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

A HIGH ASSURANCE WIRELESS COMPUTING SYSTEM (HAWCS®) ARCHITECTURE FOR SOFTWARE DEFINED RADIOS AND WIRELESS MOBILE PLATFORMS

David Murotake, Ph.D.
dmurotak@scatechnica.com
Mobile: +1-603-321-6536

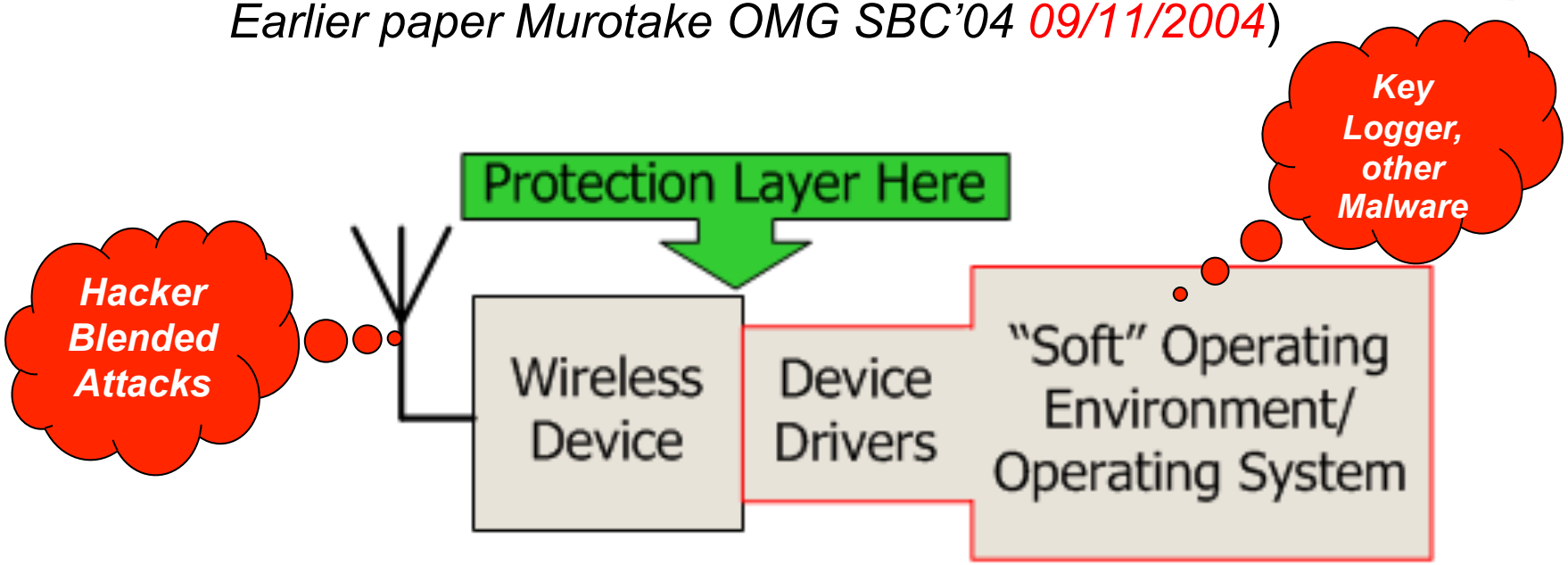
Antonio Martin
Tony.martin@scatechnica.com

SCA Technica, Inc.
Nashua NH, USA

SCA technica

Problem - A *Nearly Universal* Design Flaw

(Excerpt from Murotake & Martin SDR'05 11/17/2005
Earlier paper Murotake OMG SBC'04 09/11/2004)



- 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)

theguardian

Titan Rain – how Chinese hackers targeted Whitehall

Foreign Office among departments hit ● Military involvement suspected

Column five 205mph but still three minutes late

Patrick Barkham

Titan Rain

From Wikipedia, the free encyclopedia

Titan Rain was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities (i.e., masked by proxy, zombie computer, spyware/virus infected) remain unknown. The designation 'Titan Rain' has been changed, but the new name for the attacks is itself classified if connected with this set of attacks.

Source: http://en.wikipedia.org/wiki/Titan_Rain

11/11/2006 – "Broadcom Exploit" Announced!

eWeek, November 11, 2006
http://www.eweek.com/article2/0,1895,2056023,00.asp

Computer security analysts are raising the alarm for a critical vulnerability in the Broadcom wireless driver embedded in PCs from HP, Dell, Gateway, eMachines The vulnerability, exposed as part of the MoKB (Month of Kernel Bugs) project, is a stack-based buffer overflow in the Broadcom BCMWL5.SYS wireless device driver that could be **exploited by attackers to take complete control of a Wi-Fi-enabled laptop**… ZERT (Zero Day Emergency Response Team) warns the flaw could be exploited wirelessly if a vulnerable machine is within range of the attacker. "If you are **near other users with laptops, you are at risk**. If you are at an airport, coffee shop, or using your computer with the wireless card enabled in any public place, you are at risk… "The **card's background scan of available wireless networks triggers the flaw**,"

