Generation Partnership Project (3GPP) within the security group

3GPP TSG SA WG3. Current projects include TS 33.203 Access Security for IP- based services and TS 33.210•Network Domain Security - IP network layer security.

4.2.2.4 3GPP

References [1 – 5] provide detailed information regarding the work of the Third Generation Partnership Project (3GPP) and its subordinate activity, the Mobile Execution Environment that is described in the following section.

4.2.2.5 MExE (Mobile Execution Environment)

MExE (pronounced "mexy") stands for Mobile Execution Environment. It provides a standardized application execution environment for Mobile Terminals. To realize this promise a means was necessary to coordinate and match the efforts of the major elements from mobile terminal manufacturers, network operators, and application and service developers.

For instance, applications developers needed to know the capabilities of their target platforms and networks; network operators required an understanding of the resource demands that new services might require; and all would need a negotiation process for the discovery, delivery, and execution of downloadable applications and services.

And so, in 1997, MExE began as a work item in ETSI, and has since migrated to become a working group within 3GPP.

A white paper describing MExE is provided in Reference 3. The detail specification "Mobile Execution Environment (MExE); Functional description Stage 2 (Release 4)" is provided in Reference 4.

As security is inexorably linked to the success of applications, content, and commerce in the mobile environment, it has always received prominent attention in MExE. Three fundamental elements make up the basis of MExE security:

1) A framework of permissions, which defines the permissions, transferred MExE executables have within the MExE device;
2) the secure storage of these permissions; and
3) conditions within the execution environment that ensure that MExE executables can only perform actions for which they have permission.

The structure of this framework is a matrix of various logical areas or "Domains"; entities that have permission to control the download and execution of software in the domains; and a list of actions that are performed by the software. The domains are currently defined as: MExE Security Operator Domain; MExE Security Manufacturer Domain; MExE Security Third Party Domain; and MExE Untrusted Area.

In order to enforce the MExE security framework, a MExE device is required to operate an authentication mechanism for verifying downloaded MExE executables. A successful authentication will result in the MExE executable being trusted. As the MExE device may want to authenticate content from many sources, a public key based solution is

mandatory. Before trusting MExE executables, the MExE device will therefore check that the MExE executable was signed with a private key, for which the MExE device has the corresponding public key. The corresponding public key held in the MExE device must either be a root public key (securely installed in the MExE device, e.g. at manufacture) or a signed public key provided in a certificate. The MExE device must be able to verify certificates, i.e. have the public key (as a root key or in a certificate) corresponding to the private key used to sign the certificate.

The details of MExE security are documented in [Reference 4].

4.2.2.6 3GPP2

Starting in the late 80's, the Telecommunications Industry Association (TIA), responsible for establishing cellular systems standards in the United States and Canada, created the TR-45.3 Ad Hoc Authentication Group (AHAG). This group developed the authentication protocols and algorithms that are used in the second-generation (2G) ANSI-41-based cellular systems. They also developed algorithms to protect the privacy of voice and later data communications for these digital cellular systems. This work is continuing in the Third Generation Partnership Project 2 (3GPP2). The security group here has been given the title 3GPP2 TSG SA WG4. They will now extend the AHAG work to include mutual authentication (between the subscriber and the network), integrity protection and security in the packet switched domain.

4.2.2.7 Mobile Commerce Initiatives

In addition to standards activity in the general wireless security area, the great promise of mobile financial transactions has generated a plethora of work specifically aimed at enabling secure mobile transactions.

A number of initiatives have been announced to encourage the use of mobile technology in financial services and to drive the adoption of open standards in this field. Some examples of commercial activities in this area may be found in Appendix M.

With the emergence of m-commerce, ETSI is in the process of developing Mobile Electronic Signature Standards.

4.2.2.8 Other Wireless Standards Security Activities

The Java development community has adopted the MExE security model as the basis for the security aspects of JSR 118 Mobile Information Device (MIDP) Profile 2.0. MIDP 2.0 is the part of the next generation of the J2ME standard.

The WAP Forum Security Group has been developing standards for the security layer protocol in the WAP architecture called Wireless Transport Layer Security (WTLS). They are now working with the Internet Engineering Task Force (IETF) in order to make their Transport Layer Security (TLS)-related RFCs mobile friendly.

Other on-going mobile security work is being carried out within the Bluetooth Special Interest Group, the International Telecommunication Union (ITU), the Mobile Wireless Internet Forum (MWIF) and the World Wide Web Consortium (W3C).

4.2.3 Public Safety Wireless Security Activity[8]

Security is a paramount concern for public safety users. The ability for public safety users to transmit and receive emergency information on the first attempt often means the difference between life and death. This is best illustrated by the SWAT team commander notifying the sniper with the "shoot" or "don't shoot" command.

Public safety has utilized a variety of measures to help insure varying degrees of security on radio systems. The majority of public safety radio systems are very small analog systems that have been in use for many years. Most of these systems are relatively insecure using simple Private Line (PL) tones as the main source for system security. Larger/newer public safety systems utilize device identification/authentication coupled with the ability to deactivate offending devices remotely. Public Safety systems are gradually moving toward widespread digital system proliferation.

The use of encryption to improve security in public safety systems varies based on the sophistication of the system. While low-level, analog encryption is still utilized in some systems where it fills the security need for that specific agency, many agencies have migrated to digital systems where encryption has proved to be more effective. Agencies have to adjust to encryption key management principles as their systems mature, to ensure their security concerns are met.

The public safety community has addressed security issues in the development of a standard for digital land mobile communication. The effort, called APCO Project 25, is an ongoing joint effort of U.S. federal, state, and local government, with support from the U.S. Telecommunications Industry Association (TIA). In the Project 25 process, state government is represented by the National Association of State Telecommunications Directors (NASTD) and Local Government is represented by the Association of Public Safety Communications Officials (APCO). The standards process is called "APCO Project 25" and the standards themselves are called "Project 25." Of the three groups of users, APCO (i.e., local government) members are the largest group of users of Land Mobile Radios (LMR). The current Project 25 encryption standard is DES (56-bit encryption) for Project 25 Phase 1 and Triple DES (168-bit encryption) for Project 25 Phase 2. The National Institute of Standards and Technology (NIST) has adopted Advanced Encryption Standard (AES) to replace DES as the official U.S. Government encryption standard. AES is secured with 256-bit encryption.

The primary objectives of the APCO Project 25 (P25) standards process are to provide digital, narrowband radios with the best performance possible, to meet all public safety user needs, and to permit maximum interoperability. Secondary objectives include obtaining maximum radio spectrum efficiency, ensuring competition throughout the life of systems, and ensuring that equipment is user-friendly. During the process, the needs

[8] Source: National Public Safety Telecommunications Council (NPSTC) SDR Working Group

of the user have always been put first. Performance and meeting user needs were always placed higher in priority than spectrum efficiency or reducing technical complexity.

The developers of the Project 25 standards realized system security was a vital component of mission critical land mobile communications and began work to develop a security standard for the Project 25 suite of standards. As provided for in a MOU between TIA and APCO Project 25 in January 1996, TIA issued a Security Services Overview to APCO Project 25 effort that would provide guidelines for the development of a Project 25 digital security standard. The Security Overview recommended options for the APCO Project 25 to consider in their standards process. The table of contents of the APCO 25 Security Services Overview is provided below:

1. Introduction
2. Scope
3. Overview
   - 3.1 Definitions
   - 3.2 Security Threats
     - 3.2.1 Message Interception
     - 3.2.2 Message Relay
     - 3.2.3 Spoofing
     - 3.2.4 Misdirection
     - 3.2.5 Jamming
     - 3.2.6 Traffic Analysis
     - 3.2.7 Subscriber Duplication
     - 3.2.8 Theft of Service
4. Confidentiality
   - 4.1Encryption Transformation
     - 4.1.1 Traffic Encryption
     - 4.1.2 Address Encryption
5. Authentication
   - 5.1 Chronological Integrity
   - 5.2 Message Integrity
   - 5.3 Source Authentication
6. Key Management
   - 6.1 Physical Key Distribution
   - 6.2 Over-The-Air Distribution
     - 6.2.1 Automated Key Management
     - 6.2.2 Public Key Techniques
   - 6.3 Key Compromise
7. History and References

4.2.4 Terrestrial Trunked Radio

TErrestrial Trunked RAdio (TETRA) is an open digital trunked radio standard defined by the European Telecommunications Standardisation Institute (ETSI) to meet the needs of mobile radio users. TETRA is defined to support both voice and data communications. It specifies the air interface, the inter-working between TETRA systems and other systems via gateways, terminal equipment interfaces on subscriber equipment and the security aspects in TETRA networks.

The ETS issued Document ETS 300 392-7 in December 1996, titled "Radio Equipment and Systems; Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security. The content of the report is listed below:

1. Scope
2. Normative references
3. Definitions
4. Air Interface authentication and key management mechanisms
   - Air Interface authentication mechanisms
   - Air Interface key management mechanisms
   - Service description and primitives
   - Definition of protocols
   - OTAR protocol functions - CCK
   - OTAR protocol functions - SCK
   - OTAR protocol functions – GCK
   - PDU descriptions
   - MM PDU type 3 information elements coding
   - PDU information elements coding
   - Boundary conditions for the cryptographic algorithms and procedures
   - Dimensioning of the cryptographic algorithms and procedures
   - Dimensioning of the cryptographic parameters
   - Summary of the cryptographic processes
5. General relationships
   - Enable/Disable state transitions
   - Mechanisms
   - Enable/disable protocol
6. Air Interface
   - General principles
   - Mobility procedures
   - Air interface encryption protocol
   - Service description and primitives
   - Protocol functions
   - PDUs for cipher negotiation
7. End-to-end encryption
8. History

The TETRA document is available for download at http://pda.etsi.org/pda/AQuery.asp

4.3 Activities Specific to SDR

As described in Appendix F, the SDR Forum has embarked on a program for the development of a series of documents for software download for RF reconfiguration for SDR-capable devices. The download documents produced by the SDR Forum will be provided to Standards Development Organizations for their consideration in the development of download technical specifications and standards. Security is an important aspect of the software download issues. The SDR Forum will be the focal point for the development of these download documents including security aspects related to SDR.

The Mobile VCE as described in Appendix D has developed a reconfiguration architecture for SDR. Within this structure, Mobile VCE proposes the use of Public Key

Infrastructure (PKI) to secure signaling and reconfiguration software exchanges. This work is ongoing.

Intel's Corporate Technology Group is developing a Software Radio Security Specification. The specification will define security mechanisms necessary to securely alter radio software. The specification describes the transaction types, algorithm implementations, certificate definition and key management protocols required to design and build secure software radios. The goal of the specification (currently at revision 0.2) is to define an open architecture that will allow system OEMs and peripheral developers adequate room for product versatility and market differentiation.
As stated previously, security mechanisms developed for other communications systems appear to be applicable to SDR as well as the communications systems for which they were originally developed.

Public-Key Cryptographic Systems have been around for a long time (since 1976) and are well suited to address the security issues surrounding SDR. One advantage of a PKC approach is that the manufacturer would not be required to install a unique shared key into every SDR device. Instead, the manufacturer stores a root key in every SDR device that is used to verify the digital signature of the software downloads. Thus, the key management problem has been eliminated. Also, a root key stored in a PKC-based approach does not need to be kept secret. Its integrity must be ensured, but this is an easier requirement than maintaining a secret key. For example, the root key could be stored in an unalterable memory of the SDR terminal, such as Read Only Memory. Also, a PKC approach allows for signatures to be generated that can be verified by a multiplicity of units, each containing the root key. Thus broadcasting of signed downloads to multiple SDR radios is possible. Finally, a PKC approach can also support a hierarchical infrastructure, which makes distribution of trust, revocation, and the inclusion of third-party developers much easier and more secure than with the sharing of secret keys. Internet security technologies, such as PKI, have successfully secured billions of dollars of Internet commerce and are more than up to the challenge for securing wireless systems.

5 Market Incentives for Deployment of Existing Security Technologies in SDR-Based Systems

Preceding sections have provided:

- Information about the security challenges from a broad general view of communications security issues, a more specific wireless communications point of view, and finally from the viewpoint of specific challenges from a software defined radio perspective.
- A description of activities that are ongoing that will mitigate these security challenges.
- Specific security activities against the security threat to software defined radio.

It is critical to both regulators and to the wireless industry that adequate protection be incorporated into SDR-based systems that prevents either malicious or unintentional modification of key radio parameters such as frequency, transmitted power, and modulation.

As documented throughout this report, a wealth of technical solutions exist that can be employed to secure digital information and systems. However, in the larger IT community it has been generally recognized that "many security risks remain unsolved or solutions are slow coming to the market as a result of certain market imperfections".[9] As stated by Dr. Ross Anderson in his paper: Why Information Security is Hard: An Economic Perspective, "information insecurity is at least as much due to perverse incentives."[10] Leading economist Hal Varian stated in his June 1, 2000 New York Times column "one of the fundamental principles of the economic analysis of liability: it should be assigned to the party that can do the best job of managing risk."[11] In the situations where this is not the case adequate security mechanisms may not be deployed. As put by Dr. Anderson, "In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected." This topic of market imperfections was the focus of a landmark first international workshop on the economics of security recently held at UC Berkeley in May 2002, co-chaired by both Dr. Anderson and Hal Varian. There is ample current literature, therefore, on the topic to make a credible survey of the market imperfections impacting general IT security, and their relevancy to SDR.

Using as a framework the EC Communication document's "Network and Information Security: Proposal for A European Policy Approach "[12] categorization of these imperfections (Social costs and benefits, Asymmetry of Information, and The public action problem); we will briefly describe each market imperfection and then their application to the particular issue of SDR.

---

[99] Network and Information Security: Proposal for A European Policy Approach: pg 2
[10] http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf
[11] http://www.nytimes.com/library/financial/columns/060100econ-scene.html?printpage=yes
[12] Network and Information Security: Proposal for A European Policy Approach pg 19

5.1 Market Imperfections in General Information Technology Security

This section first examines the basic issue of security problems associated with market inefficiencies in the general IT environment.

5.1.1 Social Costs and Benefits

As stated in the EC document "Investment in improved network security generates social costs and benefits which are not adequately reflected in market prices. **On the cost side**, market actors are not responsible for all the liabilities related to their security behavior. Users and providers with low levels of security do not have to pay third party liability. This is like a careless car driver who is not held liable for the costs of the traffic jam that occurred as a result of his accident. Similarly, on the Internet several attacks have been mounted through the ill-protected machines of relatively careless users. **Security benefits are also not fully reflected in market prices**. When operators, suppliers, or service providers improve the security of their products a good deal of the benefits of this investment accrue not only to their customers but to all those directly or indirectly affected by electronic communication - basically the whole economy."

5.1.2 Asymmetry of information

Networks are becoming increasingly complex and are reaching a wider market that includes many users with little understanding of the technology or its potential dangers. This means users will not be fully aware of all the security risks and many operators, vendors, or service providers have difficulties assessing the existence and widespread of vulnerabilities. Many new services, applications and software offer attractive features but often these are the source of new vulnerabilities (e.g. the world wide web's success is partly due to the range of multimedia applications that can be easily downloaded but these 'plug-ins' are also an entry point for attacks). Whilst the benefits are visible, the risks are not and there are more incentives for suppliers to offer new features than greater security."[13]

5.1.3 The public action problem:

In his presentation to the Berkeley workshop, Hal Varian stated, "System reliability often depends on the effort of many individuals, making reliability a public good. It is well-known that purely voluntary provision of public goods may result in a free rider problem: individuals may tend to shirk, resulting in an inefficient level of the public good."

"How much effort each individual exerts will depend on his own benefits and costs, the efforts exerted by the other individuals, and the technology that relates individual effort to outcomes."[14] The EC Communication states "Operators are increasingly adopting the

[13] ibid pg 19
[14] System Reliability and Free Riding, Hal R. Varian University of California, Berkeley http://www.cl.cam.ac.uk/users/rja14/econws/49.pdf

Internet standards or somehow linking their networks to the Internet. However, the Internet was not designed with security in mind but on the contrary was developed to ensure access to information and to facilitate its exchange. This has been the basis for its success. The Internet has become a global network of networks of unparalleled richness and diversity. Investment in security often only pays off if enough people do the same. Thus **cooperation** to create security solutions is required. But co-operation only works if a critical mass of players participates which is difficult to achieve as there are 'free-rider' profits to be made. Interoperability between products and services will allow for competition between security solutions. However there are substantial co-ordination costs involved as global solutions might be required and some players are tempted to impose a proprietary solution on the market. As a multitude of products and services still uses proprietary solutions there is no advantage to using secure standards which only give extra security if everyone else offers them."[15]

5.2 Relevancy of Market Inefficiencies With Regard to SDR

We now examine the applicability of each of the aforementioned market inefficiencies with regard to SDR.

