SECURITY CONSIDERATIONS FOR SOFTWARE DEFINED RADIOS

John J. Fitton
(Harris Corp., RF Communications, Rochester, NY. jfitton@harris.com

Abstract

This paper addresses the areas in which Software Defined Radio (SDR) security standards are known to be necessary, why they are important, major criteria for these standards as well as examples of essential security features that the resultant standards should address. Particular emphasis is placed on important security features of the underlying SDR hardware and software operating environments. Security features and attributes of the SDR Forum endorsed Software Communications Architecture (SCA) are presented as an example. Hardware based security policy enforcement and flexible downloadable security policy mechanisms are also discussed.

1. INTRODUCTION

Software defined radio (SDR) technology promises to provide many benefits to both the wireless industry and their customers. Notwithstanding these benefits, successful deployment of software defined radios will depend upon whether regulatory authorities around the globe can be satisfied that this technology has the requisite security characteristics and attributes sufficiently robust to prevent its abuse and misuse.

To date there are no accepted standards governing what constitutes acceptable SDR security and much work is yet to be accomplished in defining the essential standards. One such area is the extent to which underlying hardware and software operating environments of the SDR must possess features and capabilities that prevent and detect attempts at unauthorized software installation and execution. Another important area concerns Encryption and authentication methods.

While it is clear that global standardization of the underlying security features and mechanisms is highly desirable for application to this technology, it is also important in defining these standards to recognize that differences in security policies among global regulatory authorities as well as network operators are likely to require accommodations in the underlying mechanisms which enforce these policies.

Security features such as those required for SDR equipment, whether they be user handheld terminals, mobile radios or base station terminals cannot be effectively added ad hoc when problems arise. We frequently witness the ineffectiveness involved in ad hoc solutions in the personal computer (PC) environment today. Moreover, given the tens of thousands of users who have need for personal communications as they travel around the globe, it will be essential to develop international standards that provide the security necessary to satisfy the individual and collective concerns of regulatory bodies around the world.

Of course, regulatory bodies aren't alone in their need to be concerned about SDR security. Network operators and value-added network service providers similarly need to be (and are) concerned since it is their business interests that are involved. Manufacturers of SDR equipment face potential product liability issues if their equipment easily allows its misuse or abuse. Similarly commercial end users will want the safety and integrity of their private information and transactions secure against unauthorized access or disruption.

The obvious questions to be addressed in developing these standards are what are the threats, and how does one go about providing design elements in the SDR equipment that mitigate or prevent the events associated with the various threats? One must also ask, which of these features in particular should be the focus of global SDR standardization efforts, which are of national interest only, and what are the specific concerns of operators and service providers? Finally, how does an SDR accommodate national versus international requirements versus operator and service provider needs? Some of the possible answers to these questions will be addressed.

2. BACKGROUND

The SDR Forum (SDRF) has sponsored and supported global standardization efforts regarding software radio technology. Important aspects of the Forum's effort have been the adoption of the Software Communications Architecture (SCA) [1] by the SDRF Technical Committee, co-funding of an SCA reference implementation in co-operation with the Communications Research Centre in Canada [2], and interactions with regulatory and standardization bodies around the globe.

The SCA, developed under funding provided by the US Department of Defense (DoD) through the Joint Tactical Radio System (JTRS) Joint Program Office (JPO), is an

open standard architecture applicable to a broad variety of software radio systems. It was brought to the SDRF by the JPO in order to promote commercial industry involvement and standardization. The SCA in its current form defines much of the under-lying operating environment for a SDR. Ongoing work within the SDRF Technical Committee is furthering the definition of the radio operating environment by addressing platform services and security among others. Moreover, formal SCA standardization efforts are underway in the Object Management Group.

It is beyond the intent of this paper to discuss the SCA in any detail, however, included as part of the SCA is a security supplement and appendices which provide a definition of security architecture and associated requirements for future U.S. Department of Defense radios. While the scope and depth of these requirements are perhaps arguably beyond that necessary for commercial standardization, these requirements have been developed and are based upon many years of collective experience involving radio security. As such, they serve as a useful starting point for consideration as security features for commercial software radios. These features will be considered after addressing threat areas against which the security measures must guard.

3. THE THREAT ENVIRONMENT

Specific threat areas encompass a broad spectrum ranging from network stoppage, unintentional interference, or exposure of private and confidential user information. Except by way of example, we shall address threats only in a broad sense since much of the current work of the SDR Forum, as defined in the current SDRF 2002 work plan [3], is addressing specific threats and threat scenarios.