Zdnet, November 11th, 2006
http://blogs.zdnet.com/Ou/?p=365

According to Johnny Cache, this particular **exploit is extremely reliable and results in "100% ownage"** which means your computer belongs to the hacker if it's attacked using this exploit. Since the exploit has been rolled in to the Metasploit 3.0 framework which includes kernel-level shell code, the exploit can be performed with a moderate amount of hacking knowledge. This flaw is extremely dangerous because it **exploits the kernel of the operating system which means it bypasses all conventional security measures like anti-virus, HIDS, firewalls, and user privileges**. The attack range is limited to Wi-Fi range which is typically 100 to 200 feet but can be extended with high-powered antennas

Software Communications Architecture

Change Proposal Detail

View All CPs

Registration

Search CP#

submit

Change Proposal #295

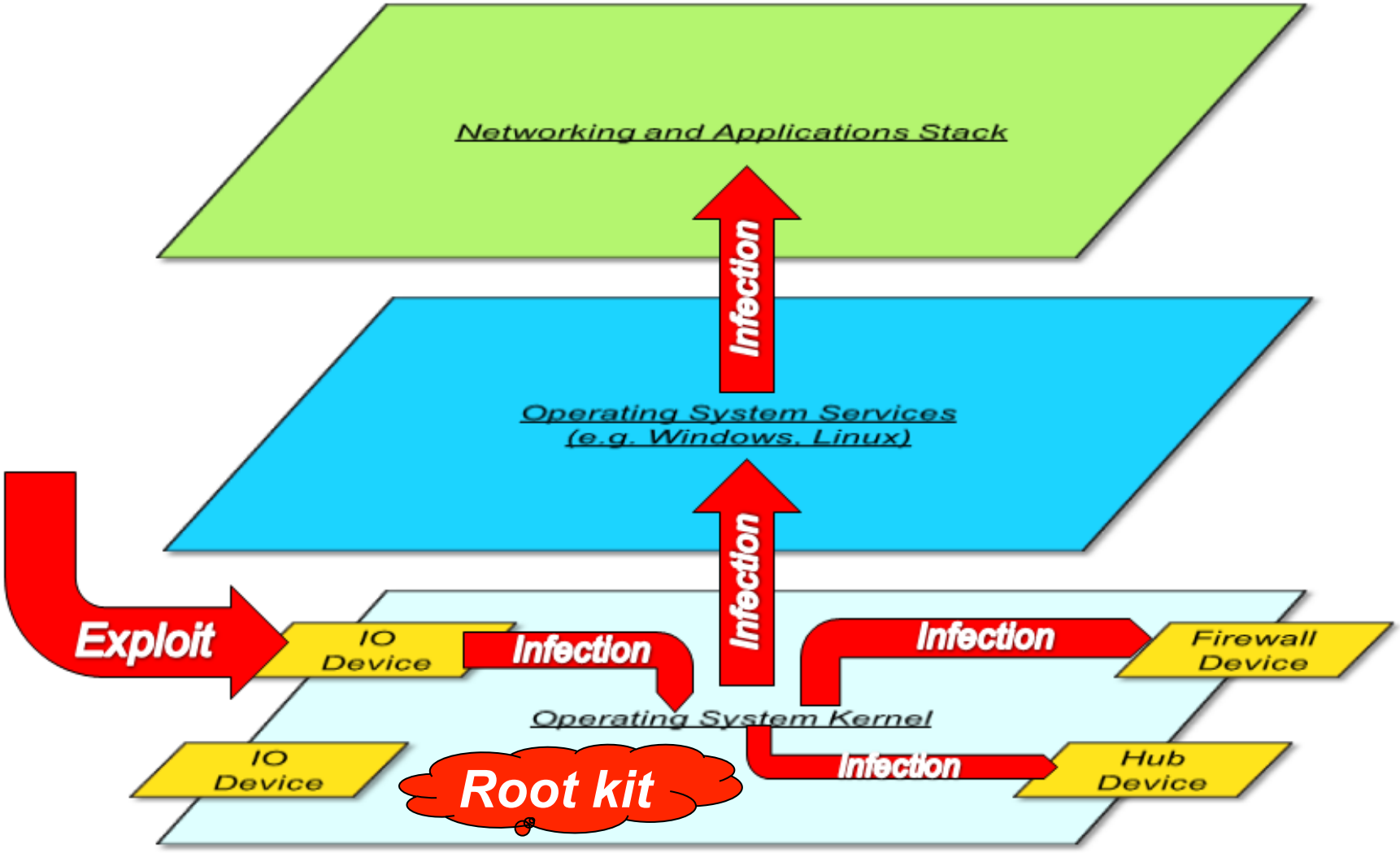
Date:	1/26/2005
Title:	Exposed Black Side
State:	
Document:	Security Supplement to the SCA
Version:	3.0
Location:	General-
Description:	In some operational scenarios, the black side of a JTRS may face the typical network threats. Discuss these threats in the operational scenario sections and create security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

"In some operational scenarios, the black side of a JTRS may face the typical network threats."

