SYSTEM THREAT ANALYSIS FOR HIGH ASSURANCE SOFTWARE DEFINED RADIOS

David Murotake, (SCA Technica, Inc. Nashua NH, USA; david.murotak@scatechnica.com)
Antonio Martin (SCA Technica, Inc., Nashua NH, USA; tony.martin@scatechnica.com)

ABSTRACT

Software defined radios (SDR) are rapidly becoming a mainstream technology for commercial, civil and military mobile terminals and wireless access points. Moreover, "wireless Internet" waveforms with weak security designs, such as IEEE 802.11 Wireless Fidelity (WIFI), a form of wireless local area network (WLAN), are becoming increasingly prevalent. Because WIFI enabled laptop computers and personal digital assistants (PDA) combine a radio and computing interface, they provide a useful case study examining potential dangers posed by hackers to networks of software defined radio terminals.

Supported in part by a US Air Force Small Business Innovation Research (SBIR) contract, we have conducted a system threat and requirements analysis for software defined radios (SDR) and wireless terminals (including non-SDR) employing WIFI. The study concludes that WIFI networks, including ubiquitous IEEE 802.11(b) "WIFI hot spots", are subject to "blended attack" methods combining coordinated attacks on the radio and computer. The blended attacks threaten the integrity of a SDR radio system, the components of which are shown in Figure 1.

This paper surveys the tools and blended attack methods used by hackers to attack and exploit WIFI equipped mobile terminals. The paper then examines parallels between the WIFI scenario and similar threats to software defined radio terminals and networks by wireless hackers. We conclude by proposing requirements and architectures for high assurance SDR.

1. INTRODUCTION

As the world order changed during the last two decades, large numbers of highly trained electronic warfare professionals and mathematicians became "displaced" as technically sophisticated armies and their radio reconnaissance battalions were demobilized. Can this explain the surge of well designed wireless hacking tools and equipment now available? Some of these tools are freely distributed software which can be downloaded from the Internet? Other tools, including enterprise-grade hardware and systems, can be purchased online. These sophisticated tools, which enable the "blended attacks" shown in Table 1, include:

- "Stumblers" which allow wireless hackers to explore the network characteristics of wireless base stations and mobile terminals
- "Sniffers" which intercept, display, and store data being transmitted over the network
- "Crackers" which break encryption codes, such as Wired Equivalent Protection (WEP) and network access codes for GSM.

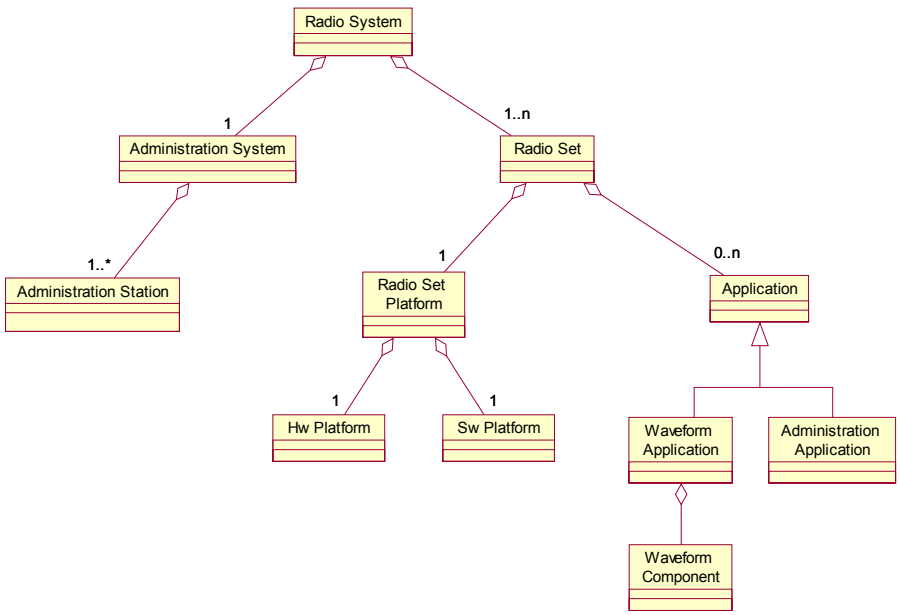

Figure 1. SDR Components. (SDR Use Cases – OMG swradio/2003-05-02)

Table 1. Blended attack methods usable against SDR. ("Security Threats & Requirements; 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects", examples by Murotake)