Beyond the scope of this paper are threats imposed by the creation and use of specialized equipment intended to disrupt, mimic or otherwise spoof network operations. Those types of threats are not restricted to use against networks and terminals employing SDR technology but can be employed against any such network that has not considered these threats in the design of the air interfaces and protocols.

Thus, SDR "threats" may be the result of deliberate overt or covert actions of third parties (e.g. viruses) or through human error (e.g. software bugs) and could intended to affect either the network infrastructure or the end user terminal.

It is critically important to bear in mind that in all cases, because we are dealing with software defined radios, the threats can only be realized through the loading, installation and instantiation (execution) of software. It is also important to acknowledge that while SDR security features can address certain types of human error, such as preventing a user from inadvertently installing a virus, the only prevention of misoperation due to software bugs based on undetected design/coding errors is testing, testing, and more testing. Thus, our primary threat model focus is on software which is either deliberately intended to disrupt or otherwise perturb terminal and/or network infrastructure behavior, or is software intended to gain access to private and sensitive information contained in the user terminal or within the network infrastructure. Parenthetically, some of the recommended security measures can also provide some measure of security against some human errors.

Clearly the primary threat mitigation for SDR security is to prevent the loading, installation and instantiation of unauthorized or unproven software. From a regulatory body perspective we must address one other aspect, resulting from either the above threats or human error/software bugs. That is to ensure that SDR operations are limited to those frequency bands in which the terminal is authorized to operate by the local regulatory bodies and network operators.

4. SCA SECURITY ELEMENTS

The SCA security supplement contains several hundred specific security requirements. Many of these are specific to military and civil government radios but if we examine the broad functional categories in which these requirements exist we can see that many are also applicable, at least in a broad sense, and in some instances perhaps specifically, to a commercial SDR application. However SCA security relevant requirements and design features are not limited to those specifically called out in the SCA security supplement. Elements of the core framework and the use of standardized interfaces supported by middleware such as CORBA can also be used to enhance radio security measures. A list of relevant security feature categories defined in the SCA are given below:

- *Encryption & Decryption Services*
- *Information Integrity*
- *Authentication & Non-repudiation*
- *Access Control*
- *Auditing and Alarms*
- *Key and Certificate Management*
- *Security Policy Enforcement & Management*
- *Configuration Management*
- *Memory Management*
- *Standardized Installation Mechanisms*

To this list I add the following item:

- *Spectrum Management*

The specific meaning and intent of these categories will become clear by describing one possible approach to SDR Security.

5. AN APPROACH TO SDR SECURITY

Ironically, the personal computer is an outstanding example of how not to provide security. Whether due to design flaws which allow hackers to exploit holes in the operating systems and take over web sites or to the spread of computer viruses, we have all been impacted in one way or another. Of course we all hear about these exploits because they are widely publicized. Generally the public does not hear about specific instances when businesses have lost millions of dollars due to computer theft in one form or another.

In the light of these facts, the term "software security" is somewhat of an oxymoron. Somewhat, because practically speaking we do not believe there is any solution to SDR security which doesn't involve the application of software as part of the threat mitigation strategy, but history has shown that aoftware alone is inadequate. The implication of this statement is that SDR security will require some elements to be enforced by hardware measures. This is not an isolated view.

At the spring meeting of the SDR Forum in Tokyo, Japan a paper was presented [4] that included a hardware device identified as an Automatic Calibration Unit (ACU). The ACU is intended to ensure SDR conformance to regulatory requirements. This approach addresses in some measure the software stability issues (i.e. bugs) common to any equipment relying on software functionality. Although the ACU approach assumed a conventional IF/RF front end to the SDR, it correctly and importantly recognized the need for a hardware enforcement mechanism in some form.

Because the paper focused on how to obtain FCC or similar agency approval for new software on existing hardware or to prove new hardware with existing software, it did not address many of the issues associated with deploying new/updated software or other applications. For example, what happens to thousands of terminals already being used? How can other software that should not be capable of altering terminal behavior be loaded and executed in the terminal while ensuring proper terminal operation? These, as well as other essential concerns, were not addressed. To avoid confusion, it is important to define and differentiate categories of software from a security aspect.

5.1 SDR Software Classes

From the perspective of an open architecture based SDR, such as that of the SCA, there are several different classes of software. The role of the software in the SDR environment determines the class to which it belongs. For purposes of this paper, these are referred to as the *Radio Operating Environment, Radio Applications, Service Provider Applications and User Applications.* These are defined as follows

Radio Operating Environment (ROE) - In the context of the SCA [1] the software that consists of the Core Framework, the operating system, devices, drivers, middleware, services such as an installer and any other software fundamental to the operation of the radio platform.

