CRITICAL FACTORS FOR APPLICATION INSTALLATION ON SOFTWARE DEFINED RADIO PLATFORMS

Lloyd Palum
(HARRIS Corporation, Rochester, New York, USA; lpalum@harris.com)

ABSTRACT

The ability to easily add or update application content is a distinguishing feature of Software Defined Radio (SDR). It is through this facility that a radio can approximate the capabilities of a general computing device. Installation of new applications or the ability to upgrade existing applications allows the radio to become a communications platform that can be enhanced to meet the changing needs of the users and the network service providers.

In the past radio platforms have for the most part been special purpose devices that are typical of many embedded software applications. The application content was programmed at the factory and updating software required completely reprogramming the device. This certainly is not the case with the software defined radio platforms. By design, the architecture allows the user to update or add capabilities without complete reprogramming. This opens a Pandora's Box of system level security and reliability concerns. We need look no further than the varied examples of malicious or ill formed software in the network and general computing environment to understand the threat of unchecked applications. It is critical that a number of security facilities be a part of the SDR to make it possible to assure installed application content is valid, and that the correct content is installed on the particular platform version.

1. INTRODUCTION

In this paper we will outline the critical system considerations that factor into the ability to update SDR content in a secure manner, and the current standardization efforts that are going on in this area. Furthermore, we outline the features of a practical Application Installation Service that is appropriate for use in a family of radios supporting the Joint Tactical Radio System (JTRS) Software Communications Architecture (SCA) [1].

2. WHO ARE THE STAKEHOLDERS

There are a numerous groups that are concerned with SDR application and content distribution. Each of these groups has a different perspective on two key questions: what are the important features of the system that will enable this capability and how to securely update terminal software. Depending on what part of the process we consider the roles of the interested parties and what their specific interests are will change. The perspectives of users, regulatory agencies, network operators, and equipment manufacturers all need to be considered when outlining the process of specifying, creating, authorizing, deploying, and installing applications.

2.1 Manufacturers

Manufacturers in the commercial sector are largely driven by the market's desire for smaller and more feature rich devices. The role of security from the manufacturer's perspective is for the most part a second tier concern. The emerging standardization efforts that are being driven by the changing terminal and network characteristics will tend to increase the significance of the security components of the commercial devices. Cost-effective implementation of security features will be a large concern of the commercial equipment manufacturers and the standards play a critical role in providing the means to reach a cost effective security solution. In military applications there is more of a focus on application security and there are formal requirements imposed on the terminals, with which the manufacturers need to comply. Many of the military SDR security features may begin to make their way into the commercial market, as the terminals increasingly become extendable application platforms.

2.2 Network Operators

The operators of commercial cellular networks have a large investment in their infrastructure. The promise of increasing revenue by providing application and content distribution is attractive; however, along with these revenue opportunities comes the increased vulnerability to network security threats. The network operators are interested in having standardization of the security methods that are used in the terminals and network infrastructure in an effort to keep the costs of deploying security down and to maintain their investments as the capabilities increase over time. The cost of security infrastructure and the cost of maintaining the infrastructure are big concerns for the network operators. Does the cost of deploying the features outweigh the potential revenue? Military applications typically have specific doctrine and methods to assure the security of their deployments. However as the scale of the network services used by the military increases, the means by which secure

distribution is accomplished may need to be re-evaluated. The mechanisms that were used in the past to securely distribute key material and configuration information are being challenged by the scale of the networks and the speed at which those networks need to be re-configured in military operations.

2.3 Regulatory Agencies

The regulatory agencies that govern commercial applications are interested in maintaining order in the use of spectrum and the signaling that is used in a given application. The ability to update the terminals in a broad sense could go as far as enabling completely new signaling and air interface capabilities. Under these circumstances the agencies need to have a means to verify the integrity of an application before distribution, and to provide a stamp of approval that gate whether the application can be used. Military applications have similar concerns relating to transmission integrity and verification that the application has been certified.

2.4 Users

Users want total control over the features of their terminal. They are interested in knowing when application content is being installed and that they can trust the source. There is also a need to provide a level of continual assurance to the user that their terminal is "virus free". Similar to the needs of PC users, the SDR will need to have facilities to verify its integrity and perhaps clean or quarantine suspect software under the direction of the user. All of this comes with a prevailing need to keep it simple and responsive. The need for increased security can not come at the expense of usability. Military applications are particularly sensitive to this concern. The SDR plays a life critical role in military operations and the security facilities of the platform need to function as transparently as possible.

3. PROBLEM DEFINITION

Taking these different perspectives into account, what are the characteristics of secure application distribution that need to be considered? Authenticity, validity, and security all need to be addressed, to ensure that rouge applications and content are not injected into the system.

3.1 Authenticity

Software and content needs to be verified to be from reputable source(s). This requirement is no different than that of many of the secure e-commerce applications that are widely used on the Internet. The content providers, regulatory agencies, and network operators all must have a way to validate content and place their seal of approval on a given application or piece of content. The user's terminals need to validate the installed content and provide feedback that the content is "good".