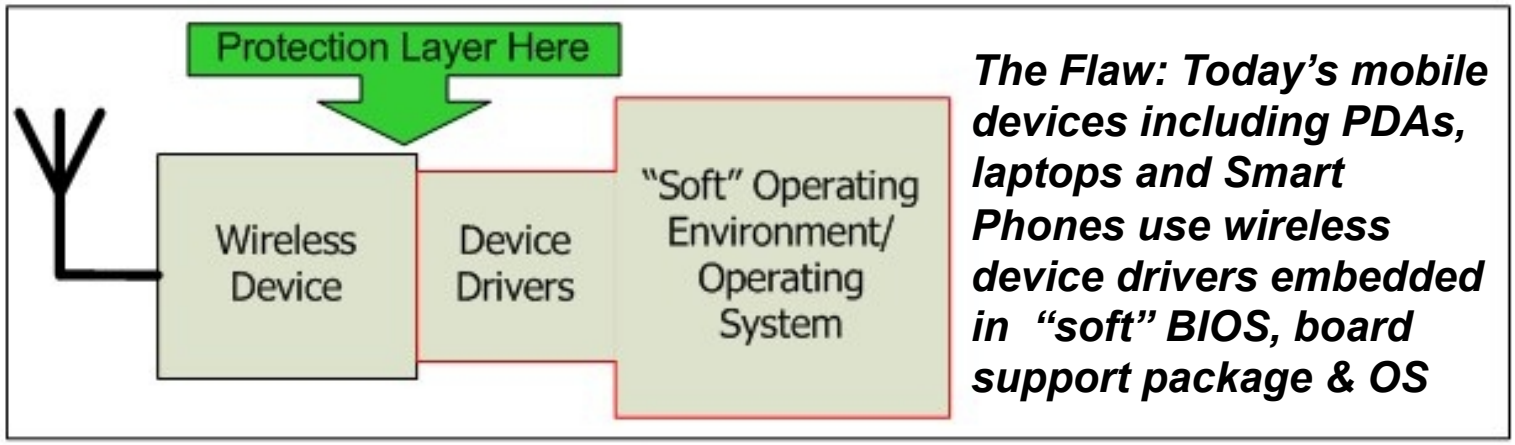
JPEO Resolutions

Notes:	
Attachment:	None

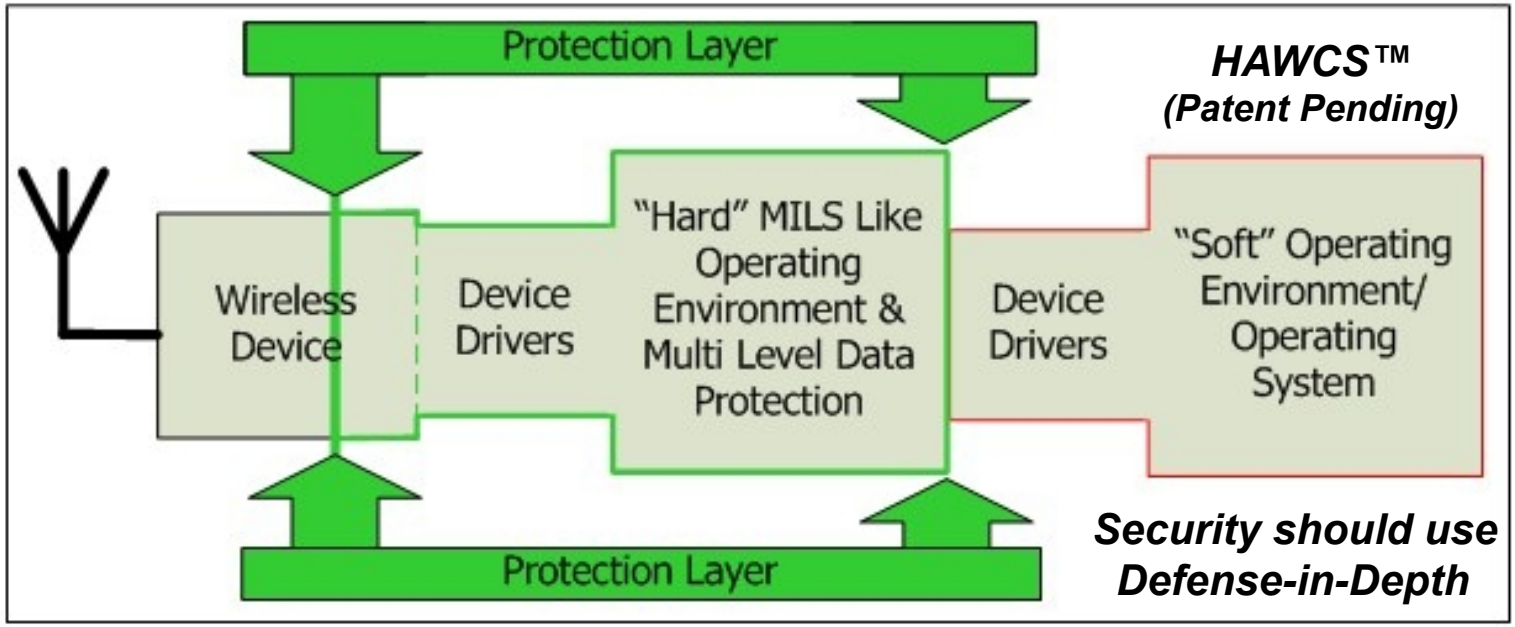
Cyber Security Issue: Kernel Exploits Bypass Firewalls, Encryption, VPNs…



