Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Wireless at the hospital and the threats they face

At the core of IT security is the CIA-triad the need to protect the Confidentiality of data, the need to protect the Integrity of data and the need to protect the Availability of data. Unfortunately when it comes to wireless networks the Availability aspect will always be at a risk due to the inherent properties of wireless communications. Additionally, since wireless networks offer very little protection to hardware at lower layers of the OSI model, attackers can exploit this flaw to initially gain unautho...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

# Wireless at the hospital and the threats they face

*GAWN Gold Certification*

Author: Warren Platt, warrenplatt1@gmail.com

Adviser: Joey Niem

Accepted: April 17th 2008



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

## Outline

1. Abstract ..... 4

2. Introduction ..... 4

3. The application of wireless on the rise ..... 5

4. Setting the stage ..... 7

5. Specifications ..... 8

6. Exploiting the weakest link ..... 9

7. Attack with a double-edged sword ..... 11

8. The Implications ..... 15

9. The forgotten wireless threat? ..... 16

10. Putting it into perspective ..... 18

11. Conclusion ..... 21

12. References ..... 24



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

“By failing to prepare, you are preparing to fail.”

- Benjamin Franklin

© SANS Institute 2009, Author retains full rights.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

## 1. Abstract

At the core of IT security is the CIA-triad – the need to protect the “Confidentiality” of data, the need to protect the “Integrity” of data and the need to protect the “Availability” of data. Unfortunately when it comes to wireless networks the “Availability” aspect will always be at a risk due to the inherent properties of wireless communications.

Additionally, since wireless networks offer very little protection to hardware at lower layers of the OSI model, attackers can exploit this flaw to initially gain unauthorized access of a device connected to a wireless network, and then gain total control of the system by launching an attack at the heart of the device – the CPU.

## 2. Introduction

The use of wireless networks has exploded over the past decade and the application of wireless technology seems to have no boundaries, particularly in hospitals. Robots that are connected to wireless networks bring medication to patients, the increased use of wireless intravenous (I.V.) pumps or even operations performed on patients using streaming imaging over wireless networks when local doctors need the expert opinion of other physicians that are not at the same facility. The application is amazing, but the risks are ever-increasing.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

New research in ways of exploiting systems regardless of their software patch level or even operating system means that the CIA-triad in wireless networks especially is at risk of being compromised regardless of what the wireless infrastructure is based on – be it Wi-Fi Protected Access (WPA) or WPA2, Temporal Key Integrity Protocol (TKIP) or Counter-Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).

In addition to patching installed applications and operating systems, organizations will now need to make regular updates to outdated drivers and BIOS too and these will have be regulated during routine wireless audits.

## 3. The application of wireless on the rise

The proliferation of wireless components and the application of this technology is ever-increasing meaning the possibilities for exploitation of the systems is also on the rise. One such study performed by RSA on the deployment of wireless in businesses, showed for example a 180% increase in access points (APs) between 2006 and 2007 in London and that the implementation of security measures on wireless networks had increased from 74% in 2006 to 81% in 2007 in London, England. However, less than half of these were deployed with at least WPA or stronger, with similar results for New York and Paris[1].



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

Also the use of wireless networks is rapidly changing. One of the newest applications of a wireless network is to have courier TUG robots bring medication, meals and equipment to doctors and nurses[2]. The robots do not actually take the place of doctors or nurses per se, but they do the “simple” tasks in the hospitals so that vital hospital resources can be concentrated in areas requiring specialist human intervention.

Already back in 2004 the potential of using wireless in the hospitals for uses other than user connectivity was put into use, when Sharp Healthcare started using the wireless architecture at some San Diego based hospitals by deploying wireless intravenous pumps. It (Sharp Healthcare) “completed deploying 200 Wi-Fi-based "wireless pumps" – intravenous (I.V.) infusion units from Alaris Medical Systems that connect to a central server over the WLAN and allow doctors and nurses to remotely monitor delivery of medications.”[3].