Threat Category	Attacks on Radio Interface	Attacks on Other Parts of System
Unauthorized access to data	Example: Use of "stumbler" SW to detect WIFI hot spots, identify wireless access point (WAP) characteristics. Use of "sniffer" SW to intercept data.	Intruders may eavesdrop signaling data or control data on any system interface, whether wired or wireless. This may be used to conduct other attacks on system.
Threats to integrity	Hacking encryption codes using SW e.g. WEPCRACK. Planting malicious SW in radio component.	Intruders may modify, insert, replay or delete signaling or control data on any system interface, whether wired or wireless. Planting malicious software on computer.
Denial of service	Intruders may prevent user traffic, signaling data and control data from being transmitted on the radio interface, e.g. jamming.	Intruders may attempt to prevent user traffic by a coordinated transmission of large numbers of packets by means of a virus infection of a network..
Unauthorized access to services	The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication.	Intruders may impersonate a user to utilize services authorized for that user.
Repudiation	Repudiation of user traffic origin: A user could deny that he entered the network (no access logs).	Repudiation of user traffic origin: A user could deny that he sent user traffic.

"Blended" attacks (Table 1) combine five attack methods (unauthorized access to data, threats to integrity, denial of service, unauthorized access to services, and repudiation) against both the radio and computing interfaces [1] of a wireless mobile terminal. Special techniques allow the hacker to jam encrypted WIFI networks, making normal access points "invisible" to WIFI terminals and allowing hackers to use their own access points to seize control of networks. Even the "victims" of hacking today appear to be "willing victims". "Rogue" WIFI networks, installed by employees despite corporate policies to the contrary, threaten the integrity of over 30% of corporate networks.

2. SYSTEM VULNERABILITIES

The *Radio System* components model shown in Figure 1 can be further detailed with security vulnerabilities, as shown in Figure 2 [2]. The vulnerabilities affect both hardware and software in the *Radio Set* and the *Administration System* components. Hackers can exploit security vulnerabilities by blending the five basic attack methods, shown in Table 1, against both the radio and computer interfaces.

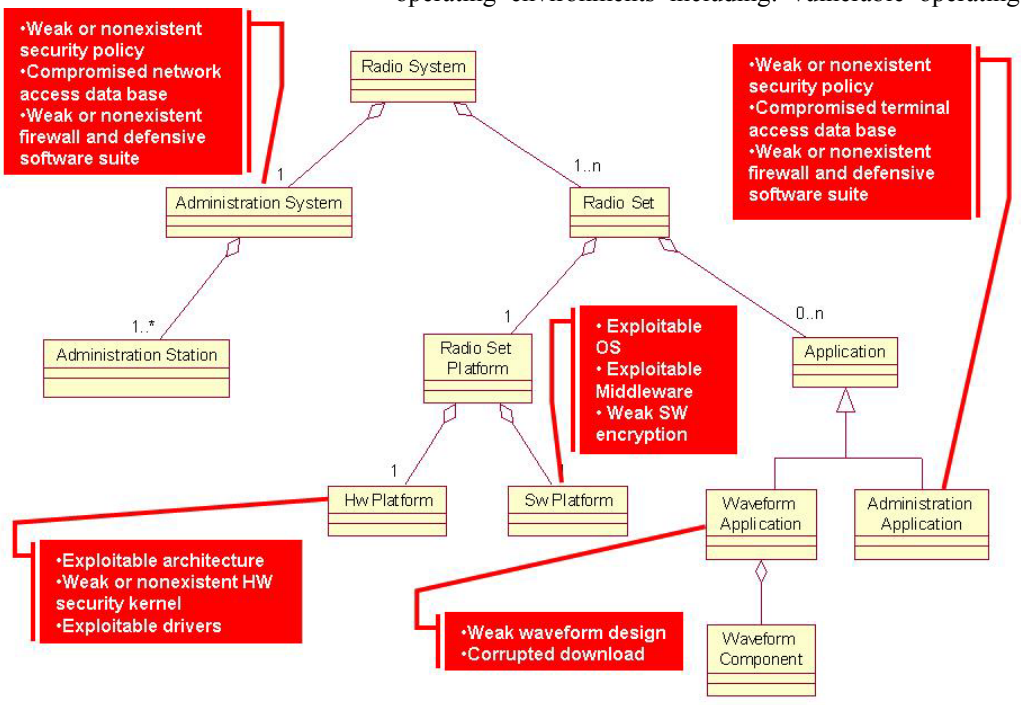

Figure 2. SDR System Vulnerabilities. (Murotake, "System Threat Analysis Case Study for Software Based Communications", OMG Software Based Communications Workshop, September 2004)

In the *Radio Set*, vulnerabilities affect the stability and integrity of both the *Radio Set Platform* hardware and software, and the *Radio Set Applications*.

