UPDATED SYSTEM THREAT AND REQUIREMENTS 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

During SDR'04, we provided the results of a case study of the effect the download of a waveform with a weak security design, such as IEEE 802.11 Wireless Fidelity (WIFI), into a software defined radio (SDR). Wirelessly networked computers, interfacing with the Internet via WIFI, GSM, and other vulnerable waveforms, are becoming increasingly prevalent, and provide a useful case study highlighting the potential dangers posed by hackers to networks of software defined radios. Within the past year, our report on the threats posed by WIFI and SDR has had wide impact on the SDR security community.

Supported in part by a US Air Force Small Business Innovation Research (SBIR) contracts, we have conducted a system threat and requirements (STAR) analysis for software defined radios and wireless computers employing WIFI, commercial waveforms, and other waveforms. The study concludes that numerous commercial wireless networks, and other wireless networks with certain characteristics, are subject to "blended attack" methods combining coordinated attacks on the radio and computer interfaces.

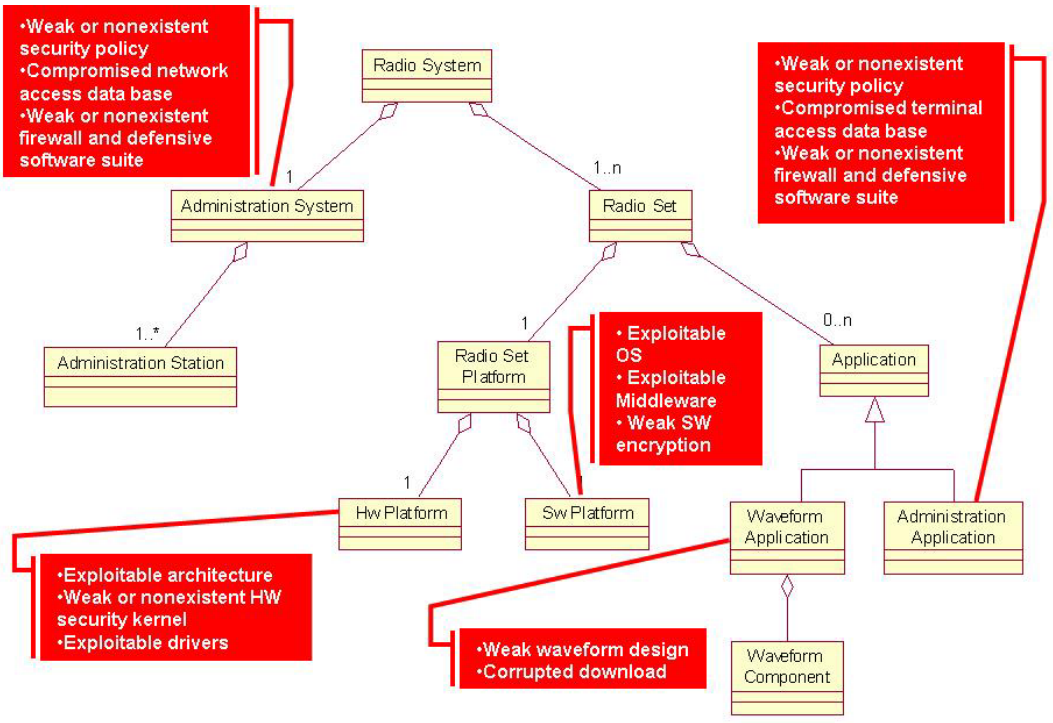
Building on the results of last year's paper, we survey various approaches which may help to mitigate the threat posed by blended hacking attacks on software defined radio terminals and networks. We also recommend a security architecture approach for consideration by the SDRF.

1. INTRODUCTION

SDR is a key technology for Joint Tactical Radio System (JTRS), and may provide enabling technologies for Project SAFECOM and other public safety radio systems. However, recent studies indicate that wireless Internet access waveforms, such as IEEE 802.11 Wireless Fidelity (WIFI), are susceptible to wireless hacking [1] [2] [3].