What's the Problem? How to Solve?

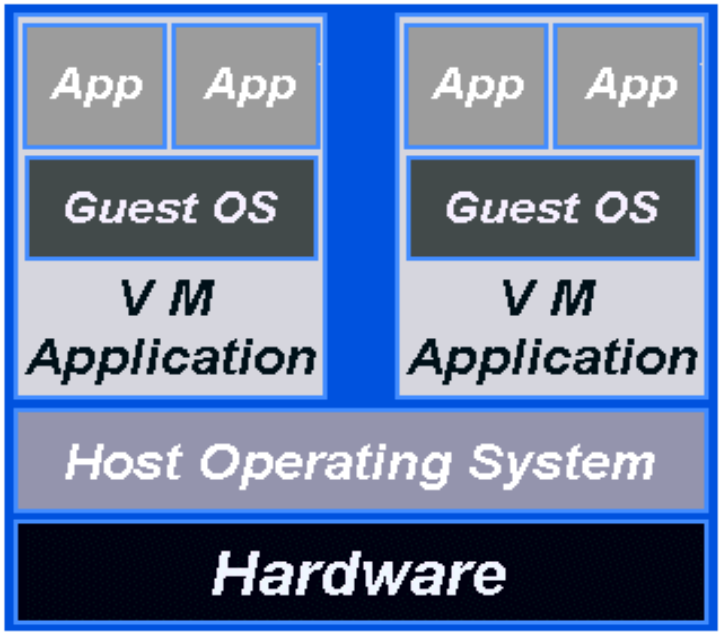


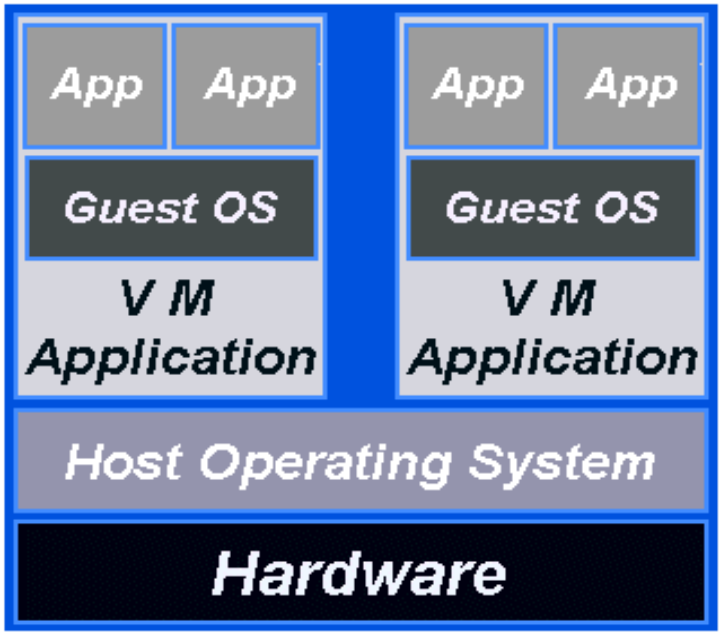
The Flaw: Today's mobile devices including PDAs, laptops and Smart Phones use wireless device drivers embedded in "soft" BIOS, board support package & OS