The article also goes on to mention something very noteworthy: “… scores of doctors and other medical professionals also use the WLANs to access the Sharp network with their Wi-Fi-enabled PDAs and laptops. More and more are requesting access all the time.”[3].

The statement is noteworthy because by its very nature, wireless has virtually no protection against attacks in the lower layers of the Open Systems Interconnection Basic Reference Model (OSI model)[4] – particularly at layers 1 and 2. In fact, a US-CERT release in



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2004 has the following notification regarding the use of 802.11: “Due to the inherent vulnerabilities in 802.11 (VU#106678, VU#391513, RF interference), do not deploy 802.11 networks for applications that require high availability (e.g. safety, critical infrastructure)”[5]. According to a report from St. Luke’s Hospital in Houston even the transport elevator would occasionally cause network disruptions to the wireless infrastructure[6].

There are many wireless vendors that have access points with the capability to automatically detect rogue APs, to detect and block malicious traffic on the wireless network and to load-share traffic. However, because of the fundamental flaws in the characteristics of wireless networks an attacker can easily bypass these countermeasures to cripple a wireless infrastructure through techniques such as Radio Frequency (RF) signal jamming or by attacking a wireless client directly at layer 1 or layer 2 – more specifically, the wireless card itself.

## 4. Setting the stage

According to a study conducted by IDG, the implementation of wireless at hospitals is seen as a means for “accessing and updating electronic medical records (EMR) at patients' bedsides, matching bar-coded patient wristbands and medication packages to physician orders, and using wireless badges for voice communication”[7].



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

We will therefore assume that a certain hospital has similar requirements to the wireless infrastructure and because the new infrastructure will be dealing with sensitive patient information, security is a top priority. On the advice of their chosen vendor, the hospital's wireless network is configured to run WPA2 with CCMP instead of TKIP because of recent new developments in tools that exploit TKIP[8].

Lastly, the hospital will acquire state-of-the-art Tablet PC's from Panasonic. These are specifically designed for the healthcare industry to enable doctors and nurses to access patient information from the bed side or even make house-calls whilst still having access to patient information.

## 5. Specifications

The Toughbook® H1 mobile Clinical Assistant for Medical Professionals has the following noteworthy specifications (http://www.toughbook.eu/media/CF-H1_Spec_Sheet_Engl.pdf):

| | |
|---|---|
| CPU | Intel® Atom™ Processor Z540 (1.86GHz, 512KB L2 cache, 533MHz FSB) |
| OS | Genuine Windows Vista® Business Service Pack 1 or Genuine Windows® |



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

| | |
|---|---|
| | XP Tablet PC with SP3 (Downgrade) |
| WLAN | Intel® Wireless WiFi Link 5100 Series (802.11a/b/g/draft-n) |
| Software | Adobe Reader 8, PC Information Viewer, Keyboard Button Manager, Intel® PROSet / Wireless WiFi Connection Utility, Bluetooth™ Stack for Windows® by TOSHIBA, Wireless Switch Utility, Battery Recalibration Utility, Infineon TPM Professional Package |

## 6. Exploiting the weakest link

Security in all computer architectures comprises different “rings”, or security levels that dictate what functions various computing requests can carry out. Ring 0, also known as the kernel, is at the heart of the computer and has the highest security level. On the outer, lower security level is ring 3, or the user level. Even “root” or “administrator”, only has access to this level because they are merely part of the “user ring”. The 4 rings and some of their functions are as follows[9]:

Ring 0: Operating system kernel - CPU.

Ring 1: Remaining parts of the operating system.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

Ring 2: File system drivers and operating system utilities.

Ring 3: Applications and programs – Web browser, email client, database.

