Anamitra Bose
Spring 2013

SDR Security: Challenges and Existing Solutions

Introduction to SDR

A software-defined radio (SDR) is a radio communication system where the typically implemented hardware components (amplifiers, modulators, detectors, mixers, etc.) are instead implemented by means of software on a person computer or embedded system. While the concept of SDR is relatively new, the rapidly evolving capabilities of digital electronics allow SDRs to successfully achieve processes that may otherwise be practically impossible.

SDR defines a collection of hardware and software technologies where some or all of the radio's operating functions (also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies such as FPGA (field programmable gate arrays), digital signal processors (DSP), general purpose processors (GPP), programmable System on Chip (SoC) or other application specific programmable processors (Wireless Innovation). A basic SDR system may consist of a simple microprocessor equipped with a sound car or other analog-to-digital converter along with some form of RF front end. In a SDR, significant amounts of signal processing are handled by a general-purpose processor rather than being done in special-purpose hardware.

The benefits of SDR are compelling. For radio equipment manufacturers and system integrators, SDR enables a family of radio "products" to be implemented using a common platform architecture, allowing new products to be more quickly introduced into the market along with allowing software to be reused across radio "products" reducing development costs dramatically. For radio service providers, SDR enables new features and capabilities to be added to existing infrastructure without requiring major new capital expenditures along with allowing use of a common radio platform for multiple markets, significantly reducing logistical support and operating expenditures. Finally, for end users, SDR technology aims to reduce costs in providing access to ubiquitous wireless communications – enabling users to communicate with whomever they need, whenever they need to and in whatever manner is appropriate (Wireless Innovation).

SDR Security

One of the major challenges for the wide deployment of SDR and cognitive radio (CR) technology is to provide an adequate level of security. It is well known that security is an important element in wireless communications. While SDR and CR based systems should guarantee the same level of security of conventional wireless communication systems, they may also present new vulnerabilities or security threats.

As a general rule, communication systems based on SDR and CR technology must validate communication security requirements like Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization. This is a consequence of the general conformance to standards and regulations already defined for the wireless communication systems, with which SDR and CR devices must interoperate. For example, if SDR and CR devices are used in the public safety domain, they should satisfy the government approved security requirements defined by the TETRA or APCO 25 standards (Baldini et al., 2012).

SDR and CR concept may provide new powerful capabilities but they may also be vulnerable to new types of security attacks, beyond the ones already defined for conventional networks. The principal accessibility of a SDR's computer code for dynamic (de)installation and (un)loading of radio applications can introduce new security vulnerabilities in comparison to conventional radio systems, where the radio application is embedded in the design of the components.

A security threat is defined as a potential violation of security. Examples of security threats are loss or disclosure of information or modification /destruction of assets. A security thread can be intentional like a deliberate attack or unintentional due to an internal failure or malfunction. The security risk measures the impact of the realization of a security threat. Security countermeasures (protection techniques) strive to eliminate or reduce the security risks. For a SDR, the following security requirements are defined (Baldini et al., 2012):

1. *Controlled access to resources*: The system should ensure that actors are prevented from gaining access to information or resources that they are not authorized to access.

2. *Robustness*: The system should be able to provide the required communication services as described in the specific service level agreements.

3. *Protection of confidentiality:* The system should provide capabilities to ensure the confidentiality of stored and communicated data.

4. *Protection of data integrity:* The system should be able to guarantee the integrity of stored and communicated data.

5. *Protection of system integrity*: The system should be able to guarantee the integrity of system and its components.

6. *Compliance to regulatory framework*: The system should be able to guarantee the compliance to the regulations active in the area, where the system operates.

7. *Accountability*: The system should ensure that an entity cannot deny the responsibility for its performed actions. In this context, accountability is used as a synonym for non-repudiation.

8. *Verification of identities*: A telecommunication network should provide capabilities to establish and verify the claimed identity of any actor in the telecommunication network.

Communication systems based on SDR/CR should provide the capabilities to address additional security threats, which may undermine the requirements described above.

Existing Threats and Challenges

A variety of threats exist for SDR that might affect the overall functionality of the SDR and compromise the security and safety of the data transferred over the SDR. As mentioned previously, these threats might be intentional (a deliberate attack from a third party) or unintentional (a malfunction in the implementation of the SDR itself) (Palkovic et al., 2012). However, both these kinds of threats need to be handled accordingly to improve the overall safety and security for the user. One of the biggest challenges that SDR currently faces is dealing with these threats.