5.2.1 Social Costs and Benefits

Because of the enormous number of cellular devices which are deployed, improper, erroneous, or malicious operation of a terminal device may have great potential for causing system disruption. Handsets are also, by virtue of their consumer focus, extremely cost sensitive; and so represent the severe case of potential risk from cost consideration induced security lapses.

If we consider a worse case, where Byzantine behavior of a rogue handset completely denies an entire cell cite, the impact on the operator is readily identifiable:

1. Lost revenue- the operator loses revenue for all the calls that would have been made during the period that the cell site is down.
2. Lost subscribers- The churn ratio (the number of subscribers who change operator) is very high in the commercial wireless industry, representing subscribers readiness to switch service providers. Since the typical cost of acquisition for a subscriber can be several hundreds of dollars, operators are highly competitive with regard to providing subscribers maximum quality of service. A major disruption to many subscribers simultaneously would have substantial financial impact to the operators; both from the loss of customers directly affected, and the negative publicity that would ensue.

The value of secure operation, then, is substantial and immediately recognized by operators. This value directly translates to a key product requirement that handset manufacturers, and component manufacturers compete to deliver to their customers.

[15] Network and Information Security: Proposal for A European Policy Approach pg 19

The additional bill of material costs to incorporate additional security features, are expected to be well below the added value they will provide, by virtue of the ever-increasing processing power and memory included in latest generation handset.

The SDR security situation is not like the general IT situation where the value and benefit of security mechanisms is not recognized and therefore not deployed in some instances. In the case of SDR, the value of security is immediately recognizable and quantifiable and easily justifies the expected marginal incremental cost required to deploy such security mechanisms especially when security is a key criterion from the onset. Because SDR devices are not widely deployed, the cost efficiency of incorporating security measures is higher than if such measures were to be incorporated after wide scale deployment.

5.2.2 Asymmetry of Information

Unlike the general IT situation where there is varying levels of control over client devices attached to a network; from closely controlled private networks, to no control of devices connected to the internet; commercial handsets must be qualified to operate on an operators network before they are allowed to connect. Therefore operators have complete control over the capabilities of devices they allow to connect to their network. As such there is no asymmetry of information in the case of handsets deployed on an operators network.

5.2.3 The Public Action Problem

As mentioned above, commercial operators have enormous and adequate incentive to incur the cost required to deploy technology to protect their networks and service to their users. However another question is whether such actions will be adequate to protect other spectrum owners. This question is answered in several ways:

1. The technologies deployed to secure operation in authorized bands, by default will prevent operation in non-authorized bands.
2. Wide-band capability that would be required to interfere with non-authorized bands requires more costly components that are price prohibited in the sensitive consumer market. In addition, in a digital system the cost required to "mask" off specific digital areas (and by design their corresponding areas on spectrum) is negligible. Therefore even in the case of a software bug causing unintentional operation of a handset, the risk of it impacting other frequency bands is greatly reduced by natural economic conditions.

In the area of SDR for commercial wireless services, the risks, liabilities, and value of security are well distributed between all parties who will develop and deploy.

6 Future Work

The SDR Forum plans on continuing its investigation and analysis of security threats to SDR and ongoing activities to mitigate those threats. The Forum will document the results of this future work in a second, more comprehensive, report. Specifically the Forum will:

1. Analyze the application of security mechanisms developed for other communications systems and for general threats to wireless communications systems to the more specific problem of security threats to SDR-based communications systems.
2. Report on additional activity by industry in mitigating the threat to SDR-based systems.
3. Report on the SDR Forum's activity in working with other organizations. It is envisaged that the Forum may generate additional requirements for security standardization that will be provided to recognized standards development organizations (SDOs) to develop the appropriate standards.
4. Report on the progress of the SDR Forum series of documents on software download for RF reconfiguration which includes the security aspects of software download.
5. Provide motivation to industry to accomplish SDR security tasks by providing a focal point on SDR-related security matters.
6. Encourage industry to develop common SDR security solutions (or a small universe of solutions) rather than many unique and proprietary solutions.

Encourage industry to develop security measures that are globally accepted by regulators and commonly applied by industry across differing wireless communications systems.

7 References

[1] "A Guide to 3 rd Generation Security"; (3G TR 33.900 version 1.2.0); 3rd Generation Partnership Project, Technical Specification Group SA WG3; available at:
ftp://ftp.3gpp.org/specs/archive/33_series/33.900/33900-120.zip

[2] "GPRS Security Focuses"; SG Doc. 033/01, March 2001; Security Group GSM Association

[3] "Mobile Execution Environment (MExE) White Paper"; December 2000; available at:
http://www.mexeforum.org/MExEWhitePaperLrg.pdf (High Resolution)
http://www.mexeforum.org/MExEWhitePaperSml.pdf (Low Resolution)

[4] "Mobile Execution Environment (MExE) Functional description Stage 2 (Release 4)"; 3GPP TS 23.057 v4.4.0 2001-12; 3rd Generation Partnership Project, Technical Specification Group Terminals; available at:
ftp://ftp.3gpp.org/specs/archive/23_series/23.057/23057-440.zip

[5] "Security Threats and Requirements"; 3GPP TS 21.133 V4.1.0 (2001-12); 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects; available at:
ftp://ftp.3gpp.org/specs/archive/21_series/21.133/21133-410.zip

[6] "Security Principles for International Mobile Telecommunications-2000 (IMT-2000)", ITU-R Recommendation M.1078; available for purchase through the ITU at:
http://www.itu.int/publications/index.html

[7] "Evaluation of Security Mechanisms for IMT-2000", ITU-R Recommendation M.1223; available for purchase through the ITU at:
http://www.itu.int/publications/index.html

Appendix A: SDR Forum Request for Information: FCC Inquiry on Methods for the Security and Authentication of Radio Software

Inclusion of the responses (Appendix B through E) to the SDR Forum RFI implies no endorsement of these views by the SDR Forum and the viewpoints represented in these responses are not to be construed as SDR Forum approved or official positions. The RFI responders have authorized the SDR Forum to include their submissions in this document.

SDR Forum Request for Information: FCC Inquiry on Methods for the Security and Authentication of Radio Software

At its meeting on Sept. 13, 2001, the FCC adopted a Software Defined Radio (SDR) First Report and Order, which removed barriers to entry of SDR products in the marketplace. The new rules allow manufacturers and operators to reconfigure devices after they have been deployed in the field and will speed the introduction of advanced technology and new services.

SDR provides an efficient and comparatively inexpensive mechanism for the design and implementation of multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades, thus addressing many of the most challenging issues confronting the wireless industry.

SDR technology provides the building blocks to affordably integrate a wide variety of mobile Internet applications over multiple air interfaces, using multiple technologies to provide rapid access to advanced wireless networks.

These great benefits of programmability come with the responsibility for diligence in deploying security measures to protect against un-wanted operation.

In the Report and Order, the FCC made clear its view that it is critical "to ensure that software changes cannot be made to a radio that will cause it to operate with parameters outside of those that were approved in order to prevent interference to authorized radio services." But the Commission accepted the argument of the Forum that it would be unwise for it to "to set specific security or authentication requirements."

As it has considered software defined radio issues, the Commission has consistently looked to the SDR Forum for relevant technological expertise. This was nowhere more true than in its consideration of security issues. The Commission noted that "the SDR Forum has indicated that it is continuing to develop methods for the security and authentication of radio software and that it will report its findings to the Commission." The Commission asked that such findings be reported to it within the year.

Accordingly the SDR Forum is preparing a mid-year report to the FCC on industry measures to address these security concerns including:

- The development and deployment of software security related technologies including dynamic security algorithms, mechanisms, and technologies; authentication technology including biometric devices and Digital Rights Management for valuable content protection.
- Security initiatives in Special Interests Groups;
- Activities of Standards Bodies Organizations.

The issue of software security spans the breadth and depth of industry today from financial institutions providing secure transactions; to the security measures of enterprises and institutions against network damaging viruses and denial of service attacks; to the entertainment industry protecting piracy of valuable music and video content. Recognizing this the SDR Forum is soliciting input from a wide range of organizations who's development and activity in the area all contribute to a common knowledge base. **Organizations are encouraged to contact the SDR Forum by April 1, 2002 to be included in this report.**

Appendix B: Intel Corporation, Intel Response to the SDR Forum Request for Information for its Mid-Year Report to the FCC on Industry Measures to Address Methods for the Security and Authentication of Radio Software

Intel Response to the SDR Forum Request for Information for its Mid-Year Report to the FCC on Industry Measures to Address Methods for the Security and Authentication of Radio Software

Revision 0.1
June 3, 2002

INTRODUCTION

Intel is pleased to provide this contribution to SDR Forum's request for information on the activities in the area of security for software download.
Intel has a long history as a leader in the area of digital security; as a manufacture of security products and building blocks such as the Intel® VPN product family; in advanced security research and development in its Corporate Technology Group; and by founding and participating in industry initiatives.

Moreover, Intel has invested substantial resources specifically targeted to assuring security for software download on mobile devices by making secure environments for users, networks, and enterprises the cornerstone of the Intel® Personal Internet Client Architecture.

GENERAL DIGITAL SECURITY

One example of Intel's leadership in the area of digital security is the Trusted Computing Platform Alliance (TCPA) http://www.trustedcomputing.org/tcpaasp4/index.asp . The TCPA, formed in 1999 by Compaq, HP, IBM, Intel and Microsoft, originated as the Intel Trusted Computing Initiative within the Intel Architecture Labs (IAL) and the Desktop Architecture Lab (DAL). This initiative was chartered to implement security technologies for the computing platform to enable fundamental criteria for e-business and e-commerce adoption.

Trusted computing (TC) is a concept for hardening the platform from software-based attacks based on the expected behavior (trust) of the platform and transactions. PC's, Servers, Mobile, Handheld, and Communications devices all play a role in the TC environment. Trusted Computing is an evolutionary sequence of infrastructure and technology ingredients defining "Levels of Trust" that address the 5 critical needs of Internet Transaction Security – Authentication, Authorization, Privacy, Integrity and Non-Repudiation. Features supporting incremental "levels" of Trusted Computing will be developed and added over time.

"Levels of Trust" is a concept of building increasing "levels" of trust benefits and features within the platform as the technology ingredients and the Trusted Computing environment evolves. The features and benefits of these levels are currently being developed by Intel and Industry leaders in order to define a model and specifications for computing platforms that deliver agreed upon value within each Level of Trust

Today TCPA has over 160 members, including leading companies in hardware, software, communications, and other technologies. These companies are joined in an open alliance to develop the necessary technology and cooperation to make Trusted Computing a reality.

SECURE WIRELESS DEVICES

The convergence of wireless connectivity and a general-purpose programmable platform heightens some existing concerns and raises new ones, so that environmental factors as well as traditional technology and market drivers will influence the architecture of these devices.

Wireless communications poses unique security challenges by virtue of the fact that the transmission is exposed to interception. This has allowed, for instance the interception of

information to clone cell phones, by using electronic scanners to record the mobile identification number and the electronic serial number and program them on to another phone.

In addition, next-generation cellular phones will be mobile IP enabled, allowing them to access the Internet and corporate intranets creating significant safety and security challenges for network operators, corporate IT departments, and government regulatory agencies. These devices and their associated network infrastructures will begin to confront many of the same safety and security issues facing the traditional PC desktop/server environment.

One of the most discussed wireless security issue is the shortcoming of the 802.11b WLAN (Wireless Local Area Network) standard's Wired Equivalency Protocol (WEP), the original WLAN security protocol. Intel has published a series of white papers documenting the flaws, and activity underway to correct them.[16]

A handset's susceptibility to malicious virus attacks must be mitigated, just as in the desktop environment. Similarly, a handset's radio frequency emissions (frequency, power) must not be altered by any unintended interactions between downloaded applications and the basic communications functions within the handset. The primary environmental factors that are shaping the architecture of next generation mobile devices economic, security, and privacy.

1. Economic: From a business perspective this is of course creating products or services that customers find attractive. There can also be non-commercial societal values desired.

2. Security: Against the great benefits of programmability, however, we have the specter of security risks. These can take the form of network damaging viruses and denial of service attacks, fraudulent use of the network, and the piracy of spectrum; access and damage to sensitive data behind corporate firewalls; digital content theft; and theft or damage of customer applications or data.

3. Privacy: Against the need for authentication to combat commercial fraud, and legitimate law enforcement requirements, we must also balance the need to maintain the privacy of individuals and corporations against unwarranted invasion such as unauthorised access to customer proprietary network information, and sensitive local user data such as stored in persistent memory or generated by context-aware technology.

To maintain both network and user space integrity, communications software will be "decoupled" and executed in parallel with user applications being written to a general-purpose processor running in a general-purpose execution environment. This partitioning maximizes the economic viability by allowing application development to evolve independent from communication standards, as well as enhancing security by providing autonomous network and user spaces.

Creating coexistent autonomy for the radio subsystem, application subsystem, and memory subsystems portions is evolving as a means to solve the triple environmental requirements of enabling economically viable products and services; while maintaining network and corporate security, and user sovereignty over application space and data privacy. Put anecdotally, "good fences make good neighbors."

Although the native security protocol for 802.11 can be breached, the technology is still rapidly deploying, even for security minded enterprises. This is because the security issue has been dealt with easily by running a Virtual Private Network over the connection. A Virtual Private Networks is a program that uses encryption, and authentication techniques to create a secure channel over an unprotected network. Many companies and organizations equip their employees

[16] http://cedar.intel.com/media/pdf/security/wired.pdf
http://cedar.intel.com/media/pdf/security/80211_part2.pdf
http://cedar.intel.com/media/pdf/security/80211_part3.pdf

with VPNs to allow them to take advantage of the multiple broadband connections now available in the home and when traveling.

The speed with which a solution was deployed that allowed 802.11 to continue to grow dramatically highlights the fundamental benefits of a de-coupled or “layered” architecture. The PC, being abstracted from the WLAN by a standard interface, was able to maintain its own security by deploying a solution separate and independent from the network interface; with minimal or zero additional cost.

By greatly reducing the interdependencies of the three players (economics, security, privacy) experimentation for finding the equilibrium can occur much more quickly and at much lower cost.

Realizing the need of meeting all three critical requirements simultaneously, Intel developed the Intel® Personal Internet Client Architecture (Intel® PCA), http://www.intel.com/pca/developernetwork/overview/index.htm?iid=ipp_wrlss+body_pca& to allow
Industry to address the new demands of the wireless Internet client market.

Intel PCA decouples the applications subsystem from the communication subsystem through an open physical and logical bus interface, while providing a link to memory subsystem.

This system-level architectural separation between the Applications Subsystem and Communication Subsystem creates a network demarcation, thereby establishing secure areas for the user’s applications and enterprise data; while maintaining network integrity by isolating sensitive network functions such as radio control from unintentional or Byzantine corruption.

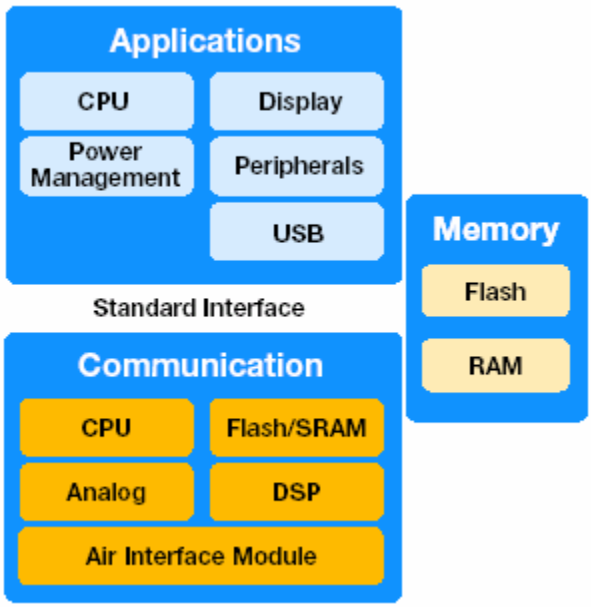


Figure 1. Intel® PCA Platform Subsystems

The Intel PCA provides a platform for the rapid development and deployment of data-enabled wireless devices and next-generation applications and services.
By defining a hardware architecture with common components and open interfaces, and providing a software framework with open interfaces and services, device and application developers can design, scale, and broadly deploy their products with less cost and in shorter time.