Using blended attack methods, hackers can exploit both hardware and software vulnerabilities within the *Radio Set*. Vulnerabilities related to hardware may result from a variety of factors, including: lack of a hardware based security kernel (such as an encryption engine); lack of hardware firewall; and exploitable hardware device architectures with corresponding exploits in the device drivers.

Software vulnerabilities may include exploitable operating environments including: vulnerable operating

system (OS) and middleware; weak software based encryption engine; use of waveform(s) with weak security design; corrupted waveform or application download; weak or nonexistent anti-virus and firewall software; and weak or nonexistent security policy.

A threat scenario for SDR using a Wireless LAN (WLAN) waveform download to enter a WLAN is shown in Figure 3. In this scenario, the victim mobile terminal (laptop) and access point can be subjected to a number of blended attack methods by a hacker equipped with a mobile terminal card, a separate access point, or both.

Figure 3. Threat scenario for WIFI. (Murotake)

In the scenario above, the following types of attack against the SDR are possible, since the standard IEEE 802.11(b) system does NOT employ strong authentication, such as the IEEE 802.1X standard:

• Attack vs unencrypted WIFI infrastructure
– Use "stumbler" SW to detect wireless network, obtain wireless access point (WAP) control information
– Enter network and use "sniffer" SW to obtain unauthorized access to data
– Install malicious software (malware) on PC to obtain unauthorized access to computer information

• Attack vs WEP encrypted WIFI
– Use stumbler SW to detect WAP control information
– Use hacking software, e.g. WEPCRACK, to break WEP encryption code. Enter network and use "sniffer" to obtain unauthorized access to data
– Use Denial Of Service (jamming) attack on target WAP. Force users to turn off encryption. Users automatically switch to Hacker's WAP on another channel.
– Install malicious software *(malware*) on PC to obtain unauthorized access to computer information

• Attack vs WPA encrypted WIFI
– Use stumbler SW to detect WAP control information
– Use Denial Of Service (jamming) attack on target WAP. Force users to turn off encryption. Users switch to Hacker's WAP on another channel
– Install malicious software (malware) on PC to obtain unauthorized access to computer information

A successful attack usually results in the following (undesired) impacts on the mobile terminal and access point, highlighting the importance of protecting the platform, and not just the data:

- The upload and download data being passed between mobile terminal and access point are compromised.
- The radio and network configuration software in the SDR are corrupted.
- A keystroke or packet repeater (a type of "Trojan Horse" software) is successfully planted on the host laptop or PDA.

3. ASSURANCE ARCHITECTURE

The best defense approach to a blended attack is a "multi-layered" defense, or defense in depth [3]. That is, a combination of methods, instantiated in both hardware and software, is implemented in both the terminal and access point, in both design and verification of high assurance systems. In the most secure high assurance systems, a hierarchical architecture is employed, where multiple layers provide specific, well-defined security mechanisms that can be used by higher levels.

A high assurance security mechanism must be: (i) always invoked, (ii) non-bypassable, (iii) tamperproof, and (iv) verifiable. Security features recommended by the SDR Forum [4] for SDR's include:

1. Security Policy Enforcement and Management
2. Information Integrity
3. Authentication and Non-repudiation
4. Access Control
5. Encryption and Decryption Services
6. Key and Certificate Management
7. Standardized Installation Mechanisms
8. Auditing and Alarms

9. Configuration Management
10. Memory Management
11. Emissions Management
12. Computer Security (virus scanning and firewalls)