Radio Applications (RA) – The software that controls the behavior of the radio as a radio. This includes any software defining the air interface and the modulation and communication protocols. In the context of the SCA, this includes software defined as being part of a waveform as well as any software used to manage or control the radio in a network environment.

Service Provider Applications (SPA) - Any type of software used to support some network or other service provider service for the user of the radio. This might include special messaging services, video services, etc. The SPA interacts with the two preceding application classes since they provide the computational environment and communications services needed to support their service.

User Application (UA) – Any software that does not fall into any of the above categories. It might consist of games, word processing, address and contact management, etc. This class of software employs only the computational and data storage resources of the platform

These definitions and terms will become more relevant as SDR security measures are addressed below.

Table 1 lists each of the categories of SDR Security and includes the author's view of the necessary basis for enforcement of the associated security mechanism. Not only *can* these security mechanisms be implemented in an ASIC, they *must be* to prevent tampering. The envisioned ASIC hardware mechanisms would include a processing core, protected internal memory, and additional features necessary to implement whatever security measures are standardized. [In this paper, the ASIC will be referred to as the Radio Security Module

(RSM).] Each of these categories will be examined as to their application to an SDR regarding standardization.

Keep in mind that the following analysis is based on the premise of preventing corrupted or malicious software from being downloaded, installed or instantiated on an SDR platform.

Security Measure	Enforcement Means		
	Hardware	Software	Both
Encryption and Decryption			X
Information Integrity			X
Authentication and Non-repudiation		X	
Access Control		X	
Auditing and Alarms			X
Key and Certificate Management			X
Security Policy Enforcement and Management			X
Configuration Management		X	
Memory Management	X		
Standardized Installation Mechanisms			X
Spectrum Management			X

Table 1. Basis of Security Enforcement Mechanism

5.2 Encryption and Decryption Services

Encryption and decryption services have several areas of application to an SDR. These services can be used (1) to maintain the privacy of different types of information; (2) to protect the information being transferred as part of an information integrity service (See 5.3) or as part of an authentication and non-repudiation service (See 5.4). Not all of these uses need be subject to SDR standardization, but SDR standardization is deemed essential to others. More importantly, the encryption algorithms and protocols employed must be compatible with and independent of the radio air interface used by any given terminal. Solutions of the past, such as that used by WAP, which introduced a cryptographic translation point, are fraught with vulnerability and must be avoided.

As noted above, encryption and decryption services can be used to protect the integrity of any class of software for download purposes. They also might be employed by an SPA (e.g. financial transactions) or by a user to protect any data stored on the terminal.

In our view, the encryption algorithms used for download should be standardized on a global level. Barring that, efforts should focus on minimizing the number of different standards that might be required in order to reduce the complexity and cost of providing this service. It is of course desirable that algorithms used by service providers within an SPA be standardized since that would allow them to be a "permanent" part of the SDR platform services and contained within the RSM ASIC. Additionally, while they need to be compatible with the air interfaces used, these SPA encryption/decryption algorithms could be downloaded and executed as part of the SPA without compromising the integrity of the underlying SDR.

Although any encryption software applications used by a user need not conform to any particular standard, if the software applications are to be installed on an SDR platform, they will have to comply with the SDR installation standards as a minimum just like software belonging to any of the four software classes.

5.3 Information Integrity

Information integrity ensures that information received (e.g. as part of a download) or stored at some earlier point has not been changed either as a result of transmission/storage media errors or intentional modification. For example, software to be downloaded to user terminals as part of a software upgrade might need to be stored in multiple locations in the network operator's network so that it can be downloaded to all the affected terminals.

One method of providing this service is to encrypt the information with an algorithm designed to prevent undetected modification of the information.

Another method might be to perform a form of mathematical calculation using all of the information and then transmit that result along with the information. In this case, the calculation result would be encrypted or otherwise protected by a suitable authentication mechanism to ensure that the parametric result hasn't also been altered.

This latter method can also be used to verify that software already installed on a terminal hasn't been modified or tampered with while the terminal was in a power down condition. Protection for such a parameter has to be tamper resistant. One method is to store the calculation result internal to the RSM ASIC in non-volatile storage; another might be to encrypt it using a key known only to that terminal.

These important SDR Security mechanisms need to be standardized on a global basis, if possible, since they are core security measures essential to SDR deployment.

5.4 Authentication & Non-Repudiation

Authentication and non-repudiation methods are well known by those familiar with public key cryptography. These involve the use of digital signatures and certificates, as well as a Trusted Central Authority.