The Intel PCA partitions the device configuration of the traditional cellular platform into: an Applications Subsystem, Communication Subsystem, and Memory Subsystem. This partitioning allows application development to evolve independent from communication standards. The Intel PCA provides open programming interfaces and services between physical platform (including communication) and application software, thereby facilitating faster development of the application and abstracting the underlying physical resources. The Intel PCA also supports the security architectures defined in wireless standards specifications such as 3GPP, and TIA. These specifications are moving toward the existing definitions for extensions to the GSM/GPRS SIM model, including definitions for user authentication to handset, user identification, and authentication for the network and cipher key generation.

SUMMARY

Intel believes that industry is producing, and deploying, a wealth of technical solutions to secure the digital assets of users, enterprises, and networks. In particular, solutions like Intel® Personal Internet Client Architecture (Intel® PCA) are addressing the specific security needs of next generation mobile devices.

Appendix C: Mobile Execution Environment (MExE), "Threats Associated with Attacks on the Terminal and UICC/USIM"

3GPP TSG-T2 #17
Vancouver, BC, Canada
13 -17 May 2002

T2-020394

Title: Liaison Statement on MExE Activities
Source: 3GPP-T2
To: SDR Forum

Contact Person:
Name: Lars Brenk
Tel. Number: +45 9631 4658
E-mail Address: LSB@TTPCOM.COM

---

1. Overall Description:

3GPP TSG T2 is glad to provide this contribution to SDR Forum's request for information on the activities in the area of security for software download.

MExE (pronounced “mexy”), which is a subworking group (SWG1) under 3GPP TSG T2, stands for Mobile Execution Environment. It provides a standardized application execution environment for Mobile Terminals. MExE is active in specifying the framework that enables the full promise of ubiquitous, connected, mobile terminals.

To realize this promise, a means was necessary to coordinate and match the efforts of the major application infrastructure elements from mobile terminal manufacturers, network operators, and application and trusted service developers.

For instance, applications developers needed to know the capabilities of their target platforms and networks; network operators required an understanding of the resource demands that new services might require; and all would the need a negotiation process for the discovery, delivery, and execution of downloadable applications and services. And so, in 1997, a work item was begun in ETSI, which has since migrated to become a specification in 3GPP.

The detailed specification “Mobile Execution Environment (MExE); Functional description Stage 2 (Release 4)” is provided in Reference [4].

As security is linked to the success of applications, content, and commerce in the mobile environment, it has received attention within MExE. In order to prevent attack either

from unfriendly sources, or from transferred applications unintentionally damaging the MExE device, a security system is required.

The fundamental elements make up the basis of MExE security, these are:

- application authentication,
- application authorization to a given domain which is a set of permissions linked to authentication authority (root certificate),
- user permissions,
- the management of the whole security system that MExE defines.

The structure of this framework is a matrix of various logical areas or "Domains", entities that have permission to control the download and execution of software in the domains, and a list of actions that are allowed to be performed by software executing in each of these domains.

The domains are currently defined as: MExE Security Operator Domain, MExE Security Manufacturer Domain, MExE Security Third Party Domain, and the MExE Untrusted Area.

The actions which have controlled access include:

- Device core function access includes functions that are an essential part of the phone functionality;
- Support of core software download;
- (U)SIM smart card low level access;
- Network security, property, and services access;
- User private data access;
- MExE security functions access;
- Application access;
- Lifecycle management;
- Terminal data access;
- Peripheral access;
- User interface input output access.

In order to enforce the MExE security framework a MExE device is required to operate an authentication mechanism for verifying downloaded MExE executables. A successful authentication will result in the MExE executable being allowed to run in one of the trusted domains. As the MExE device may want to authenticate content from many sources, a public key based solution is mandatory. Before trusting a MExE executable, the MExE device will check that the MExE executable was signed with a private key for which the MExE device has the corresponding public key. The corresponding public key held in the MExE device must either be a root public key (securely installed in the MExE device, e.g. at the time of manufacture) or a signed public key provided in a certificate, which in turn, must be authenticated by a certificate chain present on the device.
The details of the MExE security framework are documented in Reference 4.

MExE also allows "Core Software Download" which provides a means to update the core device software subsystems, including the software that runs the radio and communication functions. It is thought that a typical usage scenario would be for the user to download and run an installation application that would be responsible for maintaining the integrity of the device during the upgrade. Software such as this requires that the application performing the core update execute in the manufacturer domain.

As part of 3GPP, the MExE security activities are coordinated with other 3GPP security efforts, especially TSG SA WG3 Security.

TSG SA WG3 is responsible for the security of the 3GPP system, performing analyses of potential security threats to the system, considering the new threats introduced by the IP based services and systems and setting the security requirements for the overall 3GPP system.

SDR Forum may further contact TSG SA WG3 for further detailed information on their work in security area. SA WG3 is chaired by Mike Walker (Vodafone).

Summary:
Security is critical to the success of next generation wireless networks. As such MExE and 3GPP have been and will remain vigilant in continuously analyzing threats and risks, and developing requirements and specifications to insure the integrity 3G networks and mobile terminals.

2. Date of Next T2 Meetings:

T2#18	12-16 Aug 2002	Velen, Germany
T2#19	18-22 Nov 2002	Korea

Appendix D: Mobile Virtual Centre of Excellence in Mobile and Personal Communications, "The RMA as Security Architecture"

Project Title:	Mobile VCE Core 2 Programme – Software Dependent Systems
Deliverable Type:	**SDR Forum Input (public)**

Document Number:	MVCE/RHUL/WA1/WP12/sdrf-reg-v05pub
Title:	The RMA as security architecture – MVCE contribution for the SDRF response to the FCCs 'First Report and Order' (FCC01-264)
Work Package:	WP1.2
Nature of Contribution:	External contributory report
Editor:	K. Moessner (SUR)
Authors/contributors:	C. Mitchell (RHUL), K. Moessner (SUR) and members of the WA1 Steering Group

Created:	February 2002
Last Revised:	18/06/2002
Version:	0.5pub

Abstract:	Within this document the Mobile VCE view on security for reconfigurable devices is outlined; in particular an approach to securing the regulation of code modules for use in software-defined radio (SDR) is described.

1 Introduction

The purpose of this short document is to describe the position of the UK Virtual Centre of Excellence in Mobile & Personal Communications ("Mobile VCE"), on some of the regulatory and security issues of Software Defined Radio equipment. The document outlines a possible approach to the secure provision of software defined for use in Software Defined Radio (SDR). The approach is based on the MVCE Reconfiguration Management Architecture (RMA) and within this structure on the use of an appropriate Public Key Infrastructure (PKI) to secure signalling and reconfiguration software exchanges between the parties involved. The format for public key certificates and attribute certificates, as required by the PKI, is not defined, although it could, for example, be based on the use of X.509, [1].

This document is structured as follows.

- Section 2 describes a number of assumptions about the regulatory environment on which the remainder of the document is based. Requirements arising from these assumptions are also listed.
- In Section 3, an overview description of the functionality of the RMA is given and the security system to meet the requirements is specified. Some details of this system remain to be described in detail.
- Section 4 provides an example scenario outlining a number of security threats and the use/applicability of the MVCE radio reconfiguration security system.
- Finally, Section 5 provides some concluding remarks.

2 Background assumptions and requirements

We make the following assumptions about the underlying regulatory structure for the use and application of reconfigurable SDR equipment.

- **Domains and regulatory bodies**. We suppose that the world is divided into an number of administrative *domains*, which may correspond to single nations (e.g. the USA), or groups of nations (e.g. the EU). In some cases, it may also be the case that nations are sub-divided into separate domains. Each domain is assumed to have a single *regulatory body*, responsible for deciding which software is permitted to be downloaded and executed in SDR platforms.
- **Delegated software authorisation**. We further suppose that each regulatory body appoints one or more *delegated authorisation entities* (DAEs), e.g. third parties or vendors, to act on its behalf to verify the adherence of SDR software to rules specified by the regulatory body. The MVCE approach uses these DAEs as complement to the functionality of the AcA servers in the Configuration Control Part of the RMA.

- **Verification checking**. Finally we suppose that, prior to use, software is checked by a *software verifier* (SV) to see that the following rules have been adhered to (the role of the SV is defined in the virtual configuration procedure):

  R1. The software has been approved by a DAE as appropriate for use by this particular SDR platform.

  R2. The DAE that approved the software has been approved by the appropriate regulatory body.

  R3. The software has not been changed since it was approved by the DAE.

The location of the SV responsible for this verification checking is not specified here. However, the RMA foresees the possibility of including this within the SDR platform; alternatively it could be an entity external to the SDR platform, e.g. the AcA-server of the Mobile VCE RMA.

In the next section we show how a PKI solution as a mechanism within the Security Manager entity of the RMA can be used to support requirements **R1** – **R3**.

3 The security structure

We now propose a method for meeting the requirements identified above. This method is based on the use of a PKI and extends the RMA by supporting the interactions between regulatory authorities and the AcAs of the RMA.

3.1 Brief RMA overview

The RMA is designed to support, manage and secure reconfiguration processes in reconfigurable software defined radio equipment [2]. It is structured in a distributed manner, whereby some of the architectural elements are located within the terminal (n.b. these are: a) the Radio Module Part (RMP) which executes the instances of radio software and implements the actual radio and b) the Configuration Management Part (CMP), which manages the reconfiguration processes of the RMP), whilst a controlling element, to influence or even suspend terminal reconfiguration, is located within the network (i.e. the Configuration Control Part (CCP)). The RMA also delivers the algorithms for reconfiguration processes and the internal mechanisms necessary to pursue the reliable reconfiguration of SDR terminals. Internally, the RMA consists of a number of different modules, each implementing a specific task. The modules in the CCP include: 'AcA server', 'reconfiguration software database' and a 'Rules & Policies Tool'. The RMP is seen as processing platform capable of implementing any type of radio, depending on the availability of suitable radio configuration software. Finally the CMP consists of: 'Configuration Manager', 'Reconfiguration Management Controllers', a 'local software repository', a 'configuration rule handler', a 'tag-file handler', a 'configuration software bus' and a 'security manager'.

3.2 Supporting entities

We start this discussion by defining the three main types of security entity required to support the proposed RMA security structure. Those entities in the RMA which require messaging/communication via the air interface (i.e. the AcA in the Configuration Control Part (CCP), and the security manager in the Configuration Management Part (CMP), in the network domain and the reconfigurable terminal, respectively) will require the support of following authorities to be enabled to pursue secure operation of the system.

- **Certification Authorities**: We suppose that there exists one or more Certification Authorities (CAs), which will support the system within a particular domain. Each CA will use its signature private key to create public key certificates for other entities within the system.

  These CAs must be trusted by the entities within the system to behave honestly. The CAs could, for example, be operated by, or on behalf of, the regulatory body. The (root) public keys for these trusted CAs are assumed to be available to all the SVs. They could, for example, be distributed as part of the SV software. Provisions would need to exist for securely updating and, where necessary, revoking these root keys. (N.B. if local regulation permits, the same organisation might operate a CA and an AcA.)

- **Regulatory Body Attribute Authority**: We suppose that the Regulatory Body operates (or has operated on its behalf) an Attribute Authority (AA). This AA will use its signature private key to sign attribute certificates for other entities within the system.

- **DAE Authority**. Each DAE will operate an authority whose task will be to digitally sign code for downloading to SDR platforms. Each piece of signed code will have associated with it a number of pieces of information, including:

– a *code serial number*, unique for the DAE authority, and which can be used to identify the code;

– a series of *code attributes*, indicating the authorised use of the code[17] (each attribute might indicate a type of SDR platform for which the code is intended, together with any usage restrictions applying to this platform);

– *code validity period*, after expiry of which a receiving SV should disregard the code.

3.1 Creation and use of certificates

We divide our discussion of the operation of the security structure into the following subheadings:

- *Initialisation*, covering the tasks that must be performed before the system can operate,

[17] The syntax of such attributes is a topic *for further study*.

- *Code authorisation*, covering the tasks that need to be performed by DAE authorities in authorising the use of code, and
- *Code verification*, covering the tasks performed by an SV when it wishes to decide whether or not a piece of code is authorised for use by a particular SDR platform.

3.3.1 Initialisation

Prior to any use of the system, the following tasks will need to be performed.

- All the supporting entities will need to generate one or more digital signature key pairs.
- The CA public keys will need to be reliably transferred (by some means) to every SV within the domain.
- A public key certificate will need to be generated by (at least) one of the CAs for every supporting entity public key. This will require the reliable transfer of the public key to the CA in such a way that its integrity and origin can be verified by the CA. The CA will then generate a public key certificate and return it to the requesting entity.
- The Regulatory Body AA will need to issue an attribute certificate for each of the authorised DAEs. This attribute certificate will be signed by the Regulatory Body AA's private signature key. The attribute certificate will specify the scope of the DAE's authority for authorising code. For example, the attribute certificate may specify that this particular DAE is permitted to authorise code for a particular specified list of SDR platform types.

3.3.2 Code authorisation

When a DAE is provided with a piece of code for authorisation, the following tasks will need to be performed by the DAE.

- The DAE will need to satisfy itself that the code meets all the rules laid down by the regulatory body for the specified SDR platform(s) for which the code is intended. How this is to be performed it outside the scope of this document. However, the DAE might avail itself of tests performed by the code provider, and/or may perform its own tests and other code verification processes. In any event, prior to starting any testing or verification, the DAE will need to check that the code does genuinely originate from the claimed vendor, and that it has not been modified since leaving the vendor. This might be provided by a variety of possible security measures, including a digital signature on the code by the vendor – however, again this is outside the scope of this document.
- The DAE will then need to assemble all the information that needs to be signed with the code. This will include defining appropriate values for the code serial number, code attributes, and the code validity period.
- The DAE authority will then create a digital signature on the code and accompanying information.

3.3.3 Code verification

We conclude by considering the checks that a receiving SV should perform in order to decide whether or not to permit code to be run on a particular SDR platform.

- The SV will need to obtain a trusted copy of the public key of the Regulatory Body AA for the relevant domain. This can be achieved by obtaining the public key certificate for the Regulatory Body (which might be supplied with the code) and verifying it using a CA root key available to the SV.
- The SV will need to verify that the DAE that approved the software has been approved by the appropriate Regulatory Body (to meet requirement **R2**). This can be achieved by verifying an attribute certificate issued for this DAE by the Regulatory Body AA. The certificate can be verified using the trusted copy of the Regulatory Body AA's public key.
- The SV will need to obtain a trusted copy of the public key of the DAE authority that signed the code. This can be achieved by obtaining the public key certificate for the DAE authority (which might be supplied with the code) and verifying it using a CA root key available to the SV.
- The SV will need to verify the correctness of the code (to meet requirement **R3**). This can be achieved by using the trusted copy of the DAE authority public key to verify the signature on the code.
- The SV will need to verify that the software is appropriate for use by this particular SDR platform, and it has been approved by the DAE for this platform (to meet requirement **R1**). This can be achieved by examining the code attributes and code validity period. It may also be necessary to consider the detailed contents of the attribute certificate for the DAE, to ensure that this DAE is entitled to authorise code for this particular SDR platform.

4 An operational scenario

There are many different cases in which the need for terminal reconfiguration may arise and, even though there are only a restricted number of reconfiguration classes (i.e. partial layer-, layer- and complete reconfiguration) there are many unaccounted possible threads to reconfiguration and system security. These are threads of varying severity, depending on the degree of the attempted reconfiguration. Considering the potential that a reconfiguration may set a terminal into a state outside the regulatory boundaries requires means capable to ensure that a permitted degree of reconfiguration becomes not exceeded. The Mobile VCE RMA and its here presented security mechanism mainly aim to secure configurations of and reconfigurations in software reconfigurable communications equipment. We illustrate the threads and mechanism by the example of a cellular communication environment.