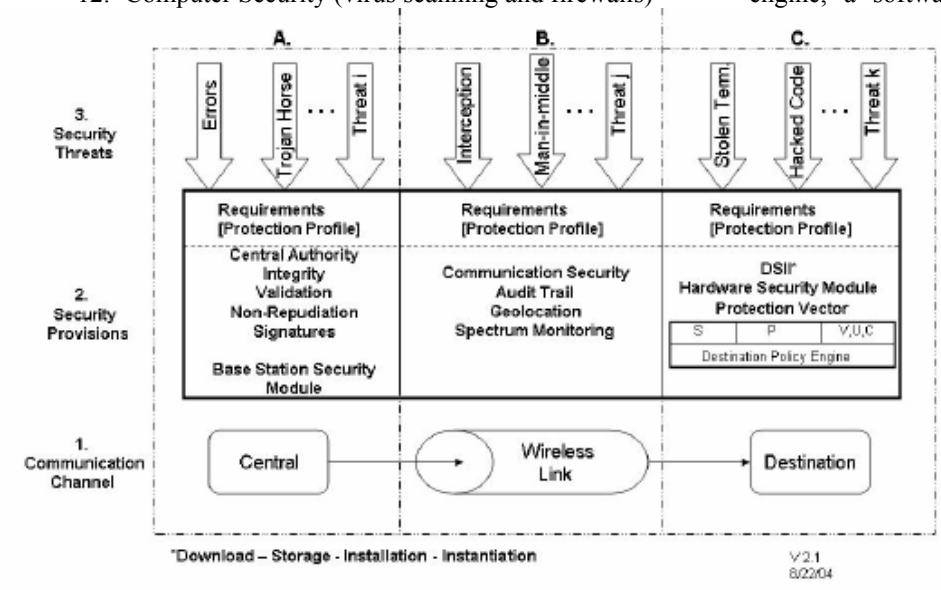

Figure 4. SDR Forum Security Reference Architecture. (SDR Forum DL-SIN, SDRF-02-W-0005-V030)

Figure 4 shows the SDR Forum's security reference architecture model. The model displays the requisite "mutli-layered" character needed to provide the defense in depth against blended attacks.

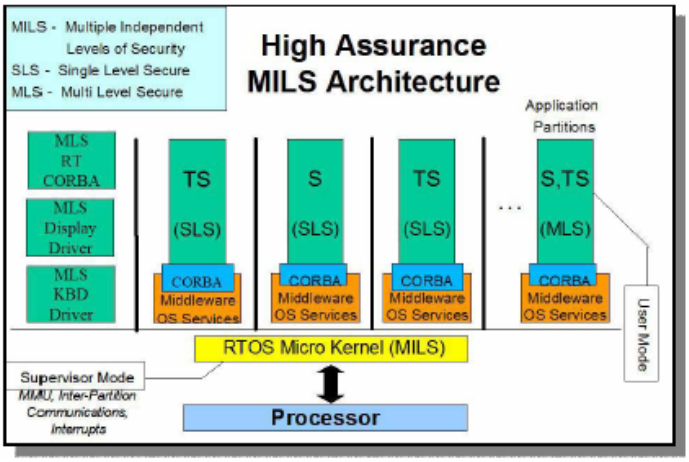

Figure 5. High Assurance MILS Architecture. (Alves-Foss et al, 2004)

The model also suggests use of a hardware security module. Secure download, storage, installation and instantiation (DSII) of waveforms and other applications is also shown.

Security can be enhanced by incorporating a strong hardware security kernel within the SDR. By using an FPGA or ASIC which includes a hardware encryption engine, a software radio micro-kernel and a secured programming gateway, hackers will have a greater difficulty in corrupting the system software and applications.

Another approach used in high assurance systems is the use of robust operating environments and middleware. One method is in the use of high-assurance software components, such as real time operating systems (RTOS) and object request brokers (ORB). One way of doing this is by selecting components which provide an Common Criteria (CC) Evaluated Assurance Level (EAL) of 5 or above (on a scale of 1-7, EAL 7 has the highest level of security). An "extreme" example of this is a *multiple independent levels of security* (MILS) architecture, as shown in Figure 5. The MILS operating environment employs a real-time, partitioning micro-kernel RTOS and a MILS (ORB), rated at EAL 7.

4. INTEGRATED BIOMETRICS

One method of enhancing end to end assurance in SDR is through the use of integrated, multi-mode biometric systems to enforce certain aspects of the security policy. Biometric techniques, which can be easily incorporated into SDR mobile terminals, include fingerprint scanners and speaker verification systems, as shown in Figure 6.

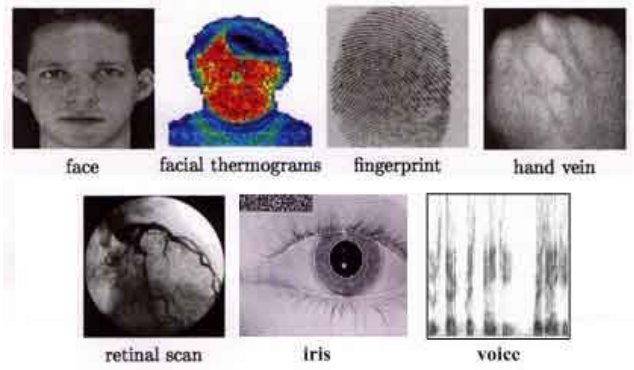

Figure 6. Biometric techniques (Sonetech)

Biometric systems themselves must protect themselves against hacking and other forms of attack [5]. Figure 7

shows the vulnerable points (red lines) of a typical biometric sensing system.