The author views these security functions as one of the most critical to solving the SDR download security since they provide the means to verify the legitimacy of a software package downloaded onto a SDR terminal. They can be used regardless whether the download occurs via the air interface, a network infrastructure connection to a base station radio, or via a CD-ROM, etc.

A single digital signature is not deemed adequate protection for either the ROE or RA software application classes: Network operators might also require multiple signatures for the SPA class. In fact, it is possible that up to three signatures may be advisable for single downloads of either the ROE or RA classes. One signature could be from the originator of the software, which could be a 3rd party vendor, or the manufacturer of the terminal. It is likely that network operators would want to sign the download also as an indicator of their approval of the package. The third signature could be from the regulatory authority in whose area the terminal receiving the download is operating.

In practice, it is possible through the security policy function to define a flexible signature policy enabling a terminal to determine exactly how many signatures are needed and who must sign any given package.

Minimally, two signatures should be required for these classes. This provides a guard against so called "back-doors" being installed. Of more concern might be disgruntled employees or even terrorists who have gained a position inside a manufacturers organization in an attempt to subvert the contents of a software package and disrupt network operations. These types of threats should mandate that new software packages be thoroughly tested and scrutinized and that appropriate security safeguards be included throughout the testing phase, through signature and delivery.

For the UA software class, a single signature should be mandated before any terminal could install and instantiate any UA. This could virtually eliminate viruses from an SDR environment assuming the other necessary security measures are implemented.

5.5 Access Control

Access control mechanisms in today's environment generally consist of user passwords. Some computer systems can use mechanisms such as a finger print scanning while others may employ a physical key.

The need for access control methods for an SDR other than robust passwords is not apparent

Two areas of concern regarding access controls (where some standardization may be necessary) are (1) how passwords are protected within the terminal; and (2) what access control mechanisms are necessary to access any terminal security audit log either from the terminal keypad and display or via the air-interface. These could include minimum length of passwords as well as security policy governing the use, structure and requirements of allowable passwords.

5.6 Auditing and Alarms

The auditing and alarm security functions provide a means to capture events that the terminal records in some manner when a security process is violated. This process might be a receipt of an improperly signed software download or a report of numerous failed attempts for password entry.

Regulatory bodies may wish to standardize which events should be recorded and which should be automatically reported to network operators, service providers or to the user. What is recorded and reported and how this information could be governed by a flexible security policy mechanism are others for which standardization should be considered.

5.7 Key and Certificate Management

Several of the security measures discussed require the use of cryptographic keys and certificates. These should be stored in non-volatile storage within the RSM. This allows rapid and tamper-protected access to the essential information by the security functions within the RSM.

Key lengths, formats and key tags identifying the function of the key, expiration dates, etc., are all candidates for standardization. Similarly, digital certificates and their contents must be standardized for use in an SDR.

Clearly, standardization efforts must go beyond format and content, and address how, when and where keys and certificates will be updated and replaced, and what security mechanisms are required to protect these items while they are in transit from the point of creation until they are stored within the RSM of an SDR.

Finally, decisions must be made to define who may have the authority and resources to create keys and certificates, and who will be the designated Trusted

Certification Authorities. This, too, might be an area where a flexible security policy is needed since various regulatory venues may have different requirements.

5.8 Security Policy Enforcement & Management

Security policies have been referenced several times in the preceding sections without specifically defining what is meant. In this regard, security policies are simply defined as rules governing how the security mechanisms are to be employed and possibly whether or not a given security mechanism is even applicable to whatever element of terminal operation is being subjected to the scrutiny of the RSM.

Any given Security Policy (rule) can be implemented as a permanent facet of the hardware and/or software design of the terminal. Given the global nature of the application of SDR technology, it is recognized that SDR terminals will likely require the ability to support a flexible security policy mechanism whereby the rules change depending on the regulatory venue or in whose network the terminal is operating. Thus specific security policies could (and should) be downloaded and installed in the same manner as keys or digital certificates.

In developing standards in this area, the input of regulatory authorities around the globe is paramount so that their individual requirements can be given appropriate consideration. Of course, the needs of network operators, service providers, equipment manufacturers, etc., are also of primary importance, but their contributions to the standardization effort will occur in the standards body which undertakes this effort.

5.9 Configuration Management (CM)

Given the broad array of terminals and software likely to be available when SDR technology is deployed, the ability to determine and manage the configuration of an SDR is critical.

Configuration management is necessary within the SDR to ensure that the terminal has the required hardware capability to support a new software download, or that the software being downloaded is not actually replacing a newer software release that has already been installed.