"Blended" attacks against commercial wireless interfaces have been studied by standardization groups such as the 3rd Generation Partnership Program [4]. Five attack methods (unauthorized access to data, threats to integrity, denial of service, unauthorized access to services, and repudiation) can be used against both the radio and computing interfaces of a wireless mobile terminal. These methods do not only pose threats to 3G wireless systems. The threats identified in [4] apply equally against reconfigurable systems which interface wirelessly, either with private networks or the public Internet. This includes the class of software of defined radio terminals and networks. To address these threats, the Joint Tactical Radio System (JTRS) recorded Change Proposal 295, "Exposed Black Side" in January 2005 [5].

Figure 1. Potential vulnerabilities of SDR System, from [3].



2. SYSTEM VULNERABILITIES

The SDR vulnerabilities shown in Figure 1 were described in last year's paper [3]. The vulnerabilities affect both hardware and software in the *Radio Set* and the *Administration System* components. An outstanding treatment of these threats, their relative significance, and impacts on commercial waveforms can be found in [4]. For all intents and purposes, if a commercial network waveform (including WIFI, GSM with GPRS, 1XRTT, etc.) are programmed into a SDR, the SDR becomes vulnerable to all threats described in [4] with few exceptions. Hackers can exploit security vulnerabilities by blending five basic attack methods as described in [3] and [4].

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 (soft) operating systems (OS) and middleware (Figure 2); 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. Consumer operating systems, BIOS and Internet applications have many exploitable features, and are difficult to protect even with constant updates and the addition of software protection (e.g. anti-virus and anti-spyware applications).. 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.

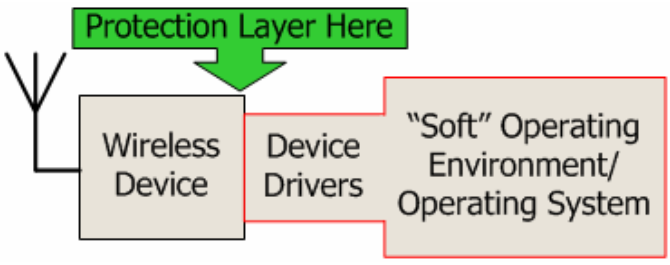


Figure 2 – A hackable, wirelessly connected device with exploitable device drivers and "Soft" operating environment.

As complexity of systems grow, the number of exploitable features increases. This becomes particularly dangerous in the wireless communication area since an exploitable "Soft" operating environment can be directly touched by a Wireless device. This allows a hacker to touch / exploit weaknesses within the operating system, operating processes, device drivers and possible weaknesses in the wireless device; such attacks can include packet injection, malformed data packets and buffer overflow exploits. Security layered on a "Soft" operating environment will not help when device drivers can be exploited, offering root level access to the target environment. These "Soft" environments include the various Linux and Windows, etc, operating systems where security issues are found on a daily basis. To help prevent such attacks, a protection layer must be wedged between the Wireless Device and the "Soft" operating environment.

3. ASSURANCE ARCHITECTURE

The best defense approach to a blended attack is a "multi-layered" defense, or defense in depth [6]. That is, a combination of methods, implemented 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 [7] 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, firewalls)

The security model in [7] model also suggests use of a hardware security kernel. 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 robust (hard) operating environment and a secured programming gateway, hackers will have a greater difficulty in corrupting the system software and applications.

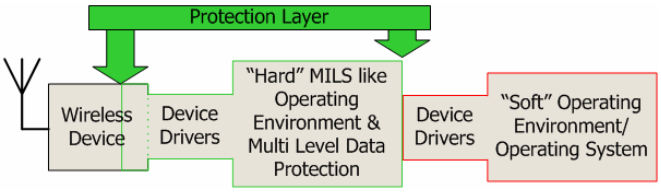


Figure 3 "Soft" systems can be protected by using an in-line "hard" kernel (strong protection profile). An example of such a protection layer is the High Assurance Wireless Computing System (HAWCS™) for consumer/commercial wireless.

