A HIGH ASSURANCE WIRELESS COMPUTING SYSTEM (HAWCS™) FOR SOFTWARE DEFINED RADIO

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

ABSTRACT

In 2004 and 2005, the authors provided details of wireless network threats discovered during software defined radio (SDR) threat analysis study that exposed a potentially serious flaw in the security architecture of SDR. The reconfigurable radio terminal, and the host to which it is attached, is potentially vulnerable both to exploitation and malicious reconfiguration as a result of "proximity wireless" and Internet based network attacks. These vulnerabilities extend to mobile computing devices with embedded wireless and/or wired network interfaces including wireless laptops, PDAs and Smart Phones. During the past two years, the industry has responded rapidly. The Joint Tactical Radio System (JTRS) issued Change Proposal CP295, "Exposed Black Side", in January 2005. The United States Government altered certain procurement specifications for SDR and global networks by December 2005. The Software Defined Radio Forum considered these threats during preparation of security related Recommendations in 2006.

Supported in part by Small Business Innovation Research (SBIR) contracts, a prototype of a new security architecture called High Assurance Wireless Computing System (HAWCS™) has been developed and demonstrated to information assurance experts in July 2006. HAWCS™ is a hardware-based defense-in-depth solution employing state of the art FPGAs and separation kernel technology to fortify user end-node integrity and isolates "soft" operating systems and applications from network threats. HAWCS™ can address CP295 and other potential security flaws in SDR and can be made compliant with the Software Communication Architecture.

1. INTRODUCTION

There has been considerable discussion and research in network and wireless threats to mobile platforms and software defined radios. An outstanding treatment of threats to wireless systems including SDR, their relative significance, and impacts on commercial waveforms can be found in [1]. By example, in [2] we examined the use case of a "proximity wireless" attack by a wireless hacker, using a variety of methods to attack (and defeat) both unencrypted and encrypted wireless LANs (Figure 1). The best defensive approach to a blended attack is a "multi-layered" defense, or defense in depth [3]. That is, a combination of methods, implemented in both hardware and software, is implemented throughout the end-to-end communication path if possible. As a minimum, the defensive means should encompass an endpoint (such as the mobile terminal) in the communications chain.

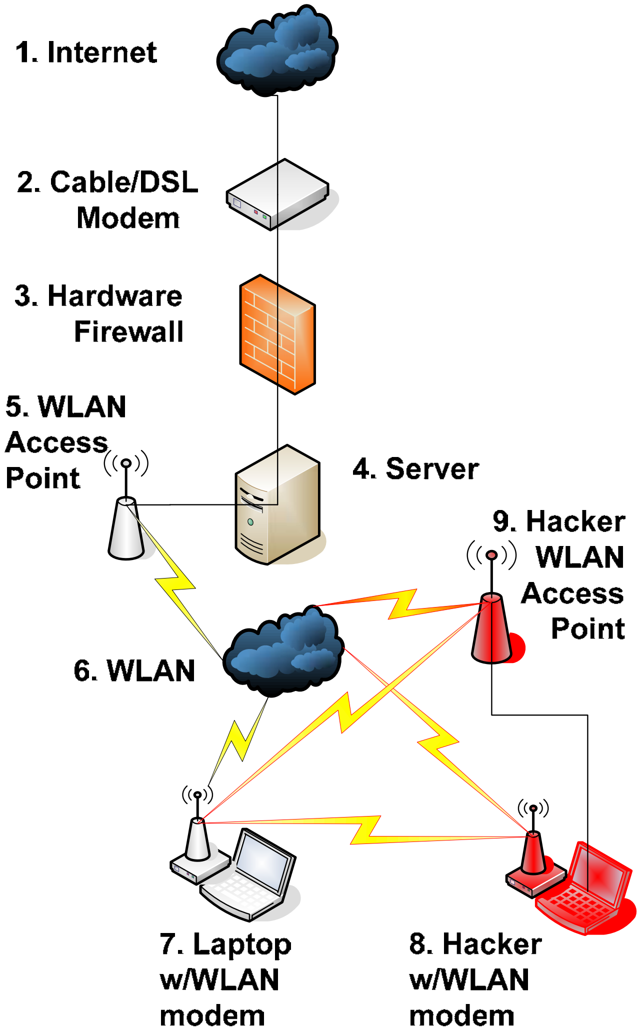
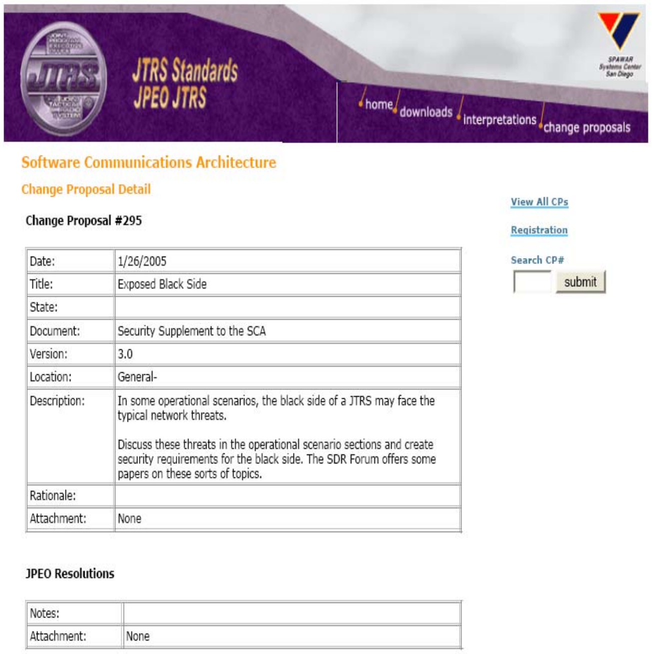