Recall that as mentioned previously, a US-CERT notification identifies that there is very little protection against wireless networks at the lower layers of the OSI model, particularly at layers 1 and 2. Since hardware interacts directly with the CPU for allocation of resources, attacking the unprotected wireless hardware and compromising it would give an attacker direct access to the kernel, from where they would be able to have full control over the system. There are already numerous exploits available that target wireless cards, such as the Metasploit code that targets the BCMWL5.SYS driver used by the Broadcom wireless adapter. According to the Metasploit exploit description by Johnny Cache and LMH[10], "The Broadcom BCMWL5.SYS wireless device driver is vulnerable to a stack-based buffer overflow that can lead to arbitrary kernel-mode code execution". Depending on the attacker's intentions the "Confidentiality", "Integrity" and/or "Availability" of data could be compromised.

Additionally, recent developments in proof-of-concept code that exploits the actual CPU itself are on the rise. Kris Kaspersky recently presented this idea at the October 2008 Hack In The Box Security Conference showing some samples of code that exploit Intel-based CPUs in his slide show (http://conference.hitb.org/hitbsecconf2008kl/materials/D2T1%20-



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

%20Kris%20Kaspersky%20-

%20Remote%20Code%20Execution%20Through%20Intel%20CPU%20Bugs.pdf). As Mr. Kaspersky notes in the presentation abstract[11]: "Intel CPUs have exploitable bugs which are vulnerable to both local and remote attacks which works against any OS regardless of the patches applied or the applications which are running."

## 7. Attack with a double-edged sword

Now that we know that there is very little protection against attacks at the lower layers of the OSI model, and we have been introduced to the notion of wireless NIC exploits using Metasploit, and to the idea of attacking the CPU itself, how about combining these attacks for complete CIA-triad exploitation?

Recall that the specifications for the Panasonic Tablet PC say that it uses the Intel® Atom™ Processor Z540. We can now take a look at the Intel Specification Update documents that are publicly available that document errors and exceptions under certain conditions by the CPU (http://download.intel.com/design/chipsets/embedded/specupdt/319536.pdf).

According to the Errata section for the Intel® Atom™ Processor Z5xx Series Specification Update, Errata AAE12 (Fault on ENTER Instruction May Result in Unexpected



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Values on Stack Frame), stipulates that “Data in the created stack frame may be altered following a fault on the ENTER instruction.” Additionally, “This erratum is not expected to occur in ring 3. Faults are usually processed in ring 0 and stack switch occurs when transferring to ring 0.” In other words, if an attacker were able to invoke this error and execute malicious code, it would happen in ring 0 – the kernel.

But what exactly does an ENTER instruction look like in an x86 architecture? Considering our Tablet PC is installed with Windows Vista which runs a 64-bit architecture, a simple ENTER instruction could look something like this[12]:

```
foo:

    enter $(8 * 2), $0

    mov %rdi, -8(%rbp)

    ...

    leave

    ret
```

In reading the Intel Errata documentation it is unknown what ENTER instruction needs



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

to be issued to the CPU to create the error condition. However fuzzing techniques can be used to eventually derive the exploit code.

Intel does, however, give a potential attacker a better hint at where to direct their malicious code in Errata AAE33 (Speculative Load from Address 1D9H May Occur During a Failed VMCALL in VMX Root Operation). Intel documents exactly what the pointer value should be (FFFFFFFF_FFFFFFFFH) and which address space the CPU will be trying to load from (1D9H). Armed with this much information, an attacker could once again create the necessary exploit code to trigger this condition and once again if successful, all code would be executed by the CPU in ring 0.