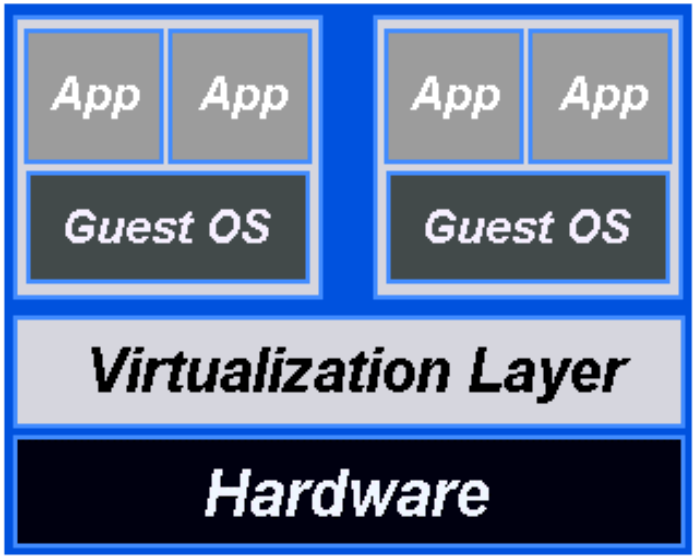


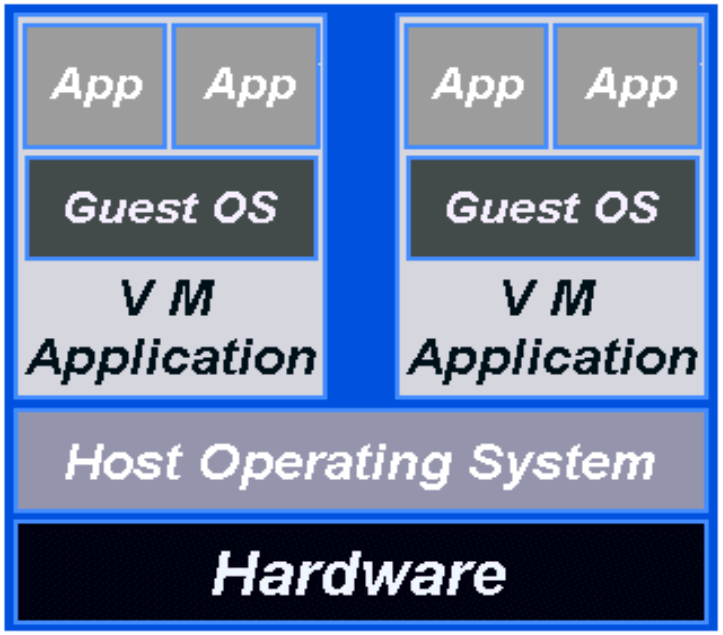
HAWCS™
(Patent Pending)

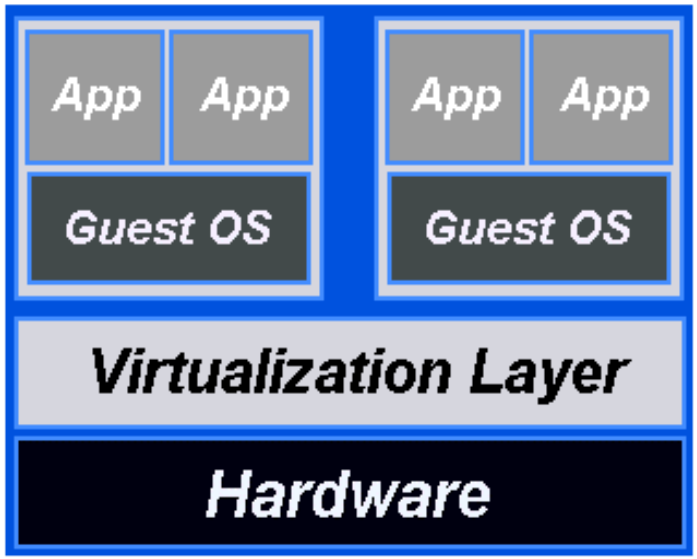
Security should use Defense-in-Depth


App
App
App
App
Guest OS
Guest OS
V M
Application
V M
Application
Host Operating System
Hardware


App
App
App
App
Guest OS
Guest OS
V M
Application
V M
Application
Host Operating System
Hardware