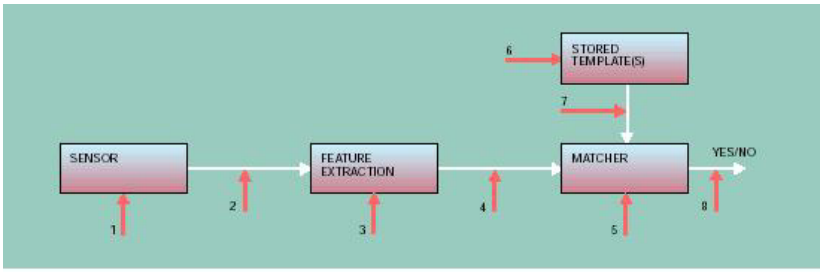

Figure 7. Vulnerabilities of a biometric sensor. (Ratha)

Because the integrated biometric system may employ reconfigurable signal processing algorithms for feature extraction and matching, the same types of programming core frameworks (CF) and application programming interfaces (API) may be developed for integrated biometric systems. Thus, the high assurance SDR software component model may look like Figure 8:

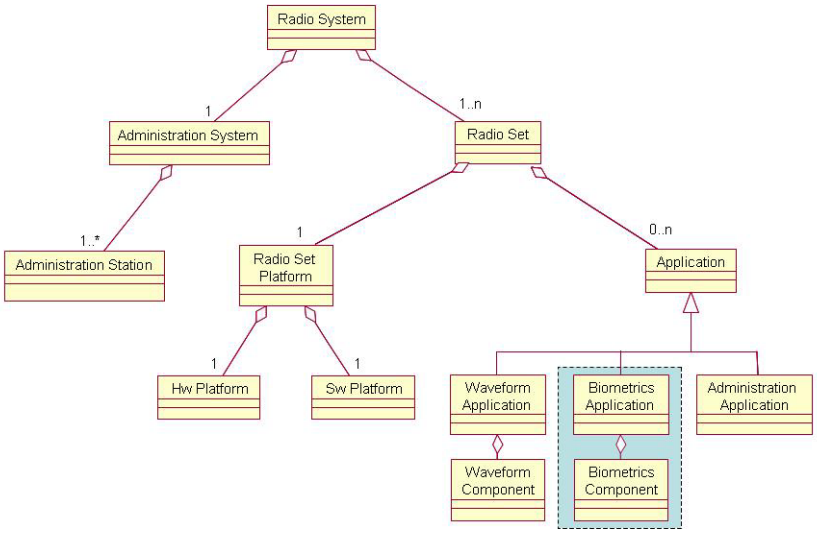

Figure 8. SDR with integrated biometrics.

5. CONCLUSIONS

SDR security is a *system level* problem. To design a system with appropriate defenses, one must first understand the system threat and defensive requirements. Hackers use blended attacks against both the radio and computer layers of the SDR. To defend against the blended attack requires a multi-layered defense-in-depth which protects both the mobile clients and servers. This includes the mobile radio, mobile host, server radio, and server host components of an SDR network. The security architecture must ensure:

- Integrity of: software applications and downloads including download, storage, installation and instantiation (DSII)
- Integrity of the reconfigurable platform against blended attacks by employing defensive layers (firewalls, intrusion detection, virus protection)
- Integrate biometric and radiometric assurance techniques
- Employ trusted architecture, high assurance operating systems and middleware

Integrity of the analog signal or data from exploitation/compromise

6. REFERENCES

[1] "Security Threats and Requirements; 3GPP TS 21.133 V4.1.0 (2001-12); 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects"

[2] Murotake, "System Threat Analysis Case Study for Software Based Communications", OMG Software Based Communications Workshop, September 2004

[3] Jim Alves-Foss, Carol Taylor, and Paul Oman, "A multi-layered approach to security in high assurance systems", Proceedings of 37th Hawaii International Conference on System Sciences – 2004".

[4] "Security considerations for operational software for software defined radio devices in a commercial wireless domain", SDR Forum DL-SIN, Document SDRF-02-W-0005-V030.

[5] Ratha et al, "Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40:3, 2001