The complexity of SDR configuration management might also exceed the capability of the terminal and would thus require SDR terminal interaction with a configuration management function located somewhere in the network infrastructure. The terminal should, in this instance, provide a copy of an installation log listing the hardware platform type and configuration as well as an identifier and version number of all installed software to the centralized configuration manager.

In either the case of centralized or terminal oriented configuration management, standardization is required in terms of how the SDR hardware and software configuration information is included, recorded and used within the SDR.

If centralized CM is deemed necessary, then specialized standard protocols would be needed to support the communications between the CM facility and the SDR.

5.10 Memory Management

Memory management can be an extremely effective security measure to guard against surreptitious attempts to modify installed software or any attempts to bypass the normal installation mechanisms. In this context, memory management includes control over portions of the SDR program storage memory and data memory containing software installation data (e.g. data equivalent to that stored in the Windows Registry or which is identified as the domain profile in the SCA).

In this role the RSM would have output control signals to allow the memory write-access control lines to activate and support writing of programs and data into memory. The RSM would only enable these “write access” controls when the software to be installed has successfully passed all required security screening mechanisms. Only then could a new software application be installed and activated to run.

5.11 Standardized Installation Mechanisms

Several of the more powerful security features of the architecture embodied by the SCA relate to the standardized interfaces at all levels of the software, the methods by which they are identified and used in the installation and instantiation process.

Specifically, these are, in part, the XML file descriptors (i.e. SAD, SPD, SCD, DPD, DMD and PRF) that are associated with an SCA compliant software application, device or Core Framework component. These files include items such as (1) connections among the software components; (2) listing which “ports” are needed and the parameters to be passed; (3) detailing dependencies and other information relating to how the software needs to be installed. These files are the source of the information loaded into the domain profile (similar to Windows registry) and to which access can be regulated using the aforementioned memory management security access mechanism. What is most important is that only those relationships and interfaces defined within these files are allowed during run time operation. It is interesting to note that the SCA does not define an “installer” as part of the SCA, but provides the

means to allow a common central installer to be implemented. From a security perspective, having a common central installer is essential since the installer is the core software governing the overall installation process. Without this measure each software package would have to include its own installer. In this case control over the installation process is lost and the potential for security breach is high.

While the above methods are particular to the SCA, the controlled access provided by these design features is essential to good security in an SDR environment. When coupled with memory management, download integrity and authentication mechanisms, the security of the SDR is virtually guaranteed.

5.12 Spectrum Management

From a security perspective, spectrum management is limited to providing the means to control the radiated spectrum of the SDR to that which the terminal is authorized to emit. Since any given terminal may need to operate in multiple bands in order to support global roaming by users, an RSM or its equivalent such as the ACU described in the paper [4] presented in Japan earlier this year, is needed to provide the necessary controls.

In order for SDR manufacturers to innovate and to have flexibility of design, the RSM is envisioned to provide a set of control outputs, each of which either defines or limits the spectrum available to the terminal. The individual equipment manufacturer could then determine the best manner in which to integrate these controls into its design. That design would then be approved and licensed by the applicable regulatory authority.

Application of control over these lines could then be enabled by part of a flexible security policy profile downloaded into the terminal and activated either by a signal from the network or when installed in the SDR.

6. CONCLUSION

The preceding has shown the importance and the need for substantial efforts to define a broad spectrum of relevant security standards applicable to an SDR. Further it has illustrated that by employing a combination of hardware and software technologies, such as those suggested for the RSM, and by enforcing these technologies through the use of flexible and downloadable security policies, a highly effective and secure operating environment can be achieved that will ensure successful commercial SDR technology deployment with the endorsement of regulatory agencies around the world.

7. REFERENCES

[1] Modular Software-programmble Radio Consortium under Contract No. DAAB15-00-3-0001, " Software Communications Architecture Specification", Available for download at http://www.jtrs.saalt.army.mil/SCA/SCA.html)

[2] Communications Research Centre, Canada, Steven Bernier Project Leader. " SCA Reference Implementation" When completed the SCA reference model will be available for download at: http://www.crc.ca/en/html/scari/home/home)

[3] " SDR Forum Structure and 2002 Unified Work Plan," available on-line at: http://www.sdrforum.org/public/02_a_0001_v0_00_workplan_08_26_02.pdf

[4] M. Togooch, K Sakaguchi, J. Takada, and K Araki "Automatic Calibration Unit (ACU) and ACU eMployed Authorization Procedure (AMAP) for SDR" , April 2002 SDR Forum input Document available on- line at http://www.sdrforum.org/MTGS/mtg_28_apr02/02_i_0020_v0_acu_2_04_04_02.pdf