To protect a wireless system which employs "soft" consumer operating systems and applications and guarantee secure eCommerce, the defensive layers must span a portion of the wireless device and act as an intermediary "shield" for a vulnerable host. Figure 3 shows an example of a multi-layered protection environment that separates the wireless device and public Internet interface from the host platform, acting as a proxy to the network and defensive mechanism for the "Soft" host. In this way, all communication must pass through the Protective Layer via a "Hard" MILS-like operating environment acting as a buffer to hacking attempts on the host system. The Protective Layer not only is responsible for protecting the host but it also can function in protecting a reconfigurable Wireless Device, Network Infrastructure and other Hosts in the network from a compromised, attached terminal. A compromised or infected host can be prevented from performing a DOS on the network, reconfiguring the Wireless device, or infecting other Hosts though trusted communication channels. Such an approach is needed in consumer and commercial systems to protect eCommerce applications on wireless laptops, PDA's and "smart" phones.

The High Assurance Wireless Communication System (HAWCS™) under development for SBIR AF03-098 Phase II employs a patent-pending combination of robust hardware and software components leveraging COTS software from Green Hill Software, Interpeak, Objective Interface Systems and Harris, and COTS hardware from Xilinx (Virtex 4) and General Dynamics (Advanced INFOSEC Machine). HAWCS™ is designed to safeguard consumer and commercial SDR's and wireless computing systems, and can be used to address JTRS CP295 when used in combination with appropriate encryption systems.

Finally, HAWCS™ can be implemented as components of a software waveform, usually without impacting the existing waveform interface standards. The HAWCS™ "augmented" waveform requires certain hardware resources on the SDR or wireless computing platform, such as a general purpose processor (GPP) with a hardware memory management unit (MMU), memory, FPGA gates, etc.. However the result is an SDR platform or wireless computer which is more secure against hackers, especially when using "weak" waveforms in combination with "soft" host environments.

4 CONCLUSIONS

SDR security is a *system level* problem. To design a system with appropriate defenses, especially if a host platform employs "soft" consumer operating environments, one must employ a comprehensive, in-depth system which includes a robust "hard" protection layer which interposes itself between wireless and Internet hackers, and the host platform. The military is developing a technology called Multiple Independent Levels of Security (MILS) which addresses this matter. Another technology, HAWCS™, is under development to address this issue for consumer and commercial platforms. The protection layer must ensure:

- Integrity of: software applications including download, storage, installation and instantiation (DSII)

- Integrity of the reconfigurable platform(s) against blended attacks from wireless and Internet attackers by employing in-depth defensive layers (robust operating environments, firewalls, intrusion detection, virus protection)

5 REFERENCES

[1] J. Walker. "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 00/362, IEEE 802.11 Committee, March 2000, DocumentHolder/0-362.zip, http://grouper.ieee.org/groups/802/11/Documents/

[2] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." http://www.issac.sc.berkley.edu/issac/wep-faq.html.

[3] D. Murotake & A. Martin, "System threat analysis for high assurance software defined radios", Proceedings, SDR'04 Technical Conference, SDR Forum, Phoenix AZ, November 2004.

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

[5] CP 295, "Exposed Black Side", Joint Tactical Radio System (JTRS) Change Proposal (CP), submitted 26 January 2005. Website: http://jtrs.army.mil

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

[7] "Security considerations for operational software for software defined radio devices in a commercial wireless domain", SDR Forum DL-SIN, Document SDRF-02-W-0005-V03