A major security issue introduced by the SDR is the consequence of its reconfiguration capability (Hill et al., 2012). Theoretically, SDR terminals should be able to download new radio applications or waveforms (through the air interface or through fixed communication link). Once activated, the radio application will change the radio transmission parameter like frequency, power and modulation types. This capability presents two main security issues:

1. Ensuring that the downloaded profile or software module (eg. waveform or radio application) comes from a trusted source and can be activated on the SDR device.

2. Ensuring that the downloaded profile or software module will behave as expected.

SDR data transfer usually takes through fixed or highly secured wireless connections. In this sense, the fore-mentioned security threats and mechanisms are very similar to conventional wireless systems, and the standard secure software download mechanism already defined in cellular networks could be applicable to networks based on SDR technology. An attacker can download a malicious software module or profile to the SDR terminals in the coverage area of the network. This makes SDR vulnerable to the same type of attacks as personal computers that are connected to the Internet, such as viruses, worms and other malware. The significant difference between a personal computer and SDR then is that an SDR terminal which has been hacked into can disrupt a wireless network or other wireless networks in the area by creating

harmful interference. Because SDR terminals can be designed to transmit in a wide range of frequencies, the potential of a network disruption is very high (Wireless Innovation). The following functionalities of a SDR can be affected by security threats:

1. *Application management* - Includes waveform download and activation.

2. *Resource management* - Computing and processing internal resources of the SDR.

3. *Data management* - Storage and retrieval of the configuration data used by the waveforms and the operating environment.

4. *Internal data transport* - Distribution of data among the various modules of the SDR.

These functionalities listed above are considered assets and can be impacted by security threats. Each of the threats can be directed against one or more SDR components. In addition, a specific type of asset is the data in the SDR. There are three main categories of data – user data, which represents data exchanged and stored in the SDR by the network user; configuration data, which is used by the real-time operating system (RTOS) and software framework and also includes control data and related parameters to control the SDR resources and waveform code, which includes the parameters needed by the specific waveform (this would include the reception and the transmission parameters) (Baldini et al., 2012). A description of the main threats to any SDR is as follows:

1. *Insertion of malicious software* – This threat identifies the insertion of malicious software on the SDR. This threat is similar to mobile malware in mobile applications.

2. *Alteration or destruction of the configurable data* – This threat identifies the alteration or destruction of configurable data, which is needed by the SDR to perform its functions. Configuration data can be corrupted or removed from the SDR platform.

3. *Artificial consumption of resources* – The threat identifies the abnormal increase in processing or memory resources of the SDR platform to cause a denial-of-serve (DoS attack). This threat can be induced by various causes, including the consequence of threat 1 or 2 or a physical failure.

4. *Artificial or destruction of waveform code* – This threat identifies the alteration or destruction of the waveform code, which is needed to support a radio access technology (RAT) or air interface. This threat may affect one or more waveforms but not the SDR itself.

5. *Alteration or destruction of the real-time operating system* – This threat identifies the alteration or destruction of components or the RTOS. This threat may affect all the waveforms and functions of the SDR itself.

6. *Alteration or destruction of the software framework* – This threat identifies the alteration or destruction of elements of the software framework and middleware, which support the waveforms and applications. This threat may affect all the waveforms and the functions of the SDR itself.

7. *Alteration or destruction of user data* – This threat identifies the alteration or destruction of user data, like customized profiles of the waveforms and applications. Without user data, the behavior of the SDR can be set back to the default status.

8. *Software failure* – This threat identifies a generic software failure in the any of the components composing the real-time operating system, the software framework, waveforms, or applications.

9. *Hardware failure* – The threat identifies a generic hardware failure in the SDR hardware platform. For example, a failure in the amplifiers, the filters, or the FPGA.

10. *Extraction of configuration data* – This is an eavesdropping threat, where an attacker collects configuration data, which can be used in subsequent attacks.

11. *Extraction of waveform data* – This is also an eavesdropping threat, where an attacker collects waveform data, which can be used in subsequent attacks.

12. *Extraction of user data* – This is also an eavesdropping threat, where an attacker collects user data, which can be used in subsequent attacks.

13. *Masquerading as authorized software waveform* – This threat identifies the download and activation of a malicious software waveform on the SDR platform. This is one of the most serious attacks as the download of waveforms is considered an important function of the SDR. A malicious waveform can disrupt the SDR network or affect conventional wireless networks through harmful interference.

14. *Unauthorized use of SDR services* – This threat identifies a security breach, where a waveform or applications can access or use services of the SDR platform for which it does not have the proper access level. For example, a malicious waveform could access specific cryptographic services to decode incoming secure transmissions.

15. *Data repudiation* – This threat identifies the possibility of repudiating the access or provision of data and services.