Figure 1

In 2005, the JTRS JPEO issued Change Proposal CP295 (Figure 2) stating that "in some scenarios the black side of a JTRS radio may face the typical network threats [4]. Thus to



Software Communications Architecture

Change Proposal Detail

Change Proposal #295

Date:	1/26/2005
Title:	Exposed Black Side
State:	
Document:	Security Supplement to the SCA
Version:	3.0
Location:	General-
Description:	In some operational scenarios, the black side of a JTRS may face the typical network threats. Discuss these threats in the operational scenario sections and create security requirements for the black side. The SDR Forum offers some papers on these sorts of topics.
Rationale:	
Attachment:	None

JPEO Resolutions

Notes:	
Attachment:	None

Figure 2

address this need, an appropriate high assurance defense in depth architecture should be applied to the Black, COMSEC and Red radio subsystems employing both hardware and software security measures.

2. HIGH ASSURANCE REQUIREMENTS

High assurance SDR security mechanism should be:

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

Security features recommended by the SDR Forum's Security Working Group include the following:

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

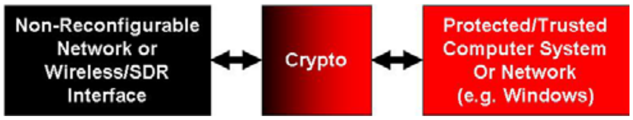

Non-Reconfigurable Network or Wireless/SDR Interface
Crypto
Protected/Trusted Computer System Or Network (e.g. Windows)

Figure 3

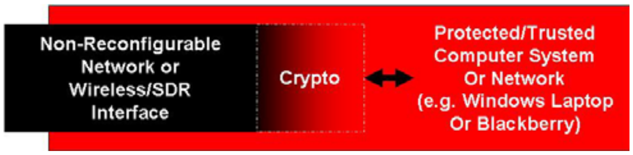

Non-Reconfigurable Network or Wireless/SDR Interface
Crypto
Protected/Trusted Computer System Or Network (e.g. Windows Laptop Or Blackberry)

Figure 4

Before embedded wireless or wired network interfaces were "built in" to communications terminals, or equivalently, before software defined radios became a reality, the use of encryption and strict adherence to Red/Black isolation were "necessary and sufficient" design practices (Figure **3**). However, when wireless or wired network interfaces became embedded in computing machines, such as laptop computers, PDAs and Smart Phones, a "flaw" in design may arise by allowing the operating system and device drivers of the "red" operating system platform to support the "black" wireless or wired network interface device (Figure 4). This "flaw" exposes possible "exploits" to wireless and network hackers, as was demonstrated during the AF03-098 Phase II SBIR program. As shown in [5] what is needed in a wirelessly enabled mobile platform or SDR is an "always invoked, non-bypassable, tamperproof and verifiable" protection layer isolating the network interface devices from the host operating system, files and applications (Figure 5).