UPDATED SYSTEM THREAT AND REQUIREMENTS ANALYSIS FOR HIGH ASSURANCE SOFTWARE DEFINED RADIOS

SDR Forum Technical Conference
Anaheim, California November 2005

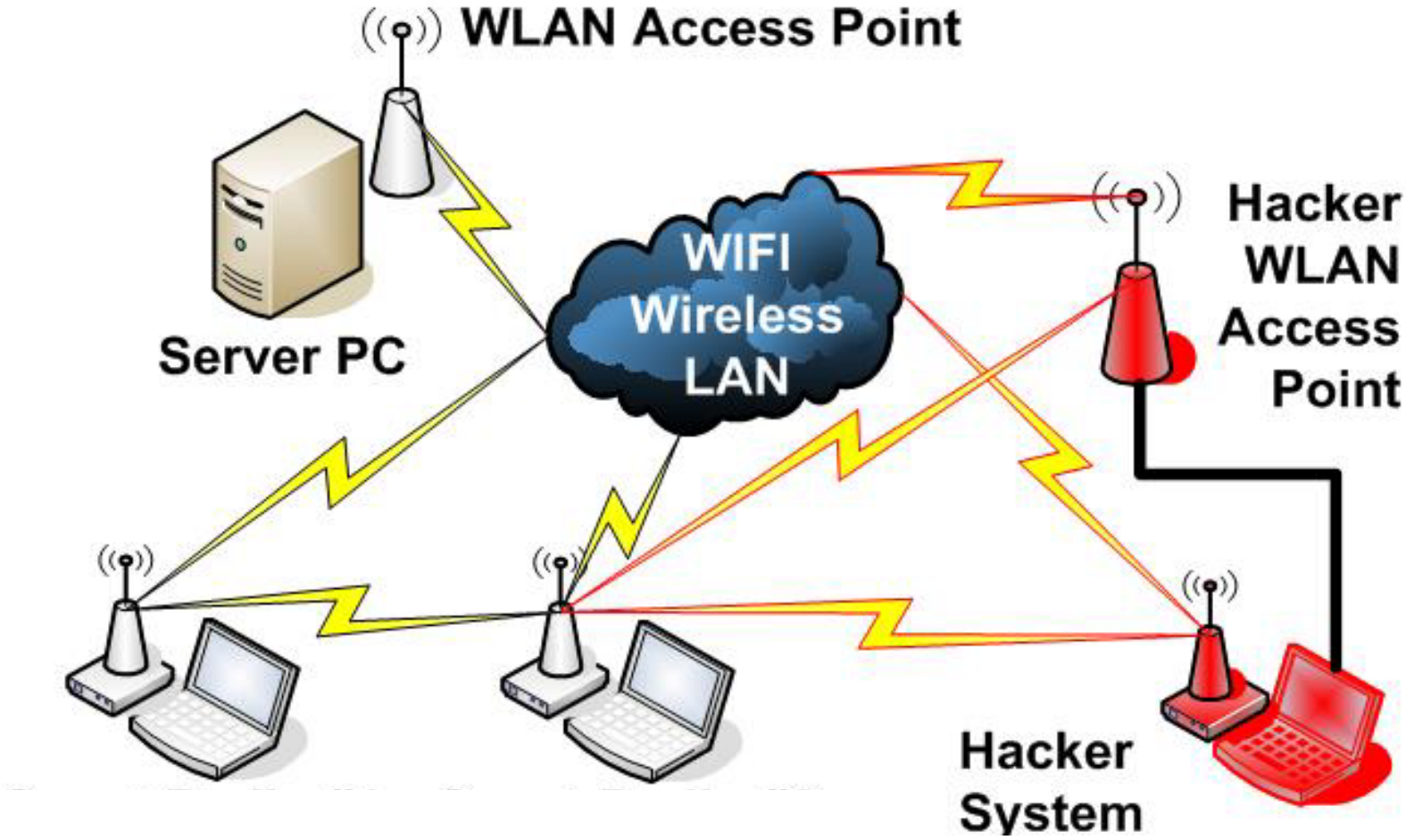
David Murotake, (SCA Technica, Inc. Nashua NH, USA; david.murotak@scatechnica.com)

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

Introduction

- SDR's intrinsically vulnerable to hacking
  - Commercial systems
  - JTRS CP 295, "Exposed Black Side"
- Threats & countermeasure requirements
  - Blended attack
  - Protection strategies
- High Assurance Wireless Computing System (HAWCS™)
  - Development progress