In practice an attacker would most likely first look to attack a vulnerable wireless card that has a buffer overflow (such as the Broadcom exploit mentioned earlier) in order to have the CPU execute the attacker's code. An attacker could use an existing exploit and tweak it so that when the buffer is over run the Instruction Pointer (EIP in Intel platforms) is set to the location of the attacker's shellcode. Below is a snippet of source code for the Broadcom exploit available in Metasploit 3.2.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

```
        # ssid tag
        "\x00" + # tag: SSID parameter set
        "\x5d" + # len: length is 93 bytes

        # jump into the payload
        "\x89\xf9" +                    # mov edi, ecx
        "\x81\xc1\x7b\x00\x00\x00" + # add ecx, 0x7b
        "\xff\xe1" +                    # jmp ecx

        # padding
        rand_text_alphanumeric(79) +

        # return address
        [target.ret].pack('V') +

        # vendor specific tag
        "\xdd" + # wpa
        "\xff" + # big as we can make it

        # the kernel-mode stager
        payload.encoded
end
```

Armed with readily available exploit code that can be altered to include the valuable information obtained in Errata AAE33, and by reading Aleph One's detailed work entitled "Smashing the Stack for Fun and Profit" (http://insecure.org/stf/smashstack.html) an attacker would be able to tailor-make an exploit to invoke the condition of Errata AAE33. The sample of machine code could include something like[13]:

xor %eax, %eax (Any value XOR itself gives zero or a clean register)

push 0xhffffffff (Push the trigger condition in reverse order onto the stack – LIFO[14])

push 0xffffffff (Push the trigger condition in reverse order onto the stack – LIFO)



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

mov 0x00000h9d1, %eax (Errata AAE33 says once the trigger condition is met, the CPU will try to load the instruction at memory location 1D9H, which we move to register %eax)

push $<exploit code>, %eax (We now push our exploit code into the register value %eax)

int 80, %eax (This causes the kernel to execute the system call at memory location %eax – our exploit code)

We now have our shellcode, executed by the CPU, running in ring 0 through a buffer overflow vulnerability in a hardware driver.

## 8. The Implications

By gaining unauthorized access to the device by initially exploiting an unpatched wireless driver and then gaining kernel-level access to the device by exploiting the CPU itself, an attacker would have complete control over the device and could therefore:

- Install other malicious software,
- Gain access to sensitive patient information,
- Alter medical records,
- Use the device as a mechanism to gain access to the rest of the network,
- Wipe all data from the device – effectively a Denial of Service (DoS) attack.

An attacker has now compromised the “Confidentiality”, “Integrity” and “Availability” of



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the CIA-triad that the security community is fighting so desperately to protect.

Therefore it is vitally important that an effective patch management policy not only includes OS and application patches but also includes driver updates to wireless hardware and BIOS updates too.

A very useful, free Windows-based tool for scanning wireless cards for vulnerable drivers is called “WiFiDEnum” by Aruba Networks. More information regarding the use as well as the download location can be found at: http://labs.arubanetworks.com/project/WiFiDEnum

## 9. The forgotten wireless threat?

Performing wireless audits is imperative if the aforementioned attack scenarios are to be mitigated. During an interview of hospital IT staff, the author was told that during one of their audits it was discovered that a large number of the printers located at the hospitals came pre-installed with wireless capabilities. The IT staff could not confirm whether the printers were enabled with wireless access after installation, or whether they were installed with factory settings for wireless capabilities.

A Google search for “wireless printers” reveals most major printer vendors have some form of wireless printers in their product line, including Dell, HP, Lexmark, Canon, Samsung



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and Epson (to name but a few). In fact, searching CNET reviews for printers for a connectivity technology as “wireless” brings up 576 items[15].

What about the security of these devices? A look at the technical specifications for a HP Deskjet 5800 series printer has some alarming details regarding the configuration of the Service Set Identifier (SSID)[16]: “Default: The Deskjet 5800 series printer ships with an open or blank SSID which enables it to automatically join a wireless network. If there is more than one wireless network in the vicinity, your printer will join the network with the strongest signal.” The specifications for HP regarding configuration of WEP or WPA is as follows: “Default: The Deskjet 5800 has no security setting.”[16]

How can this be exploited? Consider that typical printing environments have a printer connected to the wired network and that typically the drivers are installed on a server, particularly in Windows environments. Should an attacker use a directional antenna and the correct additional hardware (for example, the WiFi Predator[17] can be built for around US$100), an attacker could be located a fair distance from the wireless printer and use it as a piggyback onto the wired network if the default settings are left unchanged by the IT staff and there is routing capability on the printer.