OTA download and installation of software updates/patches

A situation where a manufacturer may be required to update the system software of terminals already shipped to the end user may arise. Our scenario considers this very

case, an outline of the procedure and describes how the RMA security manager implements the here presented security mechanism. The procedure consists of various steps starting with the manufacturer to seek approval from the DEA to perform the installation of a particular software patch, that may be applicable for a (or many) of the manufacturers reconfigurable radio platforms. Providing the DEAs approval and upon agreement with the network operator, the manufacturer may undertake the software upgrade/patch download and terminal reconfiguration. Thereby it will be independent which part of a SDR terminal is to be reconfigured, whether its lower layers, the protocol stack, application execution platform or the application itself, a download and reconfiguration process has in any of the three reconfiguration classes to comply to a consistent sequence that ensures the reliability trustworthiness and security of the intended configuration. Any reconfiguration algorithm that serves and provides these basic requirements needs to contain a sequence that ensures approval by a recognised authority (i.e. the DAE). This includes a number of approval and security enforcement elements, which perform the following sequences: 'request-for-reconfiguration-validation', 'validation-of-remote-requests', 'feasibility-of-request', 'reliable-software-availability', 'software-version-compliance', 'configuration-interface-compliance' and 'reconfiguration-procedure-abort'.

Every single request for software download and reconfiguration has to pass through an authentication and security procedure. Only if the request for reconfiguration is identified as being authentic, and once it is ensured that the request was issued by either a trusted application or was sent from a trusted and authorised network entity, the reconfiguration sequence may proceed; otherwise the process has to be prematurely abandoned and the terminal has to remain in its initial configuration.

Once the validity/originality of the reconfiguration request is established, i.e. the terminal has recognised the DAE as being authorised to request a reconfiguration of the specified reconfiguration class, the terminal will request the rules for the anticipated ‘new’ configuration and evaluates whether the terminal capabilities suffice the specifications of the new software module (e.g. crosschecks memory size, display and processing capabilities with the requirements of the software) and will initialise the actual reconfiguration process.

For this latter process, the terminal uses information obtained from the database (within the network part) to verify the availability of sufficient system resources and suitable terminal capabilities to perform the intended reconfiguration and to validate its usefulness and final conformance to transmission standards (i.e. the standard compliance after reconfiguration). Terminal capabilities may be expressed as sets of parameters or as MExE classmarks [3], using these classmarks as nominators may simplify the determination of terminal capabilities and also matches the standards framework for future and software defined radios [4]. If either the system resources are not sufficient for a reconfiguration or the terminal capabilities do not match the necessary requirements, the reconfiguration procedure becomes prematurely terminated.

Once the feasibility of a requested reconfiguration has been established, the configuration manager (within the CMP of the RMA) requests the download of the software update/patch. In case a patch consists of multiple entities, additional download sequences need to be performed until all requested software entities are available (i.e. already

downloaded). Should this approval fail for one of the required software entities, another download process may ensure that the needed software version/entity becomes available. The reconfiguration process may proceed, only if all software entities in their 'required' versions are locally available.

The here described 'authentication'-, 'reconfiguration rule and type approval'- and 'software availability'- sequences require reliable authentication mechanisms for the reconfiguration process. Exchange of information between reconfiguration manager and network requires secure signalling channels. Reconfiguration message exchange across the wireless access are imperilled and make the reconfiguration management system particularly vulnerable to third party interaction and misuse of the reconfigurability of reconfigurable terminals and network nodes.

Once authenticity and availability of all required and downloaded software entities are ensured, the reconfiguration manager produces a description (i.e. a configuration-tag-file (e.g. as xml script)) of the future configuration. This tag-file includes and describes the terminal configuration in detail and also the local and remote reference and resource locators from which the single software entities were obtained. Relying on the details described within this tag-file and delivered to the network, the AcA server performs a 'virtual' reconfiguration that ensures the interworking between the software blocks. If this 'virtual' reconfiguration has confirmed the compliance of their interfaces with the defined SDR APIs and the system compliance to given radio standards, the reconfiguration manager can proceed with the reconfiguration and instate the new configuration (i.e. the AcA grants or declines the permission to complete the reconfiguration, dependent on the outcome of the virtual configuration process) .

In case the virtual configuration fails, the old configuration remains active and an error message is dispatched to the requester of the reconfiguration/software update. Depending on the response to the error message, the reconfiguration process may be cancelled or another attempt may be initiated, however considering the problems that occurred, during the previous reconfiguration attempt. Any failure of a reconfiguration needs to be published/forwarded in a message that clearly identifies/ documents the reason and nature of the failure.

The RMA delivers the architectural framework to undertake SDR terminal reconfiguration, whereby the here proposed method based on a PKI delivers a mechanism to ensure authentication, authorisation and secure software download for reliable reconfiguration procedures for SDR equipment.

5 Concluding remarks

We conclude the document by observing ways in which the scheme described can be extended and/or modified. There is clearly considerable scope for further work in this area. There is also the possibility that this work could also be applied to other similar scenarios where regulation of mobile code is required. One example might be the automotive industry.

As described above, the proposed solution is restricted to methods for SDR software regulation **within a single domain**. One way in which the existing proposal could be

extended would be to consider a possible international domain which can also approve software, and whose authorisations may automatically be accepted within all domains (or perhaps only those domains agreeing to such an international domain).

One problem with the 'per domain' approach is that the SV may not know in which domain it currently resides, and hence will not know which regulatory body is relevant. This is most likely to be a problem if the SV is built into the SDR platform. If, however, the Mobile VCE RMA is used, the AcA-server should not suffer from this problem.

It is important to note that the regulatory code verification described above may not be the only verification performed by an SV. For example, the SDR platform owner may have its own requirements about which types of code it will permit to execute within its platforms. Also, issues relating to *Digital Rights Management* (DRM) may arise, i.e. where the SV restricts use of code modules to enforce payment for these modules.

References

[1] ITU-T X.509 (03/00) [=ISO/IEC 9594-8: 2001]. *Information technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks*.

[2] Moessner K, Gultchev S, Tafazolli R, "Managing Reconfiguration in Software Defined Communication Systems", ISCTA, Ambleside, Lake District, United Kingdom, 15-19 July 2001.

[3] "Digital cellular telecommunications system (phase 2+): Mobile Station Application Execution Environment (MExE), ETSI TS 101 438 V7.0.0, 1999.

[4] Ralston J, "SDR Framework to Enhance MExE", presentation at the SDR Forum General Meeting, Seattle, WA, 19-21 June 2000.

Appendix E: Motorola, "SDR Security Threats and Requirements"

SDR Security Threats and Requirements

June 27, 2002

Motorola Inc.
Ken Riordan
Ezzy Dabbish
Larry Puhl

Contents

1. Introduction

The continued emergence of Software Defined Radio (SDR) technologies, products and services, will heighten the need for effective security in commercial wireless systems. It is essential that products built with SDR technologies incorporate robust security methods to ensure that such technologies do not compromise the safety, stability, and interference controls of the global telecommunication systems. Security is ultimately the responsibility of equipment manufacturers. They must ensure that their products are reliable and appropriately tamper-proof. Both equipment manufacturers, and network operators, have tremendous incentive to ensure a high level of security in their products and networks, in order to guarantee a smooth and uninterrupted delivery of services to their customers.

The controlled environments in which commercial base stations operate provide greater inherent security, in comparison to commercial handsets. Programming of software into a base station requires physical access to either the base site itself, or to the Operation and Maintenance Center (OMC) which remotely manages cell sites within the network. Network operators employ robust alarm and security measures to prevent unauthorized physical access to these facilities. The data links which connect the OMC to the cell sites are private data networks controlled by the network operators, and offer no entry point for remote hackers. Furthermore, there is no internet or other publicly accessible external data connection into the OMC. The inherent security of base station equipment is demonstrated by the fact that second generation (2G) commercial base stations are remotely programmable, and have been operating in high volume for over ten years without any significant security issues. The focus of this report, therefore, will be on security issues surrounding commercial handsets.

Security requirements can be divided into the following five general categories:
Trusted System Operation: confidence that software will execute in the device exactly as intended.

Authentication: the ability to validate the origin of received information. For example, an SDR device should be able to ensure that the downloaded software originates from a trusted server, prior to installation. The SDR device should install only authenticated software.

Integrity: verification that received information has not been modified or corrupted in transit. Prior to accepting and installing new software, an SDR device should be able to ascertain that, since originating from the trusted server, the downloaded data has not been modified. The SDR unit should only install software that has been checked for its integrity.

Privacy: often times refer to as “confidentiality” this category usually refers to the assurance that other parties cannot access a user's personal information. In the case of

SDR, however, privacy can apply not only to user data, but also to the executable software, which is the intellectual property of the equipment manufacturer. Encryption techniques may be used to prevent unauthorized parties from gaining access to private user data, or to proprietary software.

Non-repudiation: positive verification of a sender or receiver's participation in a transaction.

Realization of the first requirement, "Trusted System Operation", is achieved primarily through product design and development. It requires a methodical architecting of the microprocessor systems within the device, coupled with a quality-oriented software development process. To expand on this concept, it is instructive to consider the quality assurance processes that are currently employed by equipment manufacturers, and then to consider how the emergence of SDR technologies will affect these processes. For current base station, and handheld products, it is typical for a single generation of hardware to be coupled with multiple evolutionary releases of software. Equipment manufacturers ensure the quality of each new hardware-software combination through a combined strategy of design, verification, and configuration control. Ultimately, manufacturers are confident that products delivered to the market place will meet all quality requirements, including those pertaining to emissions and safety. This confidence is the same, whether the software is loaded in the factory, or in the field.

With the emergence of SDR technologies, it will become increasingly common for the software to be loaded in the field (note that this is the norm for current generation cellular base stations). However, there need be no compromise to any of the aforementioned quality assurance steps: design, verification, and configuration control. Ensuring that only authenticated, quality software is downloaded into devices requires the effective application of the security principles discussed throughout this report.

The last four categories (i.e., authentication, integrity, privacy, and non-repudiation) require a robust security system framework, such as Public-Key Cryptography (PKC). PKC technologies are well established in other communication industries, and are well suited to address the security issues surrounding SDR. PKC, as it is currently applied to the Internet, has successfully secured billions of dollars of Internet commerce, and can be effectively adapted to address the challenge of securing re-programmable wireless products and systems.

In the remaining sections of this report, the security requirements for SDR are explored in more detail, beginning with a brief overview of PKC. The report also includes highlights of the security activity within the wireless industry, and an outline of SDR security objectives and design methodology. Finally, the report will discuss SDR security threats, possible attacks, and the security framework requirements to defend against such attacks.

By the end of this document, the following key points will be made:

- Private industry (manufacturers and operators) has tremendous financial incentive to ensure that their products and networks are secure.

- The wireless industry is fully engaged on the subject of security.
- The wireless security challenges (threat scenarios and solutions) are well understood.
- Internet security technologies (e.g., PKC) are well suited to address the wireless security challenge.
- Regulatory mandate of specific security methods would be counterproductive. To do so would provide a blue print for the malicious hacker, and would impede the industry's responsiveness to an ever-changing security landscape. Alternatively, specifying security performance (as discussed in later sections) may be appropriate.

2. Abbreviations

2G	Second Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AHAG	Ad Hoc Authentication Group
ANSI	American National Standards Institute
ASIC	Application Specific Integrated Circuit
CDMA	Code Division Multiple Access
ECC	Elliptic Curve Public Key System
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
GSMA	Global System for Mobile communications Association
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
LAN	Local Area Network
MExE	Mobile Execution Environment
MWIF	Mobile Wireless Internet Forum
PKC	Public Key Cryptography
RSA	Rivest-Shamir-Adleman Public Key Cryptographic System
SAGE	Secure Algorithms Group of Experts
SDR	Software Defined Radio
SHA-1	Secure Hash Algorithm
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WTLS	Wireless Transport Layer Security

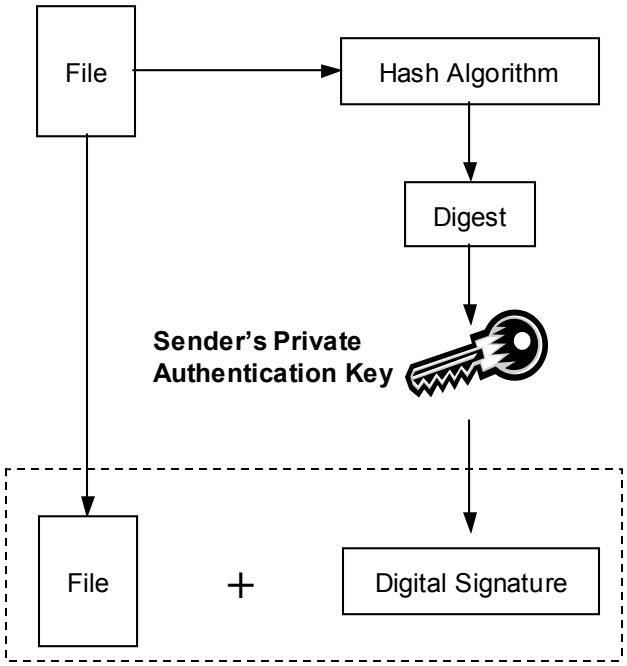
3. Public-Key Cryptography System Overview

The principles of Public-Key Cryptography (PKC), which is widely adopted within the Internet world, will not be addressed in detail in this report. Treatment of this subject is available in numerous sources. As an overview, the following sections briefly review the topic of PKC.

3.1 Digital Signature Generation

Digital signatures are an electronic replacement for handwritten signatures. Public-key encryption technology has made electronic signatures practical because a trusted party does not have to be involved in the actual "signing". Any party can generate public/private key pairs that can be used to sign documents.

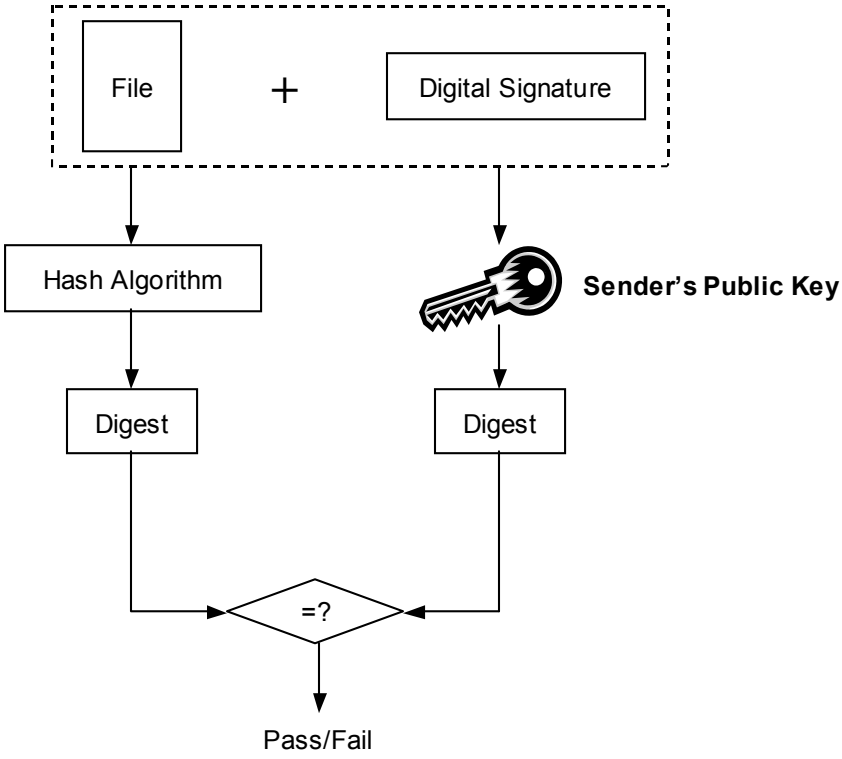
In 0, shown below, the sender uses his private authentication key to sign a file. First, a message digest of the file is generated using a secure hash function, such as SHA-1. Next, the digest is signed using the sender's private authentication key. The result of this operation is a digital signature that anyone can verify using the sender's public key.