802.11 Blended Attack Example

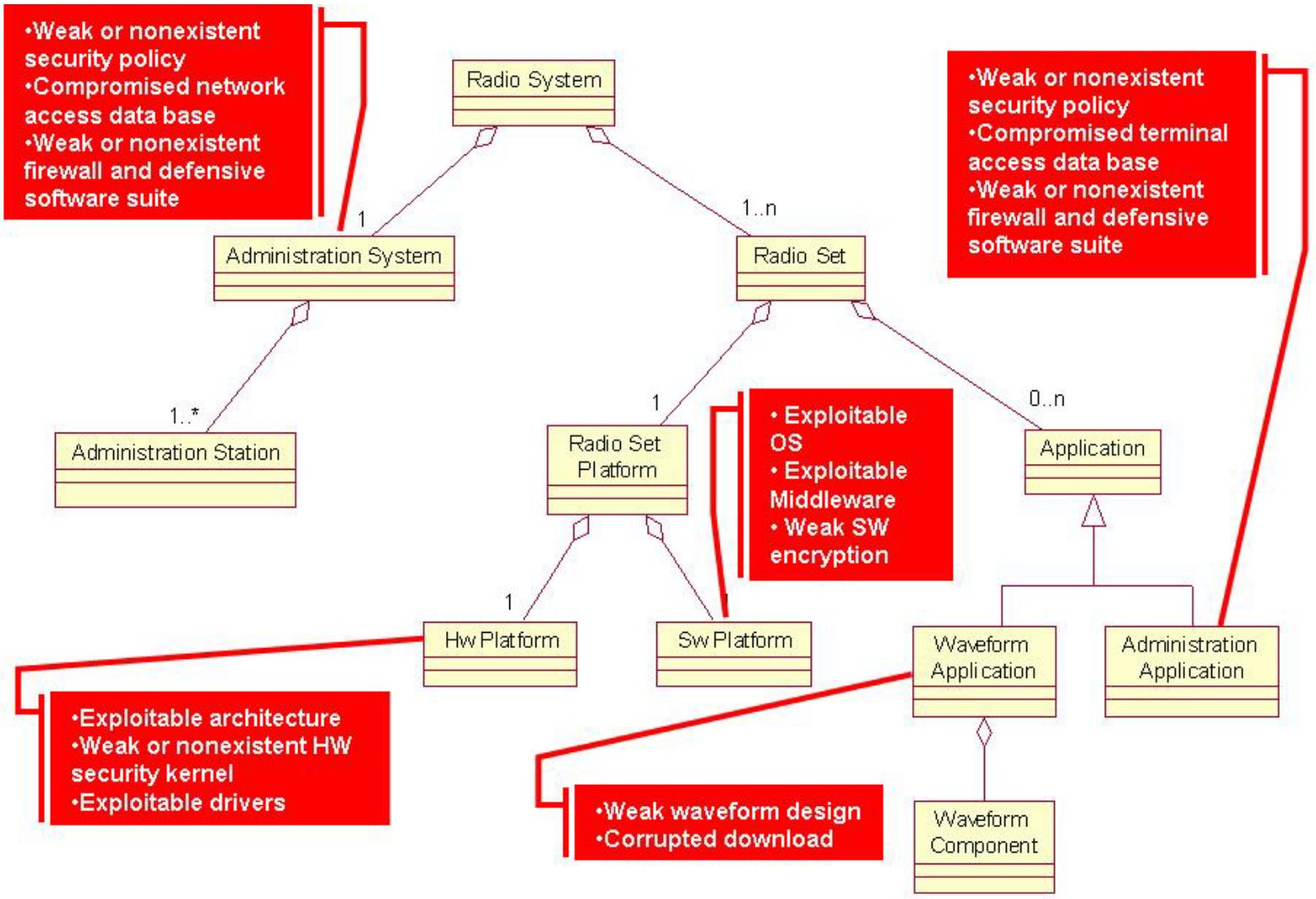


802.11 Blended Attack Example

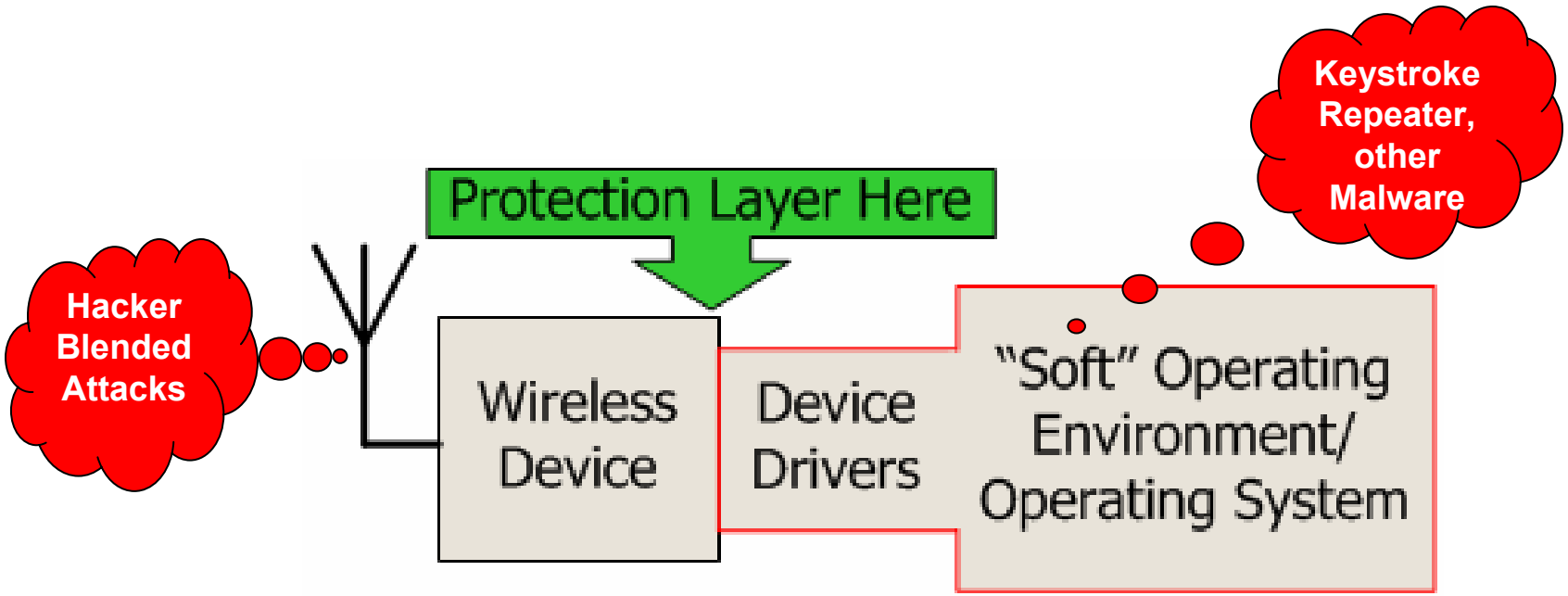
Threat Category	Attacks on Radio Interface	Attacks on Other Parts of System
Unauthorized access to data	Example: Use of "stumbler" SW to detect WIFI hot spots, identify wireless access