Although most of the existing threats to SDR is listed and described above, more specific threats exist that are specific to the implementation of the SDR and the FPGA used in the implementation.

Current Solutions

An SDR can be vulnerable to the same type of attacks implemented against conventional software computing platforms by downloading and activating malicious software through the external interfaces of the SDR node which may result in a variety of security threats. To protect against these threats, a SDR should be designed with similar mechanisms to the ones adopted to guarantee software assurance in information technology (Baldini et al., 2012). Software assurance for SDR requires:

1. A secure download mechanism, which guarantees the authenticity of the downloaded software. This should be complemented by the components in the SDR terminal to verify the software components.

2. A secure execution environment in the SDR terminal to guarantee that only trusted software can be activated and executed. Digital signatures could be used to ensure that only authorized software is activated. Trusted computing could also be proposed.

3. A module to ensure that spectrum regulations will be validated regardless of the software modules running on the SDR terminal. Software assurance requires also a complete software certification process.

Dynamic and secure software download is an important capability of SDR technology. For example, public safety operational scenarios may require the reprogramming of SDR terminals during an emergency due to unexpected requests or changes in the operational context. In addition, the downloaded software modules must be consistent with the regulations in the area, where the terminal is operating. In some situations, an SDR terminal may roam to an area where the original software configuration is not correct and a new software module must be downloaded (Baldini et al., 2012). Summarizing these considerations, it is possible to classify the protection techniques against the SDR security threats in the following categories:

1. *Protection techniques for secure software download*

2. *Protection techniques to ensure a secure execution environment*

3. *Protection techniques for conformance to regulations*

4. *Protection techniques for high availability*

5. *Data assurance*

The use of digital signatures to prevent activation of unauthorized software has very good potential for implementation. The proposed security framework is based on a public/private key scheme for the authentication and verification of software. The framework also describes the roles of the main stakeholders including the government, the manufacturer of the SDR terminal, the producer of the software components, and the wireless provider (Baldini et al., 2012). This solution has the advantage that the regulatory agencies can control the approval of software and /or software/hardware combinations. This is disadvantage is the complexity of the framework because digital signatures should be created for all the combinations of software waveforms/terminals and digital signatures must be reissued every time a new version of the software waveform is created.

An alternative mechanism for secure download uses the characteristics of the FPGA composing the SDR. The wiring of configuration logic blocks on FPGAs can be arranged in many different ways enabling high-security encipherment to prevent illegal acquisition of software using replay attack. Another important aspect of the secure software download is the integrity of the security administrative module (SAM) which is responsible for download, activation, and execution of the software modules.

A prominent protection technique for conformance to regulations is a SDR architecture which is composed of an automatic and calibration unit (ACU), a radio security module, and a location component based on a Global Navigation Satellite System (GNSS) receiver (such as a GPS). The ACU is responsible for controlling the output spectrum to be compliant with the local spectrum regulations. The SDR stores the information on the spectrum regulations in various spectrum jurisdictions around the world. The GNSS receiver provides the location of the SDR at any given time; the ACU uses the location and spectrum configuration files to determine the correct spectrum regulations (Baldini et al., 2012). The ACU represents a protection technique from security threat if the SDR services are related to transmission and communication of signals.

Alternatively, High assurance (HA) solutions could be used to counter security threats due to an internal failure. Currently, most SDR manufacturers are proposing HDR solutions mostly in the military market. An example of a HA solution would be a high assurance wireless communication system (HAWCS) which is a set of security components to provide higher HA and security to the SDR platform and waveforms.

Infrared FPGA monitoring is yet another solution that is being explored. Infrared sensors placed across the SDR can be used to monitor the power and heat consumption by the FPGA module. Since most software attacks would cause an overuse of the FPGA, a heat map would give an indication of when the FPGA is being overused and allow safety measures to be taken to counteract this overuse. However, this method is not very cost effective since the heat sensors would need to be highly sensitive to detect even minor changes in the temperature of the FPGA. In addition, a change in temperature would not necessarily correlate to an attack on the SDR which renders this method inaccurate on several occasions.

SDR Trends and Future Challenges

Several SDR projects have been started over the past several years to improve upon the existing structure of the SDR. More recently, the GNU radio project uses primarily the Universal Software Radio Peripheral (USRP) along with an USB 2.0 interface, a FPGA and a high-speed set of analog-to-digital –to-analog converters, combined with reconfigurable free software. Its sampling and synthesis bandwidth is a thousand times that of PC sound cards, which enables wideband operation. Another SDR project that is currently in the development is the HPSDR (High Performance Software Defined Radio) project that uses a 16-bit 135 MSPS analog-to-digital converter that provides performance over the range of 0 to 55 MHz comparable to that of a conventional analogue HF radio.