An attacker could also gain unauthorized access to sensitive patient information if any



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

such data is printed off by hospital staff on a printer that is accessible by an attacker. It is easy to assume an attacker is able to gain control of the printer in a similar way to our example with the Tablet PC.

Furthermore, since hospitals by their very nature are open to the public, an attacker could deploy their own unauthorized access point in a waiting room with unprotected network jacks. This threat becomes amplified by the fact that an attacker could "hide" the access point from a wireless audit, by using something like WKnock[18]. This tool, when configured on an AP gives an attacker the ability to have the AP continually listen for wireless traffic in promiscuous mode and therefore be undetectable to Wireless IDS systems or tools such as Kismet. Only when an attacker sends a specific sequence of packets to the AP running WKnock will the AP start acting like a regular AP.

## 10. Putting it into perspective

There are many scenarios that an attacker could engage in to launch an attack. Because of the very nature of hospitals, an attacker could for example steal a Tablet PC and return it again after installing malicious code. Once the compromised equipment is put into production again the attacker would have every possibility of staging another attack via the compromised system. Alternatively, an attacker could use social engineering or Google to



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

gather information about the wireless deployment of a particular hospital. With enough details of the technical infrastructure, an attacker can then piece together the tools needed for the attack.

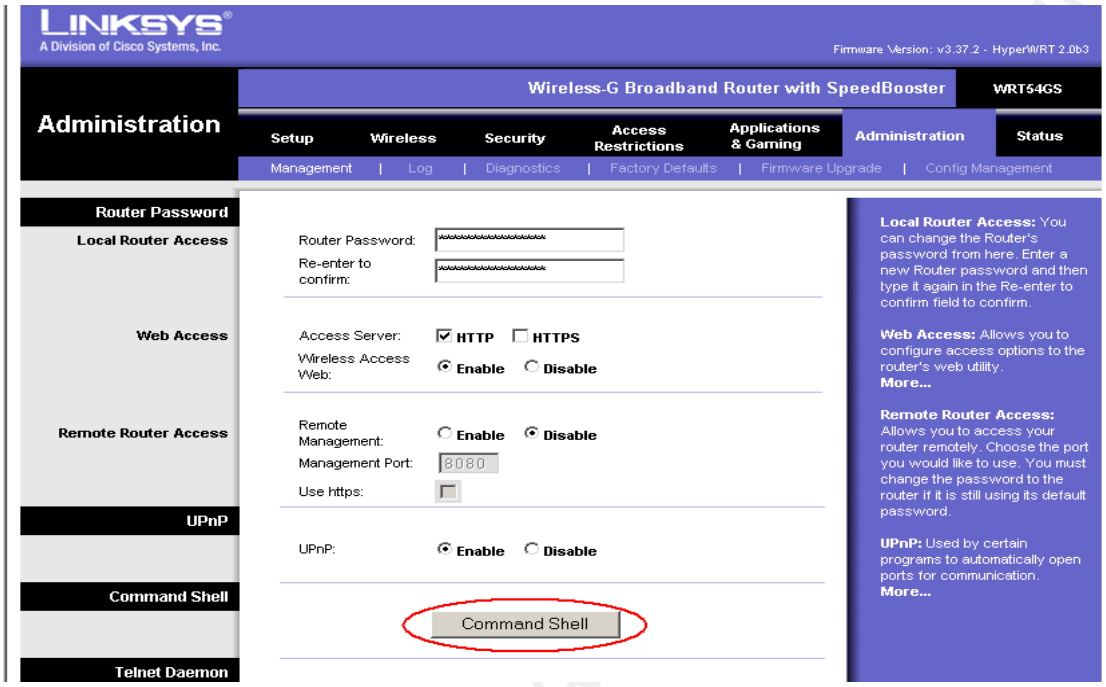
As we have seen, obtaining the technical specifications to hardware is trivial and by looking through the vast amounts of documentation that exists on writing exploits an attacker could use an existing framework such as Metasploit to leverage an attack directly against the wireless NIC and execute code directly in ring 0.