point (WAP) characteristics. Use of "sniffer" SW to intercept data.	Intruders may eavesdrop signaling data or control 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.

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

Potential SDR Vulnerabilities



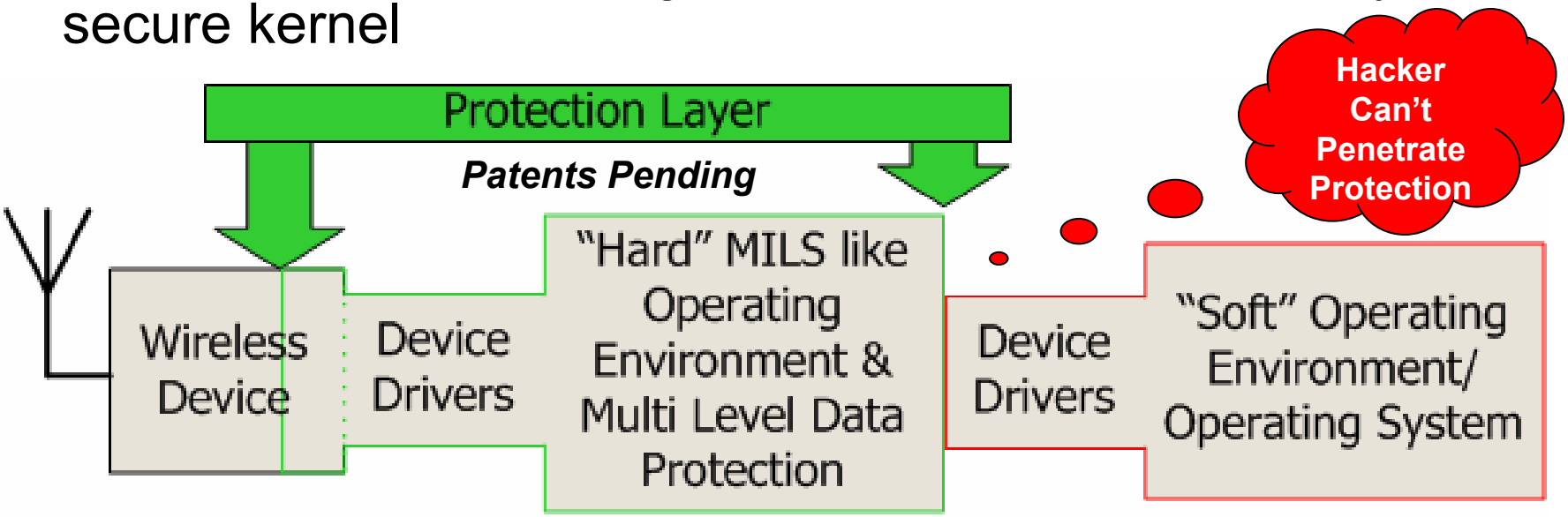
"Soft" OE (OS & Middleware)