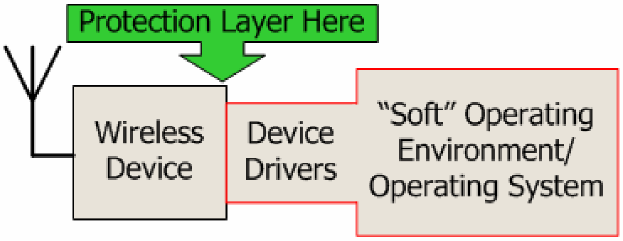


Figure 5

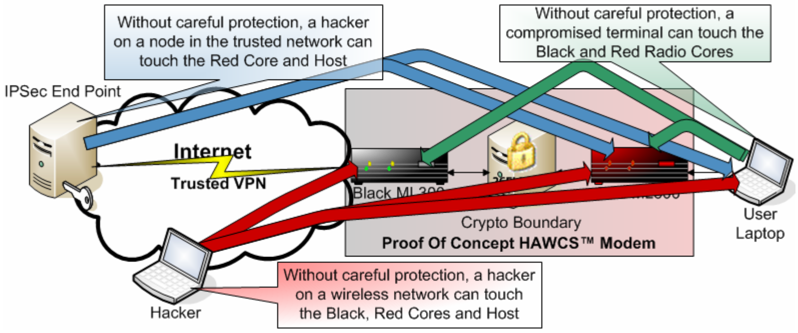
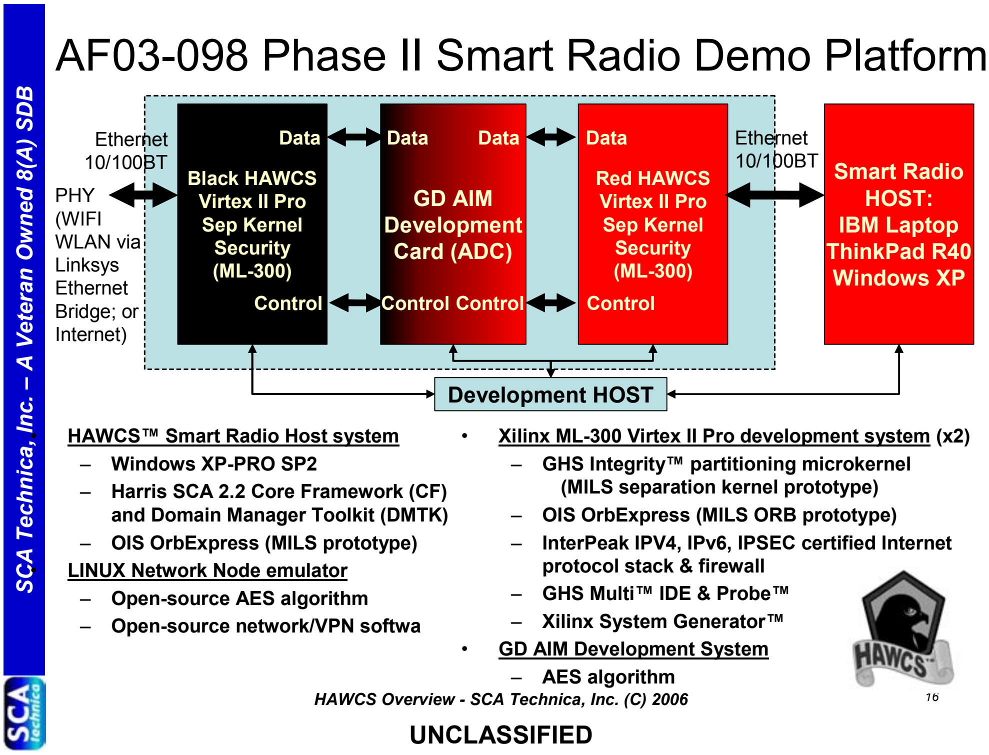

Without careful protection, a hacker on a node in the trusted network can touch the Red Core and Host
Without careful protection, a compromised terminal can touch the Black and Red Radio Cores
IPSec End Point
Internet
Trusted VPN
Black ML300
Crypto Boundary
Proof Of Concept HAWCS™ Modem
User Laptop
Hacker
Without careful protection, a hacker on a wireless network can touch the Black, Red Cores and Host

Figure 6



SCA Technica, Inc. – A Veteran Owned 8(A) SDB

AF03-098 Phase II Smart Radio Demo Platform

Ethernet 10/100BT

PHY (WIFI WLAN via Linksys Ethernet Bridge; or Internet)

Black HAWCS Virtex II Pro Sep Kernel Security (ML-300)

Data

Control

GD AIM Development Card (ADC)

Data Data

Control Control

Red HAWCS Virtex II Pro Sep Kernel Security (ML-300)

Data

Control

Ethernet 10/100BT

Smart Radio HOST: IBM Laptop ThinkPad R40 Windows XP

Development HOST

HAWCS™ Smart Radio Host system
- Windows XP-PRO SP2
- Harris SCA 2.2 Core Framework (CF) and Domain Manager Toolkit (DMTK)
- OIS OrbExpress (MILS prototype)

LINUX Network Node emulator
- Open-source AES algorithm
- Open-source network/VPN softwa

- Xilinx ML-300 Virtex II Pro development system (x2)
  - GHS Integrity™ partitioning microkernel (MILS separation kernel prototype)
  - OIS OrbExpress (MILS ORB prototype)
  - InterPeak IPV4, IPv6, IPSEC certified Internet protocol stack & firewall
  - GHS Multi™ IDE & Probe™
  - Xilinx System Generator™
- GD AIM Development System
  - AES algorithm