Digital Signature Generation

3.2 Digital Signature Verification

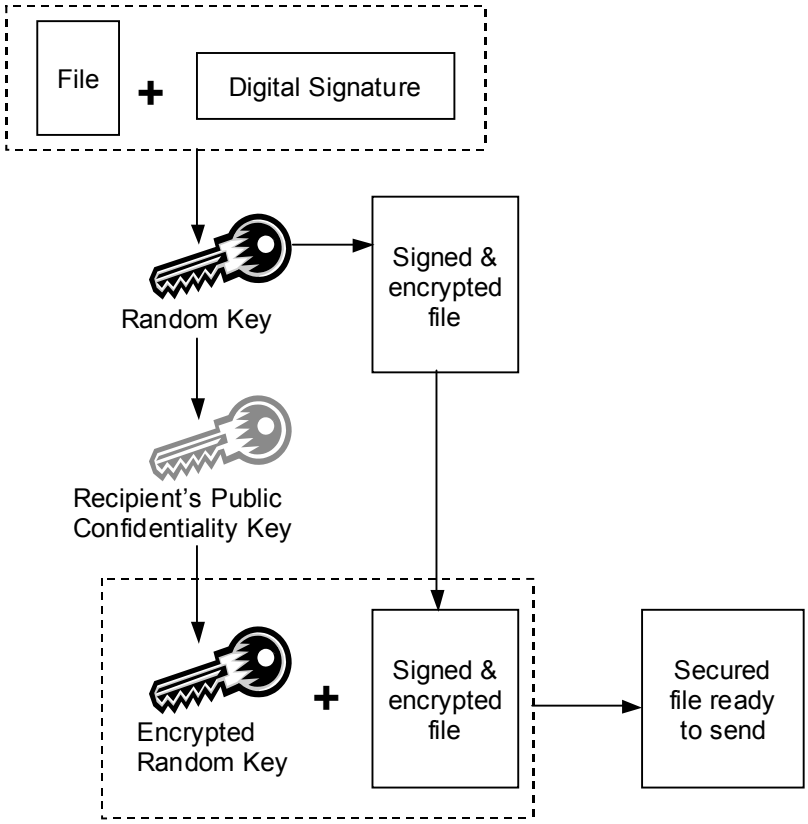
In order to verify that a file has not been modified since it was created and signed, the recipient invokes a digital signature verification process, as shown in 0. The signer's (i.e., the sender's) public key is applied to the received digital signature resulting in a message digest. At the same time, the received file is hashed to obtain a received file message digest. If the two message digests are the same, then the sender confirms that the sent data has not been modified in-transit. This process could be used to establish the integrity and authenticity of software downloaded to an SDR device.



Digital Signature Verification

3.3 Encryption

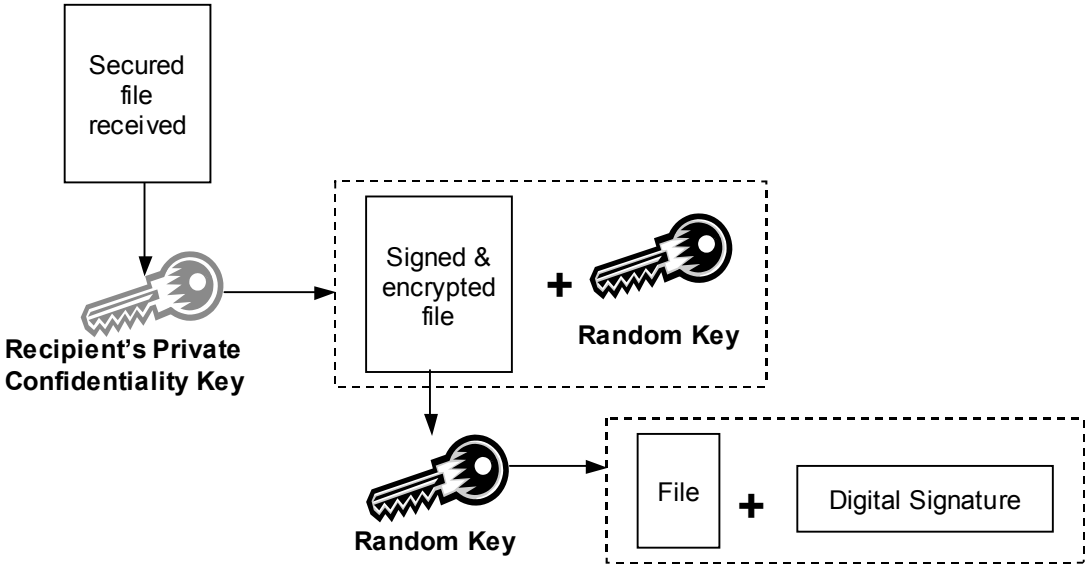
Sometimes, in addition to a digital signature, a file also needs to be encrypted. The procedure shown in 0 shows how to securely encrypt and transmit a file with a digital signature. First, a random key, or a session key, is generated. This key is used in conjunction with a symmetric encryption algorithm to encrypt the file and digital signature, thus creating a signed and encrypted file. Next, the random key itself is encrypted using the recipient's public confidentiality key. The encrypted random key is then combined with the signed and encrypted file to form a secured file that is transmitted to the recipient.



Encryption

3.4 Decryption

During the decryption process, the original text or data file is recovered. The random key that was used to encrypt the original file has been encrypted using the recipient's public confidentiality key, as was show in 0. Thus, only the holder of the corresponding private confidentiality key will be able to decrypt and access the random key. The complete decryption process is shown in 0. The recipient's private confidentiality key is used to restore the random key. The random key is then used with the symmetric decryption algorithm to decrypt the signed and encrypted file resulting in the original file plus the digital signature. (Following decryption, the digital signature of the file can be verified as was described in section 0.)



Decryption

4. Authentication

Authentication refers to the ability to validate the origin of received information. For example, prior to installing new software an SDR device should be able to verify that downloaded data originates from a trusted server. The SDR device should install only authenticated software.

Public-key cryptography can provide a full solution to the authentication problem. As was described in section 3.1 and 0, secure methods to generate and verify digital signatures are available. These basic methods can be combined to create a secure Public-Key Infrastructure (PKI) and establish trust in an SDR system. For example, the manufacturer could have private and public authentication keys. The public key would be stored in each of the manufacturer's radios as a root key and the private key would be used to sign software downloads to those radios. Prior to installing any software, the radio would use the root key to verify the digital signature of the software. Since only the manufacturer possesses the private key, only the manufacturer could have created the digital signature, thus the authenticity of software can be proven. The manufacturer could also delegate trust to other third-party entities using certificates. In this case, the public key of a third party could be put into a certificate that is signed by the manufacturer. Software could then be signed by the third-party. The radio would then check the signature of the software using the third-parties public key. Then, the radio would verify the authenticity of this public key by checking the signature of the third-party's public-key certificate using the manufacturer's root key. Many other extensions to this basic premise are also possible.

5. PKC Advantages to SDR

Public-Key Cryptographic Systems have been around for a long time (since 1976) and are well suited to address the security issues surrounding SDR. One advantage of a PKC approach is that the manufacturer would not be required to install a unique shared key into every SDR device. Instead, the manufacturer stores a root key in every SDR device that is used to verify the digital signature of the software downloads. Thus, the key management problem has been eliminated. Also, a root key stored in a PKC-based approach does not need to be kept secret. Its integrity must be ensured, but this is an easier requirement than maintaining a secret key. For example, the root key could be stored in an unalterable memory of the SDR terminal, such as Read Only Memory. Also, a PKC approach allows for signatures to be generated that can be verified by a multiplicity of units, each containing the root key. Thus broadcasting of signed downloads to multiple SDR radios is possible. Finally, a PKC approach can also support a hierarchical infrastructure, which makes distribution of trust, revocation, and the inclusion of third-party developers much easier and more secure than with the sharing of secret keys. Internet security technologies, such as PKI, have successfully secured billions of dollars of Internet commerce and are more than up to the challenge for securing wireless systems.

6. Survey of Wireless Security Activities

Starting in the late 80's, the Telecommunications Industry Association (TIA), responsible for establishing cellular systems standards in the United States and Canada, created the TR-45.3 Ad Hoc Authentication Group (AHAG). This group developed the authentication protocols and algorithms that are used in the second-generation (2G) ANSI-41-based cellular systems. They also developed algorithms to protect the privacy of voice and later data communications for these digital cellular systems. This work is continuing in the Third Generation Partnership Project 2 (3GPP2). The security group here has been given the title 3GPP2 TSG SA WG4. They will now extend the AHAG work to include mutual authentication (between the subscriber and the network), integrity protection and security in the packet switched domain.

Similarly, in Europe, the European Telecommunications Standards Institute (ETSI) had created a security group within the GSM standards effort called SMG10. In conjunction with the Secure Algorithms Group of Experts (SAGE) and the GSM Association Security Group, they developed protocols and algorithms to secure the GSM cellular system. This work is continuing in the Third Generation Partnership Project (3GPP) within the security group 3GPP TSG SA WG3. Current projects include TS 33.203 Access Security for IP-based services and TS 33.210•Network Domain Security - IP network layer security.

With respect to mobile execution environments on wireless devices, (including the Wireless Application Protocol (WAP), Personal Java (PJava) and Java 2 Micro Edition (J2ME)), 3GPP TSG T WG2 (Terminal capabilities) created SWG1 (MExE). The MExE group developed a security framework that includes a manufacturer domain, an operator domain and trusted third-party domains. There is a current movement to possibly fine-tune these domains. The Java development community has adopted the MExE security model as the basis for the security aspects of JSR 118 Mobile Information Device (MIDP) Profile 2.0. MIDP 2.0 is the part of the next generation of the J2ME standard.

With the emergence of m-commerce, ETSI is in the process of developing Mobile Electronic Signature Standards.

The WAP Forum Security Group has been developing standards for the security layer protocol in the WAP architecture called Wireless Transport Layer Security (WTLS). They are now working with the Internet Engineering Task Force (IETF) in order to make their Transport Layer Security (TLS)-related RFC's mobile friendly.

Other on-going mobile security work is being carried out within the Bluetooth Special Interest Group, the International Telecommunication Union (ITU), the Mobile Wireless Internet Forum (MWIF) and the World Wide Web Consortium (W3C).

These activities demonstrate the high degree to which the wireless industry is engaged on the subject of security. The industry is constantly reviewing, enhancing, developing, and applying new security technologies to ensure the protection of wireless subscriber devices and the wireless infrastructure networks.

7. SDR Security Objectives

A fundamental principle for designing a secure handset is the assumption that all design information is available to the attacker. It should be assumed that the only information that is not available to the attacker is the private encryption keys that are securely kept by the equipment manufacturer or a trusted Public-Key Infrastructure (PKI) service provider. By basing the security on private keys that can be securely stored, a handset can be designed that is secure against a sophisticated array of attacks, without adding significant cost to the device. Private keys will be either Rivest-Shamir-Adleman (RSA) or elliptic-curve keys. In RSA and elliptic-curve cryptographic systems, each private key has a corresponding public key. Public keys are stored inside the handset. It is assumed that the attacker knows the public keys. The mathematics of RSA and elliptic-curve cryptography makes it infeasible for attackers to determine the private key from the public key and/or encrypted data.

One important consideration when designing a secure handset is the likelihood that an attack method, developed by a sophisticated hacker, will be made available to a large number of users, possibly via the Internet. For example, a method to increase transmitter output power could become widely distributed as a PC program that accesses a handset through its test port. The handset design should prevent attacks that could easily be implemented by a large number of users. This makes securing the test port, keypad entry, and SIM interface, essential.

It is reasonable to expect that equipment manufacturers will use security methods, which are compatible with existing wireless standards such as the Wireless Application Protocol (WAP) and Mobile Execution Environment (MExE). These standards use RSA and elliptic-curve cryptography as the bases for their security mechanism. By using these standards as the foundation for security, the cost impact of security can be minimized.

Preventing widespread attacks requires the storing of a public key in the handset, so that downloaded software can be verified. Verification assures that the software was properly signed and has not been modified. A typical implementation will use the Secure Hash Algorithm (SHA-1) hash function and RSA cryptography. The SHA-1 hash function is used to map a large software data file to a 160-bit data block. RSA public-key cryptography is then used to verify that the 160-bit data block corresponds to the large downloaded data file. By using a small RSA exponent, the verification can be implemented in software and can take less than a fraction of a second on a typical handset. The verification keys, and associated software, should, ideally, be implemented in ROM, so that an attacker cannot modify them.

Effective design for security begins with a well-articulated set of requirements. It is necessary, therefore, to define detailed requirement, expressed in the form of security threat scenarios. The following section establishes model for the description of security threats to SDR enabled handsets, and provides a number of illustrative examples.

8. SDR Security Threats

For commercial wireless handsets, employing SDR technologies, security threats can be described using a three-part model, as illustrated in the following figure, and explained in the following text.

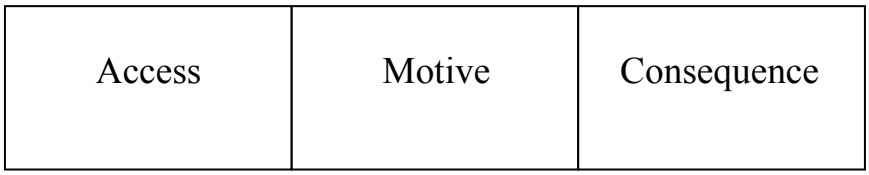


Figure: Three-part Security Threat Model

Access: refers to the means by which the perpetrator obtains access to the device.

- **Physical**: the threat requires physical control of the device.
- **Remote**: the threat can be perpetrated remotely, using the wireless connectivity of the network.

Motive: refers to the motivation of the party responsible for the threatening action.

- **Negligent**: accidentally harmful consequences of a legitimate action. (e.g. the download of authenticated software which contains an unintentional software "bug")
- **Unauthorized**: unintentionally harmful consequence of an improper or unauthorized action. (e.g. download of unauthorized black market software which is advertised to "boost" handset performance)
- **Malicious**: deliberate, improper action, specifically intended to cause harmful consequences.

Consequence: refers to the nature of the harmful consequence resulting from the threatening action.

- **Denial of Service (DoS)**: widespread impairment of the Quality of Service (QoS) for users of the network, on which, the attack was perpetrated.
- **Interference with other Services**: widespread performance impairment of, or improper access to, other networks or services.
- **Digital Rights Violation**: Unauthorized access to, or theft of, digital content and software.

The access means, motivation, and consequence are effectively independent variables in the description of a security threat. There are, therefore, 2 x 3 x 3 = 18 unique categories of threats. For each of these categories, there are many variations and permutations, resulting in a boundless array of unique threat scenarios. It is, however, sufficient to focus on the simple three-part security threat model when considering the necessary security counter-measures (as discussed in later sections). The following table contains several example security threats, and also illustrates how the three-part model can be used to classify a given threat.

	Example Threat Scenario	Access	Motive	Consequence
1	A sophisticated hacker creates and distributes a virus or malicious application that causes widespread interference **to other communication systems**, such as public safety, emergency, and navigation control communication systems.	remote	malicious	interference
2	A sophisticated hacker creates and distributes a virus or malicious application that corrupts the operation of SDR terminals or infrastructure components in a manner which causes widespread disruption of service **to the effected communication system**.	remote	malicious	DoS
3	A black market company creates and distributes a rogue application which causes an SDR terminal to deviate from its normal performance limits, and in so doing, causes widespread disruption of service to the effected communication system. (As an example: an application that causes the terminal transmitter to always transmit at maximum power, ostensibly allowing the user to get better performance, yet actually degrading the overall performance of the system).	remote	unauthorized	DoS
4	An unethical company takes in old model phones, illegally reprograms and resells the devices as "new" on the black market. The hardware/software combination of the modified phones is unreliable, and causes the devices to eventually "crash" (i.e. suffer an unrecoverable failure)	physical	unauthorized	DoS
5	A new release of software inadvertently contains a "bug" and is distributed to users in the network. The bug causes terminals to reset unexpectedly, causing widespread denial of service.	remote	negligent	DoS
6	An unethical company intercepts software downloaded to phones operating in the network, and illegally re-uses the software to build and sell black market devices.	remote	malicious	digital rights
7	An unethical company modifies the electronic identifier information on phones intended for sale in one country, and profitably resells the phones in another country where the sale is not legal. (As an example: low cost phones with reduced spectral emission specifications may be legal in one country, but illegal in another country).	physical	unauthorized	interference
8	Disreputable parties modify device software, causing them to transmit and/or receive on different frequencies, thus enabling covert communications or eavesdropping.	physical	malicious	interference

A wireless handset, employing SDR technologies, should be protected against the threats described above. Achieving robust security must be accomplished through a combination of inherent limitations in the programmability of the unit (as discussed in section 8), and the addition of specific security features (such as those discussed in section 9).