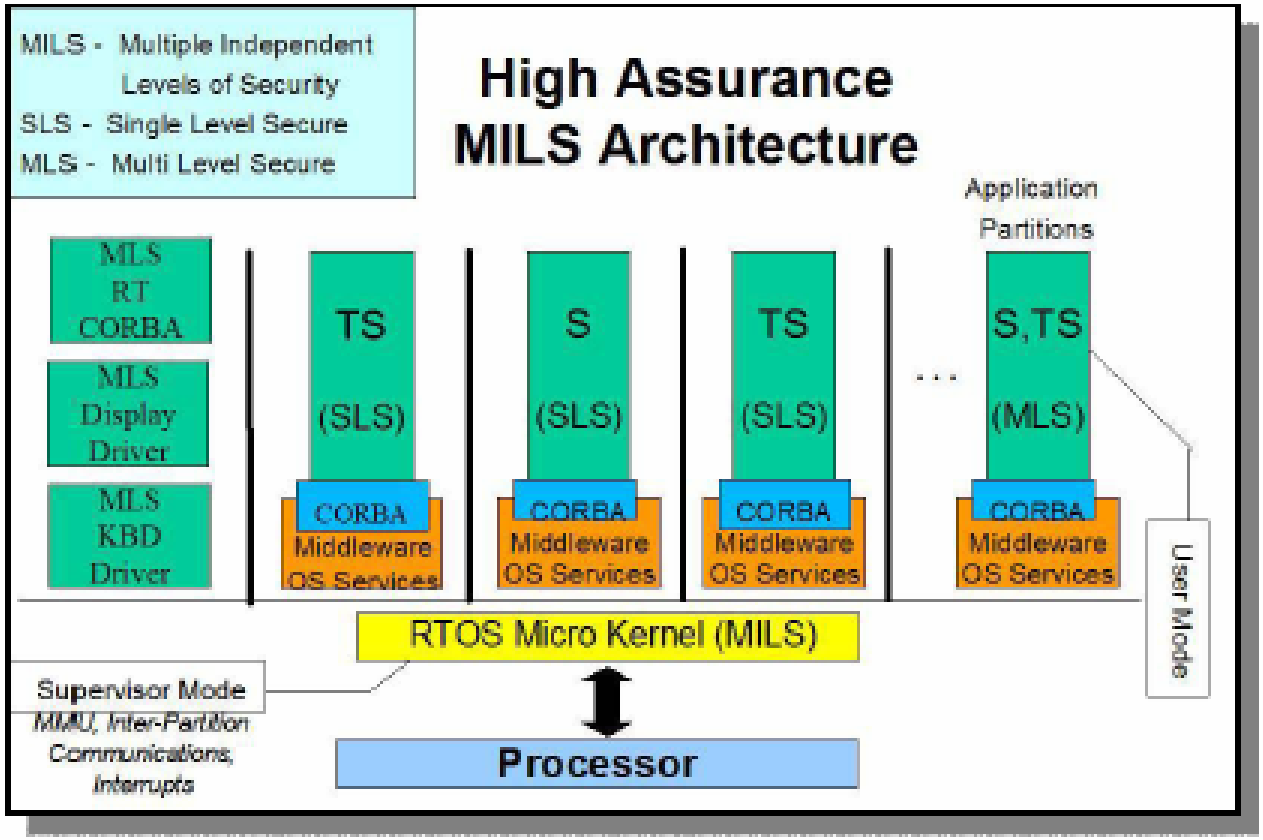
- Wireless devices supported by device drivers and BIOS hosted by "soft" OE
- This type of system is vulnerable to "blended" hacking attacks via wireless and Internet
- Viruses & malware compromise integrity of the SDR or wireless computing device (can bypass encryption)