Among the SDR security threats, the download and activation of malicious software is considered the most important challenge. Many research contributions have provided a broad range of technological options in dealing with this problem, some of which could be adopted by the industry and regulators. In most cases, the described protection techniques may require a complex certification procedure, which guarantees the trust and reliability of the software (eg. waveforms) and hardware (SDR platform). A certification authority would be responsible for making the certified waveforms with the digital signatures. The SDR platform should have an authentication mechanism (as described above), which validates the downloaded software modules (Baldini et al., 2012). In this area, the biggest challenge is to manage the complexity of the certification and software download process, which can become overwhelming as the number of waveforms and hardware platforms increase.

Another significant challenge for the deployment of security protection techniques in SDR platforms are the real-time requirements for the signal processing. The SDR hardware and waveform code must be fast enough to support the signal input/output rate. Security protection techniques may incur a significant performance penalty in terms of increased runtime overhead and increased memory usage. The performance impact of security protection techniques is an open research area, which requires further study (Baldini et al., 2012). A compromised SDR can

create harmful interference in unauthorized bands to primary and secondary users. The ACU (automatic and calibration unit) can potentially become an effective solution to enforce the spectrum regulation policies in the SDR device. The spectrum policies can be defined in configuration files accessed by the ACU on the basis of its geographical position. The ACU can also be implemented with tamper-resistant hardware and the configuration sets of the spectrum regulations can be installed in the production/certification phase. An alternative or complementary approach is based on a network spectrum monitoring system to check the spectrum environment for malicious attackers, but this solution would not be practical because it would require a considerable deployment effort.

Given the advantages of SDR, research has been accelerating at an astounding pace. The primary challenges are performance limitations imposed by the current generation of underlying hardware and software architectures. The size, weight, performance and power consumption of current digital processing hardware, such as FPGAs and DSPs are inadequate for fully realizing the potential of a software-defined radio (Palkovic et al., 2012). As a result, SDR research is ongoing in all areas: hardware solutions, algorithms, software implementations, and applications. All these areas are interrelated and tightly coupled, so it's unlikely that a solution in a single area will enable the ultimate SDR vision: a radio consisting of nothing more than an antenna, analog-to-digital converter, and a digital processor. Advancing the SDR state of the art will require cross-disciplinary research and engineering.

Conclusion

Software defined radio (SDR) technology implements some of the functional modules of a radio system in software enabling a higher degree of flexibility. SDR devices may be reconfigured dynamically via the download of new software modules. Malicious or malfunctioning downloaded software presents serious security risks to SDR devices and networks in which they operate. This paper provides an overview of the security threats and related protection techniques for SDR devices.

SDR can act as a key for enabling technology for a variety of other reconfigurable radio equipments. While SDR is not required to implement and of these radio types, SDR technologies can provide these types of radio with the flexibility necessary for them to achieve their full potential, the benefits of which can help to reduce cost and increase efficiencies in other related radio systems such as adaptive radio or the cognitive radio. Clearly, SDR has a wide variety of uses and applications and can truly revolutionize the field of wireless radio technology. Despite the existing range of threats, vulnerabilities, mitigation and protection techniques, the viable development of SDR requires further integration between the breadth of activities involved in spectrum regulation, security and certification.

References

[1] Baldini, G., M. Street, G. Godor, R. Leschhorn, A.R. Biswas, and T. Sturman. "Security Aspects in SDR and Cognitive Radio Networks: A Survey and A Way Ahead" *IEEE Xplore*. N.p., 2012. Web. 10 May 2013. <*http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5742780*>.

[2] Hill, Raquel L., Suvda Myagmar, and Roy Campbell. "Threat Analysis of GNU Software Radio." N.p., n.d. Web. 10 May 2013. <*http://www.omidi.iut.ac.ir/SDR/2007/WebPages/07_GNU/pdf/threat_wwc05.pdf*>.

[3] Palkovic, M., Raghavan, P., Min Li, Dejonghe, A., Van Der Perre, L. and Catthoor, F., "Future Software-Defined Radio Platforms and Mapping Flows," *Signal Processing Magazine, IEEE* , vol.27, no.2, pp.22,33, March 2010. < *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5438968&isnumber=5438947*>.

[4] "Software Defined Radio - Benefits" Wireless Innovation. N.p., n.d. Web. <*http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf*>.

[5] "What Is Software Defined Radio?" Wireless Innovation. N.p., n.d. Web. <*http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf*>.