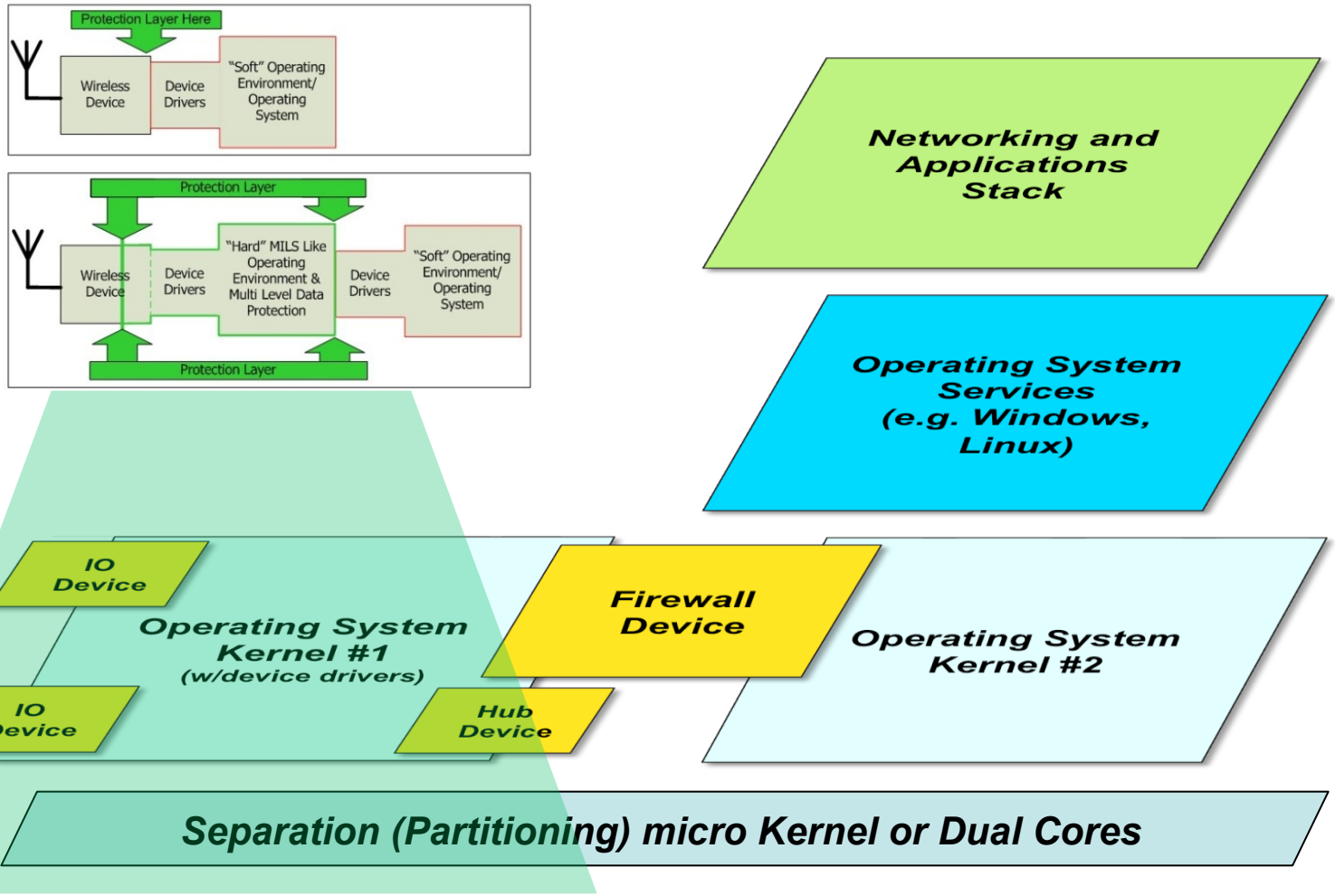

App
App
App
App
Guest OS
Guest OS
Virtualization Layer
Hardware


App
App
App
App
Guest OS
Guest OS
V M
Application
V M
Application
Host Operating System
Hardware