"Hard" Layer Protects "Soft" Host

- Wireless devices (and other I/O) separated from "soft" host by a "hard" defensive layer
- "Hard" defenses must be "in-line" and must NOT permit circumvention (i.e. no "dongles" supported by soft OE)
- Wireless devices must be supported by device drivers and BIOS services based on "hard" OE
- Boot and device reconfiguration must be protected by secure kernel



High Assurance Operating Environment

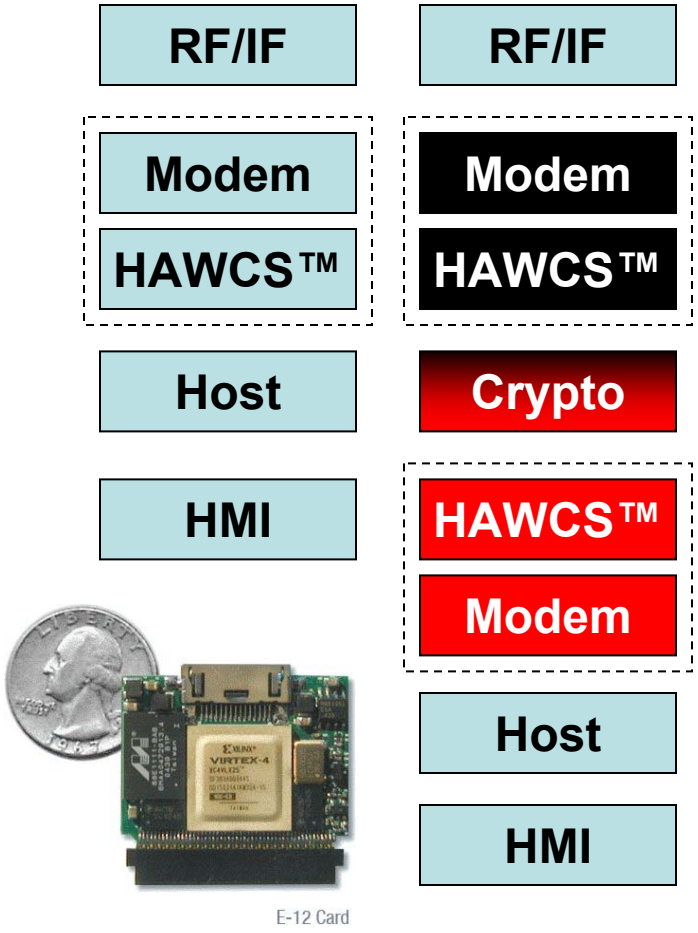


The High Assurance OE is:

(i) always invoked
(ii) non-bypassable
(iii) tamperproof
(iv) verifiable

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

High Assurance Wireless Computing System (HAWCS™)



- Hardware components
  - GPP with hardware MMU
  - Self-booting kernel
  - Security kernel
  - Can be integrated with modem hardware, e.g. FPGA
- Software components
  - High assurance OE
  - IPv6 Stack
  - Firewall software
  - Other security applications
  - Can be embedded in waveform
- Prototype being implemented on Xilinx Virtex 2 Pro
  - Transition to Virtex 4 in 2006

Summary

- Bad News: SDR has an “intrinsic” vulnerability to blended attacks (wireless + Internet)
  - Did not exist in pre-SDR communication terminals
  - Same issue affects wireless computing systems
  - JTRS CP295, “Exposed Black Side”
- Good News: The problem CAN be addressed in an affordable fashion
  - High assurance methods tailored for military or commercial implementation
  - Good progress being made on HAWCS™ test-bed (patents pending)
  - Affordable consumer/commercial solutions exist
  - Waveform component solutions possible