3.2 Validity

Software and content that are being installed need to be verified and assured to be unaltered from when they were published and signed off. It is not enough to know merely that the content or applications are from an approved source.

3.3 Security

Applications and content needs to be secure and targeted at the intended recipient. The ability to eavesdrop or highjack content is a real concern and could have privacy and loss of revenue implications for both users and providers.

4. THE ENABLING SECURITY FACILITES

As is pointed out in Fitton et al. [2], there are a number of necessary security critical features that need to be taken into account in SDR development. Many of these features are critical to providing secure software distribution and update.

- Asymmetric Cryptography (Public Key Infrastructure) for use in the authentication of the downloaded software and content. Digital Signature Standard (DSS) [3] is an example of an appropriate authentication standard mechanism.
- Encryption and Decryption for use in securing the distribution of applications and content. Advanced Encryption Standard (AES) and Triple Digital Encryption Standard (3DES) are appropriate examples of mechanisms that use symmetric shared key technology to assure privacy.
- Digital finger printing (hashing) for the use in validity checking. Secure Hash Standards SHA-1 and SHA-256 are examples of appropriate hashing mechanisms used to "finger print" applications and content.
- Key management and the ability to securely distribute and revoke key material. The scale of wireless terminal deployments makes this issue central to the ability to support millions of subscribers with a reasonable level of network overhead.
- Auditing of when content was successfully or unsuccessfully installed is a necessary feature of the terminal. This can be a problem for resource-constrained devices with limited storage.

- Access control in the form of passwords or secure ID cards to limit the exposure to critical security operations is a must.
- Configuration management dealing with what content is capable of running, or permitted to run, on a particular platform. This also extends to the interactions and dependencies between software modules that can be potentially run on the terminal at the same time.
- Memory Management that allows the software to be sequestered until it is validated and installed.

All of these facilities are critical to providing secure software distribution in an SDR. The use of a security specific module that includes trusted and validated software and hardware is also beneficial, and may be indispensable, in creating an assured solution. We want to be able to update the facilities of the SDR without compromising our trust in the security facilities. An independent hardware and software security solution go a long way to providing these capabilities.

5. STANDARDIZATION SUMMARY

Numerous standardization efforts are underway that aim to provide a framework within which to implement a scalable and secure architecture for the distribution and installation of content on software defined terminals.

5.1 3rd Generation Partnership Project (3GPP)

The 3rd Generation Partnership Project is defining a four-tier model of device capability called the Mobile Execution Environment (MExE) [4]. They take the approach that one size does not fit all and that a given device class will increase in capability over time. The device classes defined in the MExE are broken down as follows:

- **WAP enabled device** – based on the Wireless Application Protocol (WAP). This is the least capable device of the defined classes. It is assumed that the terminal is capable of performing the role of a client in the typical client server/proxy model of deployed WAP applications. The security facilities would be built up using this architecture and are typical of an internet based browsers capability.

- **Java PE** – based on the Personal Java and Java Phone APIs. This is a more capable smart phone that can draw on the security framework that is built into the Java runtime environment. [5]

- **Java ME** - The Micro Edition of the Java 2 Platform provides an application environment that specifically addresses the needs of resource constrained embedded systems. Within this class of devices there is the use of the Connected Limited Device Configuration (CLDC) with the Mobile Information Device Profile (MIDP) both of which are generic API representations supported in J2ME platforms. Again, this class can draw on the security framework that is built into the Java runtime environment.
- **The Common Language Interface (CLI)** – is specified for use in the most capable class of devices. This standard allows for applications written in different languages to execute on a common platform without being re-written. It is expected that this class of device would have similar security facilities to the Java PE and Java ME devices.

5.2 Software Defined Radio Forum

The SDR Forum Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain [6] outlines a three-tier security reference model that serves as a framework to define the system level security requirements.

- **Level 1** – Communication Channel – defines the mechanisms that are used to get the content or applications from the publisher to the subscriber. This level includes the definition of configuration management, validation of a remote terminal's right to participate in the network, authorization to download content, network facilities needed to deliver the content, packaging of the content, and the radio network air interface.

- **Level 2** – Security Provisions – defines the facilities that exist within the system used to thwart attempts to violate security. This includes evaluating the download package's credentials, deciding whether to allow installation, verification of the content, and intrusion detection.

- **Level 3** – Threats – defined as any occurrence that detracts from the perfect operation of the system. This set of threats is outlined in the definition of a Protection Profile and is concerned with intrusion, disruption, and interception.

5.3 JTRS Software Communication Architecture

The Joint Tactical Radio System (JTRS) Software communications architecture (SCA) outlines the security facilities that are available to application developers although the standard does not define the means by which application content is securely distributed for SCA capable radios. This is left up to the manufacturers of the SCA based terminals to solve using the defined security facilities of the standard. The remaining sections of this paper will present a candidate Installation Service that was developed to fill this gap in the SCA standard.