9. Hardware Capabilities and Security

To properly assess the security risks associated with re-programmable devices, it is necessary to consider the inherent hardware limitations of those devices. The notion of a "Software Defined Radio" as a device capable of near limitless flexibility is unfounded. This is particularly true for the commercial wireless handset market, where the public demand for small, lightweight, low cost, battery efficient products, is a paramount consideration for equipment manufacturers.

Manufacturers have, and will continue to, design products that operate with very specific and limited radio parameters (e.g. modulation, frequency, output power). It is true that with the emergence of new communications systems (e.g. wireless LAN) that the market will demand devices with increasing degrees of multi-band and multi-mode functionality. This demand will drive equipment manufacturers to seek out the most optimal implementation technologies (like SDR) to address the product requirements. Even in these cases, however, the capabilities of these multi-mode devices will be essentially limited to the specific set of wireless services that were considered at the time of product design.

In section 8 of this report, three categories of security threat "consequences" were defined: DoS, Interference, and Digital Rights. Inherent hardware limitations of commercial wireless handsets are most significant with regard to the first two categories, with the greatest relevance applying to Interference. Both DoS and Interference include possible scenarios involving handsets that operate outside of the normal operating limits of frequency, modulation, and output power. The remainder of this section will briefly discuss the current state, and the emerging trend, of radio technology, as it relates to these three radio parameters. The purpose of this discussion is to illustrate the inherent hardware limitations, and therefore, the intrinsic security, expected to be found in current and next generation handsets.

Advances in semiconductor technologies have enabled transmitter and receiver architectures to have fewer Intermediate Frequency (IF) stages, and less signal processing/filtering achieved in hardware circuitry. Nevertheless, current and future generation equipment must still depend on electromechanical devices such as RF filters and resonators. Demanding product size and cost constraints dictate that these hardware elements be properly (meaning "not overly") specified. Consequently, it is unreasonable to expect (current or future generation) handsets to have the inherent hardware ability to operate significantly outside of the frequency bands, in which, they were designed to operate. To qualify this last statement, it should be noted that design and manufacturing tolerances in filters and resonators will result in small degrees of hardware extensibility, beyond the specified limits. Securing this extensibility, therefore, falls to the responsibility of the security framework described in the following section.

With the continuing trend towards sophisticated modulation protocols, it is increasingly common for modem functionality to be implemented digitally. It should be noted that "digitally" does not imply a software implementation. Extremely complex modem algorithms, such as those found in CDMA-based systems, are typically implemented in

digital ASICs. Nevertheless, advances in microprocessor technologies will enable the trend towards software programmable modulators and demodulators. Therefore, of the three RF parameters (frequency, modulation, and output power), modulation will typically have the greatest degree of SW flexibility found in current and future generation radio architectures. However, an improper change to only the modulation format has limited potential to produce harmful consequences. This potential is primarily limited to Denial of Service (DoS) scenarios, where individual units are rendered inoperative due to an improper change in modulation format. Providing security against such scenarios, therefore, falls to the responsibility of the security framework described in the following section.

Much like frequency, output power is limited by inherent electrical and mechanical limitations of the hardware design. Power amplifier circuitry is optimally designed to produce the rated maximum output power, with minimal headroom. What margin does exist is the result of typical design and production tolerances. Of the three RF parameter (frequency, modulation, and output power), output power is the least likely to be impacted by the emergence of SDR technologies. Realistic security threats involving output power are mostly confined to scenarios whereby a handset operates at its rated maximum, when it should be operating at a power reduced state. Providing security against such scenarios, therefore, falls to the responsibility of the security framework described in the following section.

10. SDR Security Framework Requirements

The following security framework specifies the general methods and elements required to ensure robust security for SDR enabled devices. These methods are intended to enhance and strengthen the intrinsic security (by virtue of hardware limitations) as discussed in section 9. If properly implemented, this framework will provide effective counter-measures to the security threats discussed in section 8. The choice of the specific algorithms used for implementation should be left to the device manufacturer. By allowing manufacturers to select the implementation techniques, the commercial wireless industry's responsiveness to an ever-changing security landscape can be ensured.

1. The equipment SHOULD include a unique non-alterable identifier (Serial Number). This enables certificates to be linked securely to the device.
2. A secure configuration control method MUST be used. This prevents a hacker from changing the device configuration.
3. Private cryptographic keys MUST be stored securely. This allows the equipment to securely identify itself.
4. Public cryptographic keys (root keys) used to verify certificates MUST be stored so that the value cannot be modified.
5. A secure infrastructure MUST be provided to verify the integrity of software to control distribution of the software.
6. All software components MUST be cryptographically verified before they are executed. At minimum this should be done at start-up.
7. Watchdog processes MUST be used to insure that processors are executing instructions correctly and that software routines are not locked up.
8. Task separation methodology SHOULD be provided to insure that a non-critical task couldn't access memory or modify operation of a critical task.
9. The cryptographic level of the algorithms used SHOULD be consistent with the current state of the art and designed to prevent a dedicated attacker from using weaknesses in the algorithms to modify the specified operation of the equipment.

Each of these framework requirements address several of the threats listed in the previous section. Good security design requires that all of these framework requirements be included in order to ensure a secure design. This is a list of "best practices" as established by security experts.

Note that several of these framework requirements require a Public Key Infrastructure (PKI). A PKI is needed to sign the software and configuration parameters for SDR enabled devices. A PKI is needed to create and revocate the digital certificates used to certify compliance.

11. Conclusion

Security is an important issue facing the commercial wireless industry. The clear sense of that importance is shared between the industry, regulators, as well as other users of the precious resource: radio spectrum. With the continued emergence of SDR technologies, the need for effective and robust security measures is increasingly heightened. The commercial wireless industry clearly recognizes this need, and is fully mobilized in its efforts to identify and thwart security threats through a comprehensive application of security principles. (Section 6 of this report gives a number of examples of this effort.)

The commercial wireless industry will continue to employ an open standards approach to the specification of security protocols, thus ensuring multi-vendor interoperability.
Equipment manufacturers and network operators share a tremendous incentive to ensure that their products and networks operate safely and reliably. This incentive is based not only on the obvious financial motivations which accompany participation in such a dynamic and competitive marketplace, but also the sense of responsibility which accompanies the provision of essential communication products and networks to our communities.

The security challenge facing the commercial wireless industry is well understood. That challenge is, in many ways, a natural extension of the security challenge facing wired communication systems, and the public Internet. For this reason, Public Key Cryptography (PKC) technologies are ideally suited as the basis for an effective defense against wireless, and SDR security threats. Section 8 of this report provides a simple model for understanding the security challenge, and also provides a number of practical examples.

An important element of understanding security threats and counter-measures, is to consider the inherent capability and limitations of device hardware. Commercial handsets, in particular, will continue to be designed with very specific and limited capabilities in terms of frequency, modulation, and output power. These intrinsic limitations, coupled with the security framework discussed throughout this report, will provide the foundation for robust security performance.

Finally, it should be stressed that the very nature of the security challenge is that the "threat" is ever changing. Malicious hackers make it their business to try and decode the security systems designed to thwart their unscrupulous efforts. Therefore, regulatory mandate of specific security methods would be counterproductive. To do so would provide a blue print for the malicious hacker, and would impede the industry's responsiveness to an ever-changing security landscape.

Appendix F: Overview of the SDR Forum Series of Documents on Software Download for RF Reconfiguration

Appendix F: Overview of the SDR Forum Series of Documents on Software Download for RF Reconfiguration

Document DL-DFN provides a complete high-level perspective on the scope of radio software download in the context of SDR handheld and mobile devices and base stations with reference to application, requirements, methods and implementations. The document presents a list of considerations relevant to the later development of detailed requirements for radio software download. The SDR Forum Download Working Group developed this document with input from the Terminal and Network Architecture Working Group.

Document DL-DFN is the first in a series of SDR Forum documents on radio software download. The other documents in this series are:

- DL-TIM: Timelines for Software Download for RF Configuration
- DL-REQ: Requirements for Software Download for RF Configuration
- DL-GLO: Report on Global Radio Technology Development Organization Perspectives on Software Download for RF Reconfiguration
- DL-REG: Regulatory Report on Global Regulatory Views on SDR and Software Download for RF Reconfiguration
- DL-SIN: Software Download for RF Reconfiguration Security and Integrity
- DL-SOL: Specifications of Common Solutions for Software Download for RF Reconfiguration

The relationship of these documents is seen in Figure E-1. DL-DFN is the overarching document that provides a foundation for the remaining documents and drives the development of the other documents. Documents DL-TIM, Dl-REQ, DL-GLO, and DL-REG are parallel documents that provide the basis for further work in DL-SIN and DL-SOL. It is these latter two documents that are the ultimate goals of this series of SDR Forum documents on software download.

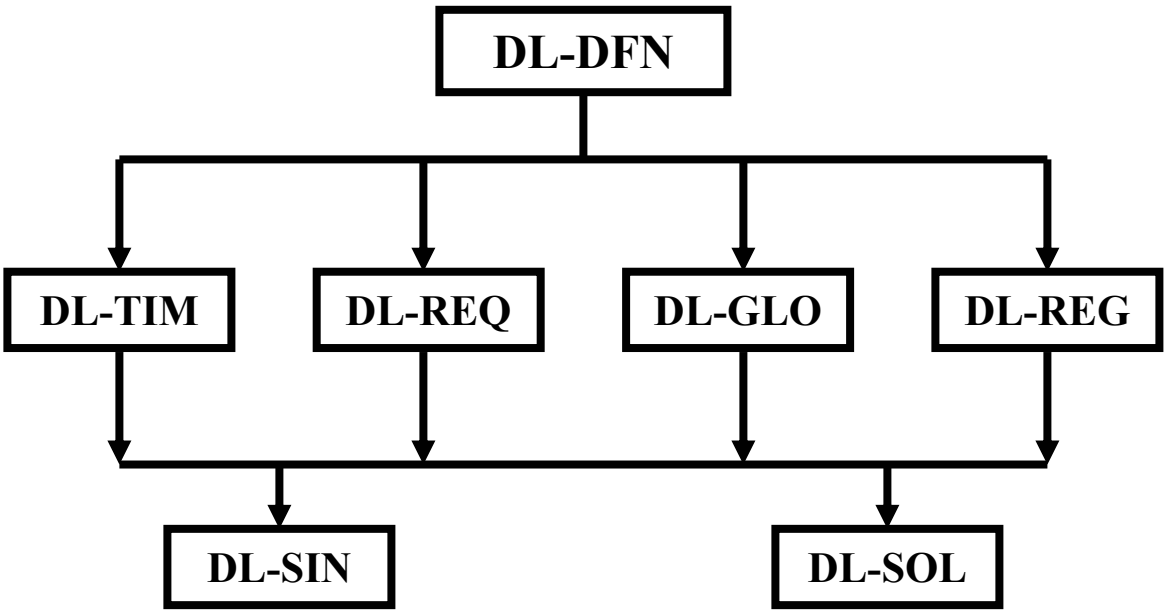


Figure E-1. Relation of SDR Forum Software Download Documents

Appendix G: Summary of Wireless Threats Defined by 3GPP

Table G-1: Summary of Wireless Threats Defined by 3GPP[18]

Threat Category	Attacks on the Radio Interface	Attacks on Other Parts of the System
Unauthorized access to data	**Eavesdropping user traffic:** Intruders may eavesdrop user traffic on the radio interface.	**Eavesdropping user traffic:** Intruders may eavesdrop user traffic on any system interface, whether wired or wireless.
Unauthorized access to data	**Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on the radio interface. This may be used to access security management data or other information which may be useful in conducting active attacks on the system.	**Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on any system interface, whether wired or wireless. This may be used to access security management data which may be useful in conducting other attacks on the system.
Unauthorized access to data	**Masquerading as a communications participant:** Intruders may masquerade as a network element to intercept user traffic, signalling data or control data on the radio interface.	**Masquerading as an intended recipient of data:** Intruders may masquerade as a network element in order to intercept user traffic, signalling data or control data on any system interface, whether wired or wireless
Unauthorized access to data	**Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on the radio interface to obtain access to information.	**Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on any system interface, whether wired or wireless, to obtain access to information.
Unauthorized access to data	**Active traffic analysis:** Intruders may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.	**Unauthorised access to data stored by system entities:** Intruders may obtain access to data stored by system entities. Access to system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.
Unauthorized access to data		**Compromise of location information:** Legitimate user of a 3G service may receive unintended information about other users locations through (analysis of) the normal signalling or voice prompts received at call set up.

[18] From Reference [5]

Threats to integrity	**Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on the radio interface. This includes both accidental or deliberate manipulation.	**Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.
Threats to integrity	**Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling data or control data on the radio interface. This includes both accidental or deliberate manipulation. Note: Replayed data which cannot be decrypted by an intruder may still be used to conduct attacks against the integrity of user traffic, signalling data or control data.	**Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling or control data on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.
Threats to integrity		**Manipulation by masquerading as a communications participant:** Intruders may masquerade as a network element to modify, insert, replay or delete user traffic, signalling data or control data on any system interface, whether wired or wireless.
Threats to integrity		**Manipulation of applications and/or data downloaded to the terminal or USIM:** Intruders may modify, insert, replay or delete applications and/or data which is downloaded to the terminal or USIM. This includes both accidental and deliberate manipulation.
Threats to integrity		**Manipulation of the terminal or USIM behaviour by masquerading as the originator of applications and/or data:** Intruders may masquerade as the originator of malicious applications and/or data downloaded to the terminal or USIM.
Threats to integrity		**Manipulation of data stored by system entities:** Intruders may modify, insert or delete data stored by system entities. Access to system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

Denial of service	**Physical intervention:** Intruders may prevent user traffic, signalling data and control data from being transmitted on the radio interface by physical means. An example of physical intervention is jamming.	**Physical intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by physical means. An example of physical intervention on a wired interface is wire cutting. An example of physical intervention on a wireless interface is jamming. Physical intervention involving interrupting power supplies to transmission equipment may be conducted on both wired and wireless interfaces. Physical intervention may also be conducted by delaying transmissions on a wired or wireless interface.
Denial of service	**Protocol intervention:** Intruders may prevent user traffic, signalling data or control data from being transmitted on the radio interface by inducing specific protocol failures. These protocol failures may themselves be induced by physical means.	**Protocol intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by inducing protocol failures. These protocol failures may themselves be induced by physical means.
Denial of service	**Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted on the radio interface by masquerading as a network element.	**Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted by masquerading as a network element to intercept and block user traffic, signalling data or control data.
Denial of service		**Abuse of emergency services:** Intruders may prevent access to services by other users and cause serious disruption to emergency services facilities by abusing the ability to make USIM-less calls to emergency services from 3G terminals. If such USIM-less calls are permitted then the provider may have no way of preventing the intruder from accessing the service.

Unauthorized access to services	**Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication has been performed.	**Masquerading as a user:** Intruders may impersonate a user to utilise services authorised for that user. The intruder may have received assistance from other entities such as the serving network, the home environment or even the user himself.
Unauthorized access to services		**Masquerading as a serving network:** Intruders may impersonate a serving network, or part of an serving network's infrastructure, perhaps with the intention of using an authorised user's access attempts to gain access to services himself.
Unauthorized access to services		**Masquerading as a home environment:** Intruders may impersonate a home environment perhaps with the intention of obtaining information which enables him to masquerade as a user.
Unauthorized access to services		**Misuse of user privileges:** Users may abuse their privileges to gain unauthorised access to services or to simply intensively use their subscriptions without any intent to pay.
Unauthorized access to services		**Misuse of serving network privileges:** Serving networks may abuse their privileges to gain unauthorised access to services. The serving network could e.g. misuse authentication data for a user to allow an accomplice to masquerade as that user or just falsify charging records to gain extra revenues from the home environment.
Repudiation		**Repudiation of charge:** A user could deny having incurred charges, perhaps through denying attempts to access a service or denying that the service was actually provided.
Repudiation		**Repudiation of user traffic origin:** A user could deny that he sent user traffic.
Repudiation		**Repudiation of user traffic delivery:** A user could deny that he received user traffic.