HAWCS

HAWCS Overview - SCA Technica, Inc. (C) 2006

16

UNCLASSIFIED

Figure 7

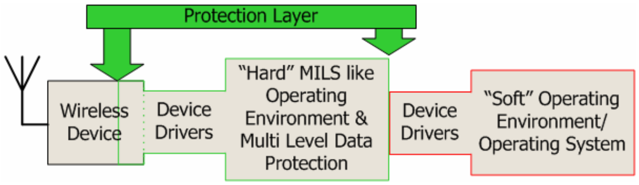

Protection Layer
Wireless Device
Device Drivers
"Hard" MILS like Operating Environment & Multi Level Data Protection
Device Drivers
"Soft" Operating Environment/ Operating System

Figure 8

3. HAWCS™

HAWCS™ is the result of an effort to develop a high assurance architecture capable of protecting mobile platforms from wireless and Internet hackers. Simplified implementations can be used to protect consumer mobile platforms. More advanced implementations which incorporate advanced encryption and security hardware, can be used to deter nation-state class network attacks.

In a demonstration witnessed by Government information assurance experts, HAWCS blocked three potential attack vectors (Figure 6). The first attack vector demonstrated (in red) occurs when a system is connected with a waveform (802.11) to an open network WiFi hotspot. The Hacker can readily connect to this network and thus shares a connection, similar to a local area network with the SDR system. The demonstration showed how a hacker can touch the Black radio, Red radio and the User's Laptop, successfully being able to install and attach to a Trojan horse or reconfigurable components. The next vector (in blue) demonstrated how a malicious or compromised system within the trusted, encrypted network was able to attack the Red radio and the User Laptop. Thus it is crucial to protect against a compromised terminal in a trusted network. Finally (in green), the demonstration revealed how a compromised terminal was able to access reconfigurable components on the Red and Black radio cores, potentially altering the waveform. All attacks were successful. For security reasons, the means of attack are not revealed in this public document.

A functional prototype (Figure 7) was developed using two Xilinx ML-300 Virtex II/Pro FPGA development systems, one Advanced INFOSEC Machine (AIM) Development Card (running an unclassified AES encryption algorithm) and one Windows XP laptop computer. The Virtex II/Pro embedded PowerPC processors employed prototypes of MILS certifiable separation kernel technology (Figure 8) to run the security layer applications which included certified IPv4, IPv6 and IPSEC compliant protocol stacks and firewall applications. One of the purposes of this approach is to isolate the host "soft" operating system (e.g. Windows, Linux, MacOS, Solaris) from network interface devices and their potential "exploits" by network attackers.

HAWCS™ requires a general purpose processor (GPP) with a hardware memory management unit (MMU), and an embedded operating system which employs either a hardware protected partitioning kernel or separation kernel. If a red/black architecture is employed, at least one GPP with a hardware MMU must be available on the red and black side, respectively. Once GPP and operating system requirements are met, HAWCS™ components can be downloaded as a combination of GPP software and FPGA firmware. HAWCS™ is compatible with Multiple Independent Levels of Security (MILS) operating systems and applications, and can utilize a MILS separation kernel if present. HAWCS™ can be made SCA compliant. In fact, on an SCA compliant system, most HAWCS™ components can be downloaded as components of a waveform.

4. CONCLUSIONS

The vulnerability of WIFI enabled mobile devices to "hacker" attacks has alerted the software defined radio industry to potentially serious compromises which can threaten the platform integrity of both mobile computing devices AND software defined radios. The threat has been recognized by both industry and Government groups.

A potentially serious flaw in security design of software defined radios has been discussed, in which exposure of the network interface devices and their drivers to a "soft" operating system may seriously compromise the platform's integrity. The ability of the computing platform to be maliciously re-programmed or reconfigured, by-passing encryption, secure browsers and Virtual Private Networks through use of root kits/key logger Trojan horses and similar malicious software, may be easy to overlook. This form of compromise has also been misunderstood by designers of software defined radios, and proper design considerations overlooked when early design efforts "stub out" security architecture and components. In some instances, a complete re-design of the wireless computing device or software defined radio may be necessary.

The patent-pending HAWCS™ security architecture employs specialized hardware, protected memory and kernel-mode techniques to isolate network interface devices and drivers from operating systems, files and applications using a defense-in-depth technique. It places security applications and component reconfiguration/programming channels within special partitions not easily reachable by network attackers, and accessible only by those with supervisor privileges. HAWCS™ can be used to correct vulnerabilities identified by JTRS CP295, "Exposed Black Side", and added to existing and future software defined radios and mobile consumer devices.

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

[3] 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".

[4] CP 295, "Exposed Black Side", Joint Tactical Radio System (JTRS) Change Proposal (CP), submitted 26 January 2005.

[5] D. Murotake & A. Martin, "Updated system threat analysis for high assurance software defined radios, Proceedings, SDR'05 Technical Conference, SDR Forum, Anaheim CA, November 2005