6. A SCA BASED INSTALLATION SERVICE

The Software Communication Architecture defines a system that is built around centralized "domain management". In this system the Domain Manager is a singular software component that coordinates the functions of the operating environment. The act of running applications and installing application content is done in conjunction with the SCA Domain Manager. The part of the system that is undefined is how to provide installation capability and maintain the set of required security facilities that we have outlined in this paper. We have developed a distinct Installation Service Component that works in conjunction with the Domain Manager and the Cryptographic Subsystem to manage the installation of unclassified software on an SCA based platform. This software installation could be any of the various types of radio content including radio applications, the operating environment, or configuration files. The Installation Service acts as a moderator for the installation of content. It ensures that platform installation policy is followed. It is important to note that this discussion centers on unclassified software and content. The Cryptographic Subsystem and its content are updated and maintained using a higher grade security system. This is a viable approach in that the security subsystem needs to be formally verified to be correct and is expected to change less frequently. It is the means by which the Installation Service assures the integrity of the rest of the platform. This is also a missing architectural distinction in many commercial applications, where the cryptographic services are often just a software module in which bound with the application. This level of separation between the services needs to be improved.

6.1 The Steps of Installation

Operators of an SCA radio that have the authority[1] to install and remove application content interact with the Installation Service using the radio user interface to view the currently installed content and to update or add to the applications and configuration of the radio.

The general process for content installation is as follows:

1st. Installation packages are created using the facilities of an automated build environment and they contain sufficient information to designate them for use in particular radio platforms.

2nd. Each installation package is signed using the Digital Signature Standard (DSS) and the private keys of the responsible agencies. Each agency maintains the physical security of their private keys, and publishes signed application packages and public key certificates through firewall mechanisms. It is important to note that the public keys of the signing agencies can be loaded into the terminals using either network based distribution methods or a more traditional fill device that is attached to the radio.

3rd. The Installation Service initiates and manages the installation process to assure the following policies are met:

a. Installed content is only allowed to enter the platform through controlled memory presented as a distinct "installation sandbox". The installable content is loaded into the sandbox either through a secure network file transfer or using a drag and drop file transfer. In this case the platform acts as a mass storage device connected to a computer using a USB interface.

b. Authentication of the source and integrity checking of the package are performed using the DSS and the facilities of the cryptographic subsystem. The content is not allowed to leave the sandbox until it is independently validated using the cryptographic subsystem.

c. Verification is performed to determine that the content is compatible with the platform. This is accomplished using the contents of a manifest that is built into the installation package:

- Name of the application
- UUID of the Component(s)

[1] Based on logging into the radio using a password that is stored on the cryptographic subsystem and is validated using the facilities of the radio security service.

- Version of the component(s)
- Build time and date
- Software Assembly Descriptor (SAD) XML scheme for the validation of software and platform compatibility.

4th. Install the software and configuration in the appropriate file system(s) with the correct permissions, and save the *digital fingerprint (hash)* of the application on the cryptographic subsystem to use at a later time for validation. Validation that is performed in the future is akin to enabling "virus checking". The digital fingerprint allows the software or content to be compared to its original authenticated form.

5th. Registration of the software application with the SCA Core Framework Domain Management. This is the standard interface to the Domain Manager that is specified by the SCA to load an application on the platform.

6th. Creation of an audit record of the installation and report results to the user.

6.2 Additional Future Considerations

Beyond this set of operations that are performed by the Installation Service, Cryptographic Subsystem, and the Domain Manager, there are a number of future considerations in the distribution of SCA application content.

- The current model of content distribution may need to be enhanced with key management and session oriented protocols. The scalability of distribution is directly affected by the efficiency of these mechanisms. The military currently lacks fixed infrastructure to perform on demand retrieval of application content. It is not clear whether this will be needed on a large scale with military applications. More direct distribution using storage media and physical control may be sufficient.

- Interoperability with commercial standards for homeland security and emergency management may be an area that forces some overlap in the SCA installation requirements and the commercial standards. The ability to interoperate with municipal application and configuration distribution mechanisms may be a big benefit in deploying military resources in domestic and international emergency operations.

7. CONCLUSION

This paper presented an overview of the critical system aspects of software and content distribution in a SDR terminal. The perspectives of radio manufacturers, network operators, regulatory agencies, and users were taken into account and in particular how security concerns play a critical role in how installation capabilities are provided and the facilities that need to be considered to assure system integrity. A brief overview was also presented on the standardization efforts that are considering SDR installation security as well as the overview of a particular JTRS SCA Installation Service that is appropriate for use in SCA based SDRs.

8. REFERENCES

[1] Joint Tactical Radio System (JTRS) Joint Program Office, JTRS-5000SCA V2.2.1, April 30, 2004

[2] Fitton, J., John, Cook, G., Peter, "A structure for software defined radio security." SDR Forum Input Document, SDRF-03-I-0010, May 2003.

[3] Digital Signature Standard (DSS); Federal Information Processing Standards Publication 186, May 19, 1994

[4] 3rd Generation Partnership Project; "Technical Specification Group Terminals, Mobile Execution Environment (MExE), Functional Description", 3GPP TS 23.057 V5.1.0, September 2002

[5] Java 2 Security, http://java.sun.com/j2me/docs/satsa-dg/

[6] Software Defined Radio Forum, SDRF-04-A-0010-V0.0 "Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain", October 27, 2004