Definitions Applicable to Table G-1

Unauthorised access to sensitive data (violation of confidentiality)

- **Eavesdropping:** An intruder intercepts messages without detection.
- **Masquerading:** An intruder hoaxes an authorised user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorised user to obtain system service or confidential information.
- **Traffic analysis:** An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.
- **Browsing:** An intruder searches data storage for sensitive information.
- **Leakage:** An intruder obtains sensitive information by exploiting processes with legitimate access to the data.
- **Inference:** An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

Unauthorised manipulation of sensitive data (Violation of integrity)

- **Manipulation of messages:** Messages may be deliberately modified, inserted, replayed, or deleted by an intruder

Disturbing or misusing network services (leading to denial of service or reduced availability)

- **Intervention:** An intruder may prevent an authorised user from using a service by jamming the user's traffic, signalling, or control data.
- **Resource exhaustion:** An intruder may prevent an authorised user from using a service by overloading the service.
- **Misuse of privileges:** A user or a serving network may exploit their privileges to obtain unauthorised services or information.
- **Abuse of services:** An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.

Repudiation: A user or a network denies actions that have taken place.

Unauthorised access to services

- Intruders can access services by masquerading as users or network entities.
- Users or network entities can get unauthorised access to services by misusing their access rights

Appendix H: Digital Rights Management

Appendix H: Digital Rights Management

Securing adequate protection for copyrighted works in the digital environment will allow development of viable business models. Viable business models will in turn help drive adoption of broadband and the innovation and sale of new products (e.g. portable devices, PCs, digital televisions, and subscription services), and expanded consumer choices through an increasing variety of formats, consumption options, and price points for enjoying copyrighted works.

Recognizing this, private sector cross-industry efforts have developed several content protection solutions. These solutions include Content Protection for Pre-recorded Media ("CPPM") for protecting pre-recorded audio content on DVD Audio, and protection for digital content as it moves among devices in the consumer home and personal environment on digital networks (Digital Transmission Content Protection ("DTCP") and High-bandwidth Digital Content Protection ("HDCP")) and recordable media (Content Protection for Recordable Media ("CPRM")).

The goal of these efforts is to create an overall architecture for protecting digital content throughout its distribution life so that it does not "leak" out in an unprotected manner for easy capture by digital pirates, including users who traffic in copyrighted works on peer to peer systems. In each case, the solutions have been developed by information technology ("IT") and consumer electronics ("CE") companies in consultation with studios and music labels and then implemented through private licenses. These content protection solutions are made available to all interested product manufacturers and content companies and are already enjoying adoption in the marketplace, with DVD video being the most notable example of wide marketplace adoption.

The industry efforts to date have concentrated on developing systems to secure content from its initial distribution through the delivery and consumption chain. These efforts are generally unable to provide protection when content is delivered "in the clear" to legacy systems. One such example is the protection of terrestrial digital broadcast that is delivered "in the clear." Companies have been actively participating in the Broadcast Protection Discussion Group. Significant progress has been made towards a technical solution that would involve a "broadcast flag" to signal that redistribution of digital broadcast content over the Internet is not authorized. In order to ensure that detection of and proper response to such a broadcast flag occurs in digital broadcast receiver products, some narrowly focused government regulation will be necessary.

This is an example of how private multi-industry efforts can yield a technical solution where narrow government action is appropriate for proper enforcement of that consensus solution.

Furthermore, this example also illustrates the value of government complementing productive cooperation among relevant industries to find solutions, as has been done in this instance through FCC and legislative forums.

An even more complicated problem is the phenomenon of unconstrained unauthorized copying and redistribution of copyrighted content over peer-to-peer networks. One contributing factor is the growing variety of increasingly decentralized peer-to-peer

networks (e.g., Morpheus, Limewire, etc). Another is that content reaches peer to peer networks from a variety of sources including unprotected distribution, circumvention of protected content, camcording from theater screens, and diversion during production. No single silver bullet solution - technical, legal, legislative, or business - exists to address this thorny form of piracy. Active co-operation and participation of all sectors--content, CE, IT, service providers, and government--will be necessary to develop a range of solutions to this complex problem.

A significant Digital Rights Management tool is the evolution of digital watermarking. The control of distribution and verification of ownership of digital information is achieved by embedding identifying information into the data. Watermarking can be utilized for many diverse purposes such as; copyright and content protection, authentication and integrity verification, image tagging (tracing illegally copied originals), security (passport photos, etc.), metadata tagging (insertion of content information, usage control and secret communication.

Robust Watermarking is a technology that embeds copyright information of digital contents with unrecognizable signals to humans into the digital contents. It shows strong resistance to tampering efforts (cropping, resizing, compression, etc.) and can be detected for verification of copyright information of the digital contents. Generally, the copyright information is embedded, however, any data can be embedded. The watermark technology can be expanded not only to the digital environment but also to the analog environment.

To test for the robustness of the image watermark, there are tools such as Stirmark and Checkmark which are used to test watermarks by attacking the image with a variety of hacking efforts. Standardization organizations such as SDMI, STEP 2001 are used to test an audio watermark. There are 12 attack patterns for audio watermarking solution. For a video watermark test, survival of watermark thorough digital to analog conversion and vice versa and clear video quality in digital broadcasting are key factors. Properties of a desirable watermark would have perceptual transparency, data capacity, and robustness to image filtering operations, resistance to tampering and a reasonable computational complexity.

Authentication Watermarking detects forged or alter data, extracts user information, show user information from only authenticated files. It can be applied to digital documents, medical images, DVR, etc. Application of authentication watermark could be expanded to a variety of the field that requires authentication and prevent forgeries.

Digital watermarking is adding DRM solutions by guaranteeing that, even after an authorized purchase, the content can be permanently ‘tagged’ with specific user information. In the context of digital rights management, digital watermarking provides a means of distinctively and permanently ‘tagging’ the content with user-specific information. Watermarks can now be applied automatically with the exact parameters of the transaction. Thus, where subsequent copyright misuse occurs, the digital watermark provides an audit trail back to the original purchaser. By permanently marking the digital content at the point of licensing, dishonest users are thwarted.

Some of the companies in this field are as follows:

Digimarc Corporation uses digital watermarking components and technologies in a wide range of security, identification and brand protection applications. Digimarc ID Systems is the leading producer of driver's licenses in the U.S., providing systems and services to 36 states. Internationally, Digimarc ID Systems produces identification documents for governments around the world. They have an extensive intellectual property portfolio, with 60 issued U.S. patents with more than 1,000 claims, and more than 300 pending applications for U.S. patents, in digital watermarking, personal identification and related technologies.

SealTronic Technology, Inc., has two product group categories. One being Copyright Protection Management (CPM). Its products prevent the pre-unauthorized duplication of digital contents. In the case of any unauthorized or illegal distribution, the CPM products enable the copyright holders to track and therefore to prove the illegal, unauthorized usages of copyrighted contents. The other product is a fraud/forgery authentication group that includes solutions, which authenticate fraud, forged files after digital conversion, or prevent forgery or fraud in analogue data such as identification card, and chips designed that are being applied to any devices for authentication. Rights@fer^{TM}, is a digital rights management tool developed by SealTronic Technology. Inc. It is designed for secure distribution, protection, management of digital contents from the creation to the end users with application of encryption technology to the digital contents transmitted via various channels such as the Internet, E-mail, mobile communication, and satellite, etc. With encryption technology, it enables the copyright holders of the digital contents and the contents providers to be able to prevent copyright infringement of the contents by unauthorized mass duplications and to prevent leakage of confidential information. It also enables authorized users to use encrypted content by transmitting decryption keys upon request. It is easy to correspond with contents providers' various service policies, supports various billing/payment solution, and modeling is easy to change.

Signum Technology has a special version of VeriData software, called iPak, especially designed to discourage the activities of counterfeiters and gray-marketers. VeriData iPak allows users to upgrade their current packaging to a very high-security design. It incorporates a sophisticated invisible watermarking that allows the incorporation of hidden identifying data into printed packaging and labels. Examples of the data that can be hidden are the manufacturing source, batch numbers or shipment destinations. With the use of an inexpensive scanning device and the VeriData iPak detection software, the hidden data can be revealed in a matter of seconds. This would enable a manufacturer or authorized agent to rapidly and discreetly sample packaging to check the legitimacy or derivation of products. The VeriData iPak software can be deployed in almost any design and print workflow, versions are available to run on most workstation platforms.

Appendix I: Information on Companies Having General Security Products

Appendix I: Information on Companies Having General Security Products

Some of the companies in this field are as follows:

SmartTrust

The evolution during the last couple of years has been extremely favorable for the SIM technology. It is now clear that almost all of the future mobile telecommunications technologies will have a smartcard based SIM, whether it is called SIM, USIM or R-UIM. More than 70 operators are using SmartTrust Delivery Platform to launch enhanced SMS services and to manage mobile end-user applications. In addition, more than 150 customers, ranging from Trust Service Providers, banks and financial institutions, government, operators and large enterprises are using SmartTrust products for digital identification and digital signatures.

InterTrust

InterTrust Technologies Corporation has developed a general-purpose digital rights management (DRM) platform to serve as a foundation for providers of digital information, technology and commerce services to participate in a global e-commerce system. The Company provides its DRM platform as software, tools and hardware to licensees, which are called partners. These partners intend to offer digital commerce services and applications that collectively will form a global commerce system, which the company has branded as the MetaTrust Utility. The Company's system addresses numerous areas of security, including securing digital information after initial use and providing tamper resistance in its InterRights Point software. The company has designed countermeasures that it intends to implement if security is compromised

RightsMarket

RightsMarket provides software and services to securely distribute digital content and prevent unauthorized use - even after delivery. Offering solutions for both text and audio in the areas of ePublishing, eLearning, and eHealth, RightsMarket enables organizations to capitalize on the enormous opportunities inherent in distribution over the Net. As experts in rights management, RightsMarket offers Systems Integration (SI) services that leverage RightsMarket technology to provide custom solutions tailored to the clients' needs. The company's flagship product, RightsPublish, is an end-to-end solution for selling, securing and tracking digital content. Easy to implement, RightsPublish provides a Web storefront, eCommerce, complete audit trail, and persistent security. RightsMarket encrypts digital content, meters usage, authenticates the user, provides rights management authorization, and creates a transaction log for reporting and billing purposes.

Digital Owl

DigitalOwl provides information management application services that leverage digital rights management to solve critical business problems. Their products and services enable customers to securely license, promote, distribute and manage premium

information within end-user communities. Focused on secure information movement in financial, healthcare, publishing and corporate markets, DigitalOwl understands the information issues facing these companies today. DigitalOwl's KineticEdge™ is a highly flexible suite of information management applications that securely licenses, promotes, distributes, and manages premium information within end-user communities. By leveraging digital rights management, KineticEdge automates the flow of premium information (information that requires controlled distribution or usage tracking) to end-users, while facilitating secured, yet seamless, content controls for premium or proprietary information that resides on desktops and PDA devices. Clients receive a robust set of usage tracking reports, which indicate how and where their premium information is being used, as well as information on pass-along flow, and recommendations within end-user peer groups.

Wireless Ethernet Compatibility Alliance

Wireless Ethernet Compatibility Alliance (WECA) works to certify interoperability of Wi-Fi (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments. WECA has worked closely with several leading vendors of IEEE 802.11B High Rate WLAN equipment and Agilent Technologies Interoperability Certification Lab (Agilent ICL) to develop an interoperability test bed. Interoperability testing is now underway at Agilent's ICL. Agilent's ICL is operating as an independent test facility. Only WECA members can submit products to the lab for interoperability testing. When a product meets the interoperability requirements as described in the test matrix, Agilent's ICL notifies WECA. WECA then grants a certification of interoperability, which allows the vendor to use the Wi-Fi logo on advertising and packaging for the certified product. The Wi-Fi seal of approval assures the end customer of interoperability with other network cards and access points, which also bear the Wi-Fi logo.

VeriSign, Inc.

VeriSign, Inc. is a provider of digital trust services that enable businesses and consumers to engage in commerce and communications with confidence. VeriSign's digital trust services create a trusted environment through four core offerings—Web presence services, security services, payment services, and telecommunications services—powered by a global infrastructure that manages more than 6.5 billion communications and transactions a day.

VeriSign serves as a gateway to establishing an online identity and Web presence, operating the database of over 27.3 million Web addresses in .com, .net, and .org on a powerful platform that is the world's de facto standard in Domain Name System (DNS) registry services. Responding to over 6.5 billion DNS look-ups daily, the powerful platform serves all of the world's domain name registrars and helps position VeriSign as a leading provider for secure high-volume transaction services.

F-Secure Corporation

F-Secure Corporation is a provider of centrally managed security solutions for the mobile enterprise. The company's products include anti-virus, file encryption and network security solutions for all major platforms from desktops to servers and from

laptops to handhelds. Customers in nearly every industry - Government, Manufacturing, Retail, Telecommunications, Finance, Energy, Transportation, High Tech and more - rely on F-Secure products to make information secure, reliable and accessible. Mobility challenges many of the fundamental assumptions upon which traditional IT systems have been based on. F-Secure supports businesses with a broad range of centrally managed and up to date security solutions to enable a truly mobile enterprise.

F-Secure is supported by a network of value-added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and Compaq

Appendix J: Companies Having Firewall Products

Appendix J: Companies Having Firewall Products

Netscreen Technologies, Inc. develops and sells scalable network security solutions. Its line of integrated security systems and appliances combine firewall, VPN, traffic management and other security functions within a high-performance platform. Their security products combine a custom, real-time operating system, purpose-built hardware designs, and ASIC technology. The products created by NetScreen show an extensive and complete range of applications, from multi-gigabit-speed security systems for the largest of carriers to solutions for a single telecommuter. They have a scalable policy-based security management system that is said to provide a comprehensive view of a customer's security position and a simplified means to deploy and manage policies in large-scale environments. The performance barriers are said to be reduced and at the same time still deliver a rigid level of security (an ICSA certified inspection firewall and a very high level of data security 3DES IPSec encryption support).

RapidStream, Inc is the developer of an integrated virtual private networking (VPN) and firewall solution that is scalable improves security and performance. Their processor is a patented network security processor that enables their products to outperform the other security systems with VPN components. The network packets are executed in the processor in a "cut-through" path that completely bypasses the main CPU and as well as the system bus which are said to be the main bottlenecks in present security and VPN system architecture. The processor is said to simultaneously execute firewalls, Network Address Translation (NAT), QoS, and IP Security (IPSec) policies at very high speeds. The system can handle large security policy rule lists without degrading network performance.

Other products produced by RapidStream are designed to cover broad range of VPN/firewall implementations, from the requirements of a small-to-mid-sized enterprise all the way to the complex needs of larger enterprises and data centers. Their products can support 10/100-Megabit and Gigabit Ethernet interfaces, firewall throughput from 20 to 620 Megabit per second (Mbps), VPN-3DES throughput from 10 to 360 Mbps, from 50 to 128,000 concurrent sessions, and from one to 20,000 concurrent VPN tunnels.

The RapidStream solutions also claim to support features for failover and redundancy between two devices. These features should ensure a high availability since no single point of failure exists within the network.

Cranite Systems Inc. has developed what seems to be a highly secure version of their BlueOrbit, an integrated wireless LAN product for the Sun Cobalt Qube ™ appliance. This product is the first to incorporate the company's WirelessWall technology. It relays on the Advanced Encryption Standard (AES) for highly secure radio data transmissions. Cranite's WirelessWall technology provides an integrated security, mobility, and manageability solution for wireless data networks of any size. Their technology unites AES encryption, improved authentication, per-connection wireless firewalls, enhanced mobility, and an advanced usability and manageability. BlueOrbit asserts a good combination of easy-to-use server functionality and a straightforward mobile networking that is based on 802.11b wireless LANs. By the integration and simplification of a quantity of key server and connectivity capabilities, it is said to facilitate small businesses

that deploy sophisticated computing and network systems. With the addition of AES encryption, BlueOrbit will further protect their customers' data with the industry's wireless LAN security approach.

Checkpoint Software Technologies, Ltd. Check Point Software Technologies Ltd. has developed a firewall product as part of their enterprise security software suite. FireWall-1 integrates access control, authentication, network address translation, content security, auditing, and more. It enables organizations to define and enforce a single, comprehensive security policy that protects all network resources enterprise-wide. Its three-tier architecture patented Stateful Inspection technology, and the Open Platform for Security delivers a highly scalable solution that is able to integrate and centrally manage all aspects of Internet security. Their firewall products integrate into the other enterprise security elements, such as quality of service and VPN solutions.