App
App
App
App
Guest OS
Guest OS
Virtualization Layer
Hardware

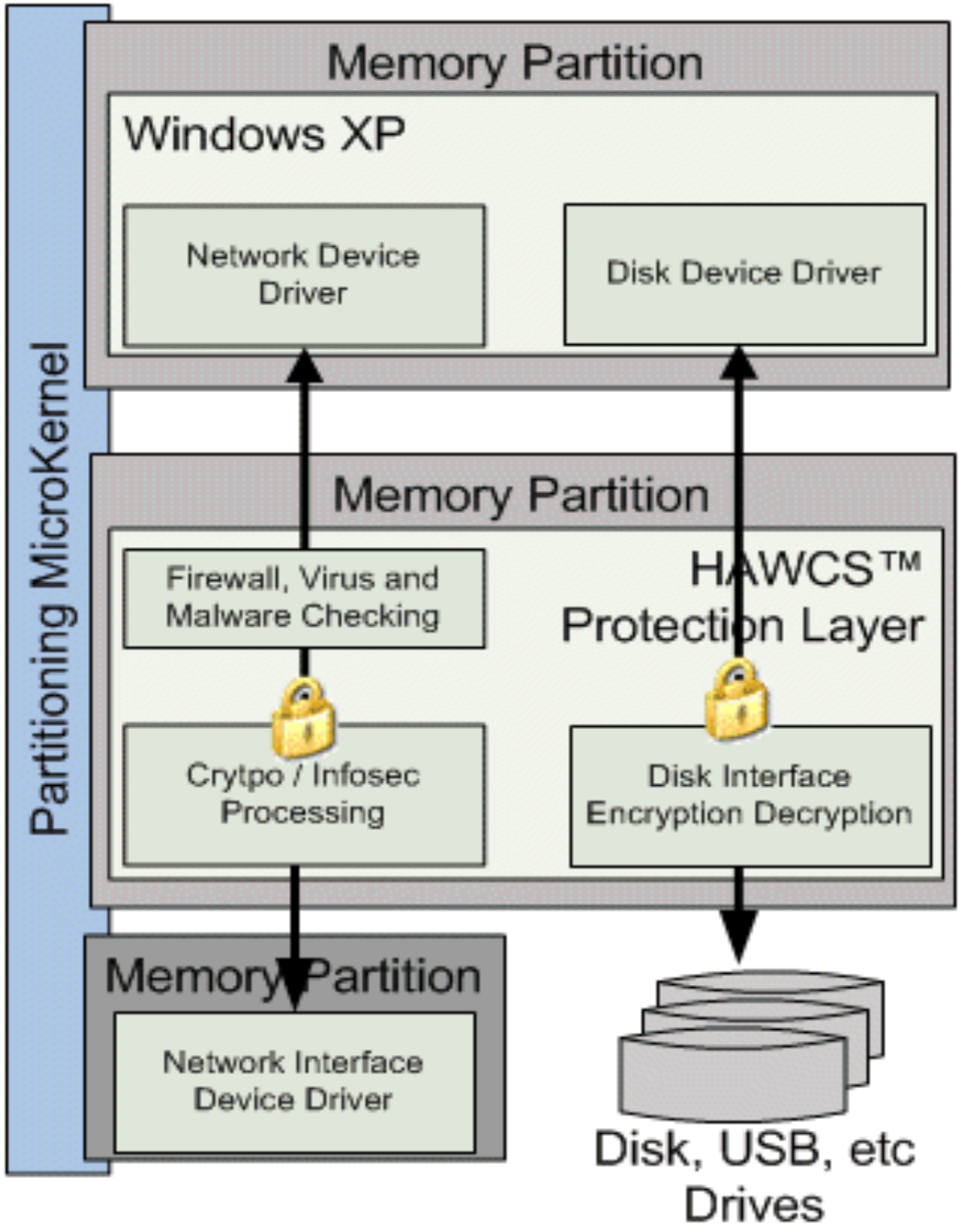

MILS Seperation Kernel
U
Windows
S
Linux
TS
RTOS

HAWCS® architecture isolates mobile device drivers, protects applications



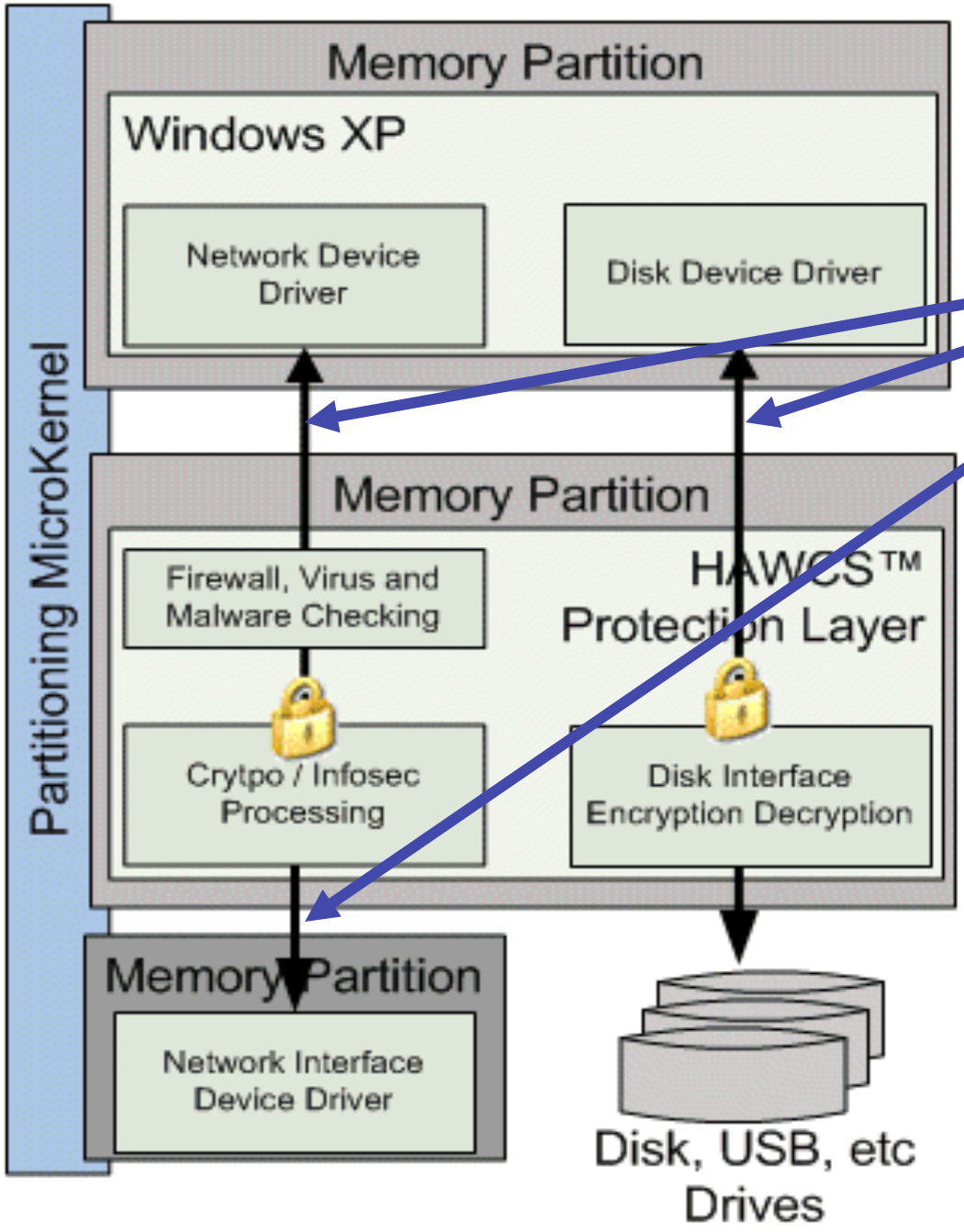
US Patent #7,490,350 B1 - Other patents pending