Appendix K: Companies Having VPN Products

Appendix K: Companies Having VPN Products

Columbitech and Diversinet

Columbitech, a company providing software for wireless access to corporate data, and Diversinet, a developer of wireless security software enabling mobile e-commerce, have collaborated on and introduced a new PKI-enabled wireless virtual private network (VPN) solution designed to secure wireless enterprise communications. The product, The Passport Wireless VPN, is a merging of Diversinet's wireless PKI technology and Columbitech's wireless VPN product. This has been done primarily in an endeavor deliver wireless security for enterprises in North America, Europe and Asia. The solution supports a full-strength encryption; authentication and certificate processing capabilities to support secure remote access to corporate networks. The companies add that the product supports the principal mobile device platforms, such as Pocket PC handheld devices and Windows-based notebook computers. Their product has been designed to operate independent of network type and wireless service provider, and is based on the standard protocols for communication and security that is supposed to confirm function with both wireless and wired communications. One of the Passport Wireless VPN's features is that it permits the mobile user to seamlessly roam between different wireless network topologies in a single VPN session. The user would not be required to log on again. In theory, this attribute would allow a wireless notebook user to move from VPN access to the office network using a WLAN and, while connected on the same VPN session, remain connected using a mobile phone connection while traveling home. The same user could then switch the notebook over to a home broadband or dialup connection without losing the VPN session.

Certicom

Certicom offers a wireless security technology designed to optimize product performance in a mobile environment. Certicom has developed the movian products to deliver handheld security applications to enterprise customers. MovianVPN is an IPSec software client that runs on handheld devices. This client enables enterprises to provide their mobile professionals with secure remote access to the corporate Intranet from wireless devices like PDAs and smart phones using their existing wired VPN infrastructures. It is interoperable with leading VPN gateways, allowing the enterprise to extend its current VPN investment. Supports Windows CE, Palm OS, and Symbian OS.

Checkpoint Software Technologies

CheckPoint's SecureClient™ for Microsoft Windows-Powered PDAs and handheld PC devices delivers end-to-end integrated VPN and firewall functionality for secure communications to the corporate network Users benefit from the improved security and scalability offered by PKI technologies and support for PKIs from leading Certificate Authorities.

Nokia

The Nokia Mobile VPN Client extends the VPN concept to mobile workers who instead of laptops now carry pocket-sized devices. Nokia Mobile VPN Client is designed for smart phones running the Symbian operating system and is almost transparent to the user.

Once an application such as email is launched, a connection is automatically established at which point the mobile user is prompted for proof of identity using a token such as a SecurID password or a digital certificate. Once authentication to the corporate VPN occurs successfully, a wireless VPN tunnel is established and all data travelling to and from the device is encrypted, no matter what the mobile application. Because of the stringent security inherent in IPSec, the data is protected from being captured and retransmitted later and is received exactly how it was sent.

Appendix L: Companies Having m-Commerce Security Products

Appendix L: Companies Having m-Commerce Security Products

Visa's 3D-Secure

Mobile 3D is Visa International's global specification that ensures the security of Internet payments made over mobile phones. Launched in September 2001, in conjunction with some 15 major industry players, including Ericsson, Motorola and Oracle Mobile, the Mobile 3-D Secure specification is based on existing payment technologies and is a result of Visa's ongoing efforts to ensure that both buyers and sellers are protected when they use or accept a Visa card.

Mobey Forum

The Mobey Forum (pronounced Mo-Bay) announced by financial institutions and mobile manufacturers on May 10th 2000 is a financial industry-driven forum, whose mission is to encourage the use of mobile technology in financial services - such as payment, remote banking and brokerage.

MeT

MeT (Mobile Electronic Transactions) announced mid-April 2000 is another industry joint effort by Ericsson, Motorola and Nokia to develop a common framework for mobile e-business. Siemens, Sony and Matsushita are also members. It aims at the creation of the personal trusted device by integrating security and transaction applications into mobile terminal platform, to develop an open and common industry framework for secure mobile electronic transactions.

It released its first specification in March 2001.

Radicchio

Launched in September 1999 with SmartTrust, Gemplus, Ericsson and "Electronic Data Systems (EDS)" as founding members, Radicchio was created to enable a dynamic global market for secure wireless e-commerce. Radicchio will persuade international organizations and government bodies of the importance of supporting security in global mobile e-commerce and of taking into account the growth potential of mobile e-commerce when drafting new legislation.

MEST

The Mobile Electronic Signature Consortium is an association of companies and organizations from the mobile phone and Internet sectors to establish and develop a secure cross-application infrastructure for the deployment of mobile digital signatures. It was founded by BROKAT, Siemens, E-Plus Mobilfunk GmbH, Mannesmann Mobilfunk GmbH and VIAG Interkom; Gemplus and Schlumberger T-TeleSec Trust Center of the Deutsche Telekom and cryptovision. It aims to develop a uniform application interface as the de-facto standard for the integration of the mobile phone into the Internet world and to use the mobile phone for implementing mobile digital signatures. The application interface will facilitate standardized communication between customers and retailers, providers of financial services, lotteries and other e-Commerce providers on the Internet.

PayCircle

PayCircle is a consortium is set up in March 2002 by Hewlett-Packard, Lucent Technologies, Oracle, Sun, and Siemens to set standards for payments with mobile phones. The consortium aims to provide mobile device users worldwide a standard means of making mobile payments, regardless of the payment systems used by merchants or service providers.

Meridea

Meridea Financial Software is a company that was formed in March 2002 by 3i, Accenture, Nokia, and Sampo. It provides multi-channel banking and financial software solution based on open standards which enables consumers to access electronic and mobile financial services through multiple channels including mobile devices, the Internet, telephones, IVR's (Interactive Voice Response systems) and digital TV.

Appendix M: Security Mechanisms Applicable to Wireless Communications Systems

Appendix M: Security Mechanisms Applicable to Wireless Communications Systems

Virtual Private Networks:

Virtual Private Networks (VPNs) are increasingly capturing the interest of many companies and organizations that would like to expand not only their networking capabilities but to also trim their costs as well. VPNs are of course in the workplace, but are additionally found in the home, where they permit employees to securely log into company networks. VPNs would be of benefit and convenience to anyone who travels or telecommutes.

They supply network connectivity over extended physical distances and utilize the public networks (Internet) rather than the necessity of relying on private lines. VPN technologies can implement restricted-access networks that use the same cabling and routers as a public network without the fear of losing any features or any of the basic security functions. They are able to support remote access client connections, LAN-to-LAN internetworking and controlled access within an intranet.

VPNs offer a cost savings to the user and represent an advantage over competing methods. Scalability is also a positive factor of VPNs. As an organization grows and adds more users, it would be comparatively easy to upgrade the VPN to accommodate the extra load. The present systems have the ability to either scale up (or down), as you need. Of course, the advantage being that you would not have to throw our your present hardware and purchase new equipment; you would merely upgrade what was currently being used. In a traditional WAN this addition can simply limit the flexibility for expansion. VPNs that make use of the Internet steer clear of this dilemma by merely tapping into the geographically disseminated access that is already available.

VPNs are founded on a tunneling strategy. The tunneling involves encapsulating packets constructed in a base protocol format within some other protocol. In the case of VPNs running over the Internet, packets that are in one of several VPN protocol formats are encapsulated within IP packets. Therefore, when a VPN connection is made, the software on one end contacts the VPN gateway, for example, an office's Ethernet router. The entryway characteristically confirms that an approved user is entering by checking the password. Then the VPN software creates the tunnel and inserts a header to the data packet that the Internet can recognize. When the packet reaches the gateway endpoint, the gateway pulls off the Internet header and routes the packet to its final destination.

Three current technologies are used by VPNs to create a tunnel: Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), and the very latest standard, Internet Protocol Security (IPSec). While the tunnel is creating the network, the encryption makes it private by scrambling data to ensure that only those who have the right digital key can decode it.

Several different companies have collaborated and developed the specifications for the PPTP. PPTP's chief strength is found in its ability to support non-IP protocols. It offers

compression, comparatively weak encryption, and is viewed by many as a "make do" remote access VPN solution.

The original competitor to PPTP in VPN solutions was the Layer 2 Forwarding (L2F) protocol – which is Cisco's proprietary tunneling protocol implemented primarily in Cisco products. In attempts to improve on L2F, the preeminent features of it along with PPTP were joined to create a new standard, L2TP. L2TP exists at the data link layer (layer two) in the Open Systems Interconnection reference model (OSI). Like the PPTP, the L2TP supports non-IP clients. However, the L2TP supports non-Internet based VPNs including frame relay, ATM, and SONET.

The Internet Protocol Security (IPsec) is essentially a compilation of multiple related protocols. The IPSec criterion takes the procedure much further by verifying and encrypting each packet of data to ensure the maximum of privacy. It can be utilized as a complete VPN protocol solution, or it can be utilized simply as the encryption scheme within the L2TP or the PPTP. IPsec exists at the network layer (layer three) in the OSI and it extends the standard IP for the purpose of supporting more secure Internet-based services (including, but not limited to, VPNs). This set of IP extensions, which are based on modern cryptographic technologies, offer strong data authentication and privacy guarantees by securing the network, rather than just the applications.

It is quite clear that industry dynamics will clearly impact the future success of VPNs. Much of the value in VPNs lies in the likelihood for organizations to save money. The attraction and appeal of VPNs should substantially increase with the solidification of VPN standards and with vendor products that will interoperate completely with each other. Success of the VPNs will also rely on the ability of both intranets and extranets to deliver on their assurances. In the past as well as the present, organizations have struggled to measure the true cost savings of their private networks, but with the verification that they provide a noteworthy value, the utilization of VPN technology should also increase.

With the proliferation of mobile devices there is a real need to implement wireless VPN solutions that will be cost-effective and flexible enough to integrate with existing network infrastructure. These solutions need to work efficiently with the limited resources available on most mobile units. It also needs to be supported on a variety of systems for maximum coverage. Finally, the solution needs to provide strong mutual authentication between the VPN gateway and the client device accessing it

Firewalls

A firewall's function is to protect a computer network from unauthorized access. It controls access to a network and enforces a security policy by means blocking traffic or permitting traffic and access to network data. They may be hardware devices, software programs, or a combination of the two. A firewall typically guards an internal network against any malicious intrusion from the outside; however, firewalls may also be configured to limit access to the outside from internal users. There are three broad methods used in firewalls, with vendors using a combination of these architectures.

Packet filters- Packets are analyzed against a set of rules to determine whether they will be allowed to pass through. This is the most basic line of defense and can be done very fast since the contents of the packets are not analyzed.

Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa. Proxy servers act as an intermediary between internal and external computers by receiving and selectively blocking data packets at the network boundary

Stateful inspection - A newer method that goes beyond simple filtering. It examines the contents of each packet and compares key parts of the packet to a database of trusted information.

Packet filters look at each individual IP packet, examine the header information of in-bound and out-bound traffic and then either block the packet or allow the packet to pass through. These decisions are based upon the contents of the source address, destination address, source port, and destination port and/or connection status played against criteria defined to the packet-filtering tool and set up by the network administrator.

Perhaps the most familiar form of Internet firewall is a proxy server. The proxy firewall forces all client computers protected by the firewall to use the firewall itself as a gateway. They also provide an extra measure of safety by hiding internal LAN addresses from the outside. In a proxy server environment, network requests from multiple clients appear to the outsider as all coming from the same proxy server address. This is also referred to as Network Address Translation (NAT).

Stateful Inspection is also referred to as *dynamic packet filtering* and works at the network layer. It tracks each connection traversing all interfaces of the firewall and makes sure they are valid. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Filtering decisions are based on the network administrator's defined rules and on context that has been established by prior packets that have passed through the firewall.

However, firewalls have now evolved past a simple blocking mechanism and are being asked to do a whole host of other jobs such as authentication, encryption, VPN, quality of service, and user screening and filtering for content. These added burdens have increased the complexity of the once simple firewalls. Firewall and security system vendors have continued to add features and services to their firewall products to increase the marketability.

Biometric Technologies

Biometric technologies involve the identification or authentication of people through the use of automated processes that analyze either physiological or behavioral characteristics. Physiological characteristics used for biometrics analysis include fingerprints, patterns of the iris and retina, facial features, and hand geometry. Behavioral characteristics include handwriting, voice, and more recently keyboard dynamics. The identification aspect of biometrics is a search against many possibilities – in effect asking the question: "Do I

know you?". The authentication aspect is a one-to-one search, asking the question, "Are you who you say you are?"

Automated Biometrics has been an emerging technology for at least three decades. It has been slow to catch on due to the high cost of implementation, lack of understanding, and competition from less expensive and better know technologies (such as proximity cards). Use was often limited to buyers able to afford the large investment of time and money involved in setting up a biometric security system. However, the industry has recently seen growth opportunities caused by increased security threats such as identity theft, online commerce and banking, point-of-sale (POS) automation, and the increased use of mobile electronics. There is even an effort to define a common XML schema for the formats specified in CBEFF, the Common Biometric Exchange File Format by OASIS, a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards.

With the recent growth in consumer wireless products the biometric industry has been working to move their technology into the cellular and wireless PDA arena. Most of the technology currently targeted at fixed or wired locations, such as fingerprint and voice authentication can be transferred to wireless devices. The most common biometric security technology currently in use authenticates users via fingerprints. Several companies have developed technology to enable fingerprint identification on small mobile platforms such as cellular and paging equipment.

AuthenTec, Inc. has recently introduced a small (14mm square), low power fingerprint identification IC. The form factor of this device is suitable for cellular equipment, mobile PC and PDA, and other portable electronics. When a finger is placed on their device, a very small signal is coupled from the device to the sub dermal layer of the skin. This signal follows the ridges and valleys of the true fingerprint. The device senses subtle variations in this signal field and uses them to generate a digital fingerprint image.

AuthenTec Inc. demonstrated their sensor technology at the GSM 2002 World Congress, by running on TI's OMAP application processors for 2.5G and 3G mobile phones, wireless PDAs and mobile Internet devices. AuthenTec's combination of hardware and software would help to reduce mobile device theft, eliminate passwords, deliver more secure e-commerce transactions and protect business and personal information.

Fujitsu Microelectronics America announced on March 11, 2002 the deployment of a fingerprint identification device suitable for cellular phones, PDAs and other mobile electronic devices. Their device, the SweepSensor™, uses a similar technology as the AuthenTec device for imaging the fingerprints.

These devices are starting to find real-world use on wireless devices such as PDAs and handheld PCs. For instance, Bioscrypt, a Canadian company, is offering to license its self-contained battery-powered biometric add-on module to wireless equipment manufacturers. Using fingerprint identification technology, this device has its own processor onboard and even encrypts the biometric data for added security. The device allows for up to six users to be authenticated.

Voice authentication technology is also starting to emerge as a viable security option. This technology is well suited for the mobile telephone market. SchlumbergerSema and

Domain Dynamics Limited introduced a voice authentication system for mobile phones, which safeguards access to handsets. The new system runs on a SIM (subscriber identity module) card and requires no additional hardware, making it cost effective and simple to introduce. A SIM is actually a small computer with memory, processor, and ability to interact with the user. The SIM card holds subscriber-specific information on GSM phones and allows for personalized services. The interface between the SIM card and mobile handset is fully standardized. Like the fingerprint identification technology, this technology only allows authorized users access to the phone or its resources (such as phonebooks). Authentication requires the user to speak a phrase or word as the phone is switched on, which is compared to the reference voiceprint stored inside the tamper-proof SIM card's memory.

Signature authentication is well suited for PDAs and handheld PCs. Direct Connect Networks (DCN) is adding e-signature pad authentication technology to Acompli and Blackberry PDAs as a value added reseller. Communication Intelligence Corporation (CIC) offers a product called Signature Wallet that secures your data and Palm organizer with biometric signature verification. Sign your name and Signature Wallet will verify your signature to allow you access to your personal data.

On the horizon are mobile devices that authenticate authorized users using facial authentication systems. Atsana Semiconductor Corp. has a new processing architecture for multimedia wireless device manufacturers that allow support for biometric applications. The low-power media processor can power camera-enabled wireless phones. Visionics Corporation and Wirehound LLC are developing facial-recognition capability for Java technology-enabled Motorola phones. The application has been developed for a law enforcement agency, and uses the FaceIt ARGUS delivery platform from Visionics for facial-recognition capabilities

Net Nanny Software offers authentication technology through the use of keyboard dynamics. The BioPassword 4.5 utility uses two methods to accurately identify individuals. First, the user must know both the correct username and password and second, the user's typing rhythm must match the biometric template that has been stored and secured by the system. While this technology is not yet available for PDAs or handheld PCs, the algorithms can be adapted to measure the rhythm of a stylus used to tap out a password on a PDA.