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



US Patent #7,490,350 B1 - Other patents pending

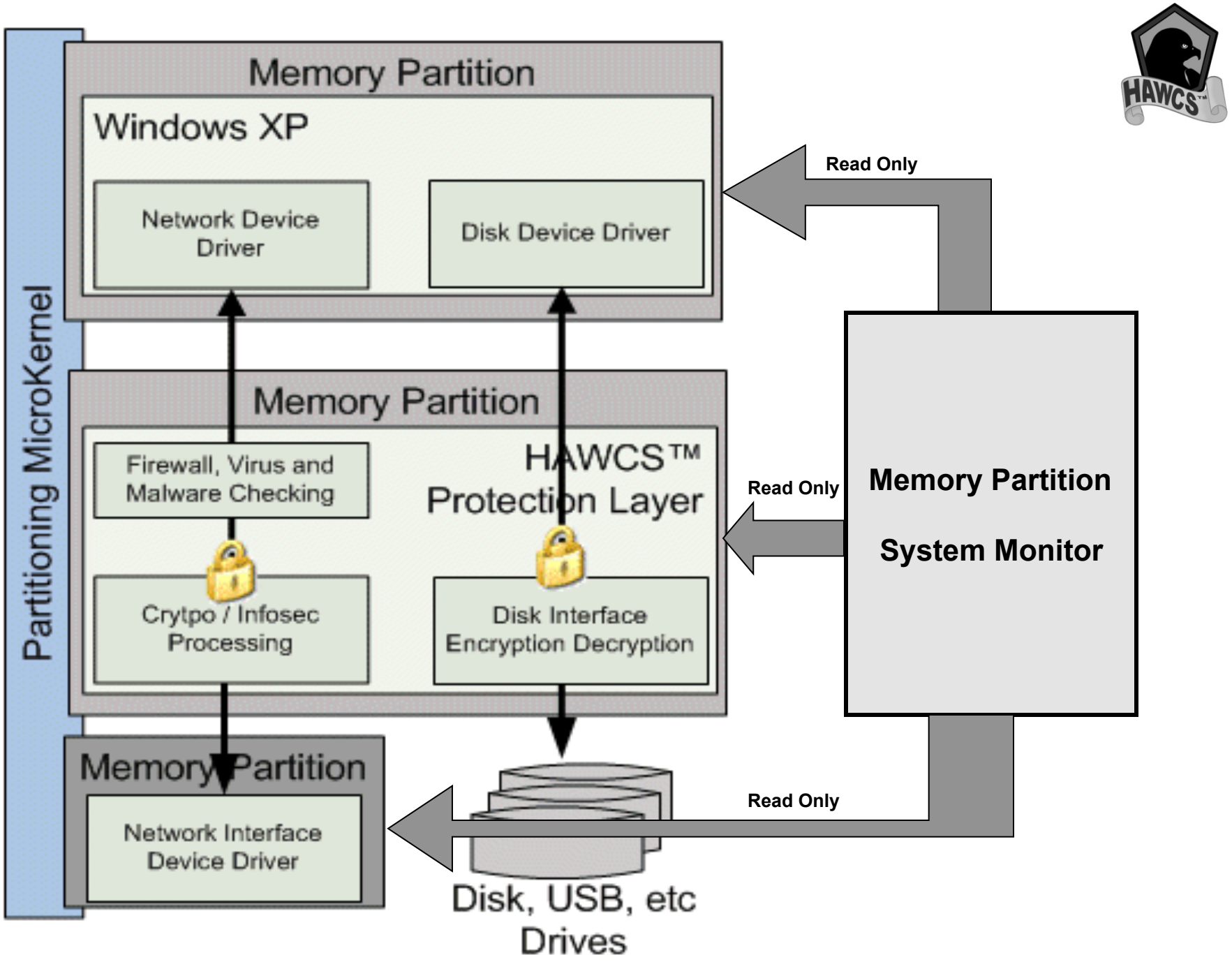
SCA Technica, Inc. – A Veteran Owned 8(A) SDB



Highly constrained interfaces

US Patent #7,490,350 B1 - Other patents pending

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



US Patent #7,490,350 B1 - Other patents pending

Thank You for your Attention!

Contact me with any questions:

David K. Murotake, Ph.D.
President, SCA Technica, Inc.
Phone: 1-603-321-6536
Email: dmurotak@scatechnica.com