Alternatively, let's assume an attacker was able to connect a rogue AP (such as the popular Linksys WRT54G) in a waiting room that had an unsecured network jack and that rogue AP's firmware was upgraded by the attacker using HyperWRT (http://www.linklogger.com/wrt_setup.htm).



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face




This would allow an attacker to start up a Linux-based command shell to configure WKnock (https://dev.openwrt.org/browser/packages/net/wknock/Makefile?rev=4667) to respond to a predetermined sequence of packets before functioning as a normal AP. Moreover, an attacker armed with hardware such as the WiFi Predator would be able to activate normal functioning of the modified AP without even having to be in the same building.

With unauthorized, unrestricted access to the network, an attacker would now be free to gather network traffic from the hospital's network at leisure, potentially collecting domain administrator credentials or confidential patient data such as Social Security Numbers (SSNs) in the US, or Central Person Register (CPR) numbers in Denmark.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

## 11. Conclusion

With the recent public focus on tools that are able to exploit TKIP, organizations are being urged to migrate to AES. As organizations do this, attackers will start looking for new ways at compromising wireless networks, by targeting the components that have little or no protection at all – the outdated drivers of wireless cards. Once compromised, attacks against the CPU itself will be on the rise as more attackers develop exploit code to gain kernel-level access of devices.

Mitigating these threats can be implemented in several steps:

1. A wireless assessment should be based on a thorough risk-analysis to identify the wireless components that could be targets for an attacker and the likelihood that these components can be compromised. The assessment should also identify any components with vulnerable applications and drivers as well as ensuring that all vendor-supplied default settings are changed and unnecessary functionality is removed. Documentation of all components will prove invaluable in the event of a compromise.

2. Defense in depth, just as with wired networks, is crucial in wireless networks where access to confidential patient data should be as restrictive as possible. Implementation or Wireless IDS Sensors, host-based firewalls and IDS



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

software, layered DMZ's and file integrity monitoring tools (such as Tripwire or AIDE) on core system files and patient records.

3. Secure backups of all critical components and the regular testing thereof is essential in the event that a compromised system needs to be completely re-installed after a secure wipe of the disk. This procedure might vary depending on the facility's security policy since it might be necessary to perform a forensic analysis of the system prior to a wipe.
4. A well-defined and regularly tested incident response plan.
5. An effective patch-management policy that includes driver updates and BIOS updates too.

Unfortunately, even if a wireless audit revealed that a deployment was based on the most secure standards available today and that all systems were fully patched, the very nature of the wireless constructs would still make the deployment vulnerable to physical attacks at the lower layers of the OSI model via RF signal jamming attacks. Here the mitigation techniques are beyond the capabilities of most organizations, especially hospitals – very high perimeter walls, signal dampening windows or even signal reducing paint[19]. From a pure security point of view with the CIA-triad at the core, wireless networks will always fail in



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the category of “Availability”, since this aspect can never be guaranteed with 100% certainty. It is also this CIA-triad that is covered by the HIPAA security rules.

In essence: system-critical and potentially life-threatening equipment should not be using wireless as the only method of data carrier. Every risk assessment conducted by an organization in the health-care sector (and others too), must put the potential to cause harm to people higher than any other factor and this should drive the solutions that are implemented.

As Benjamin Franklin put it: “By failing to prepare, you are preparing to fail”.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

## 12. References


1. RSA Press Release (2007, June). Wireless Adoption Leaps Ahead, Advanced Encryption Gains Ground in the Post-WEP Era. Retrieved August 10, 2008, Web site: http://www.rsa.com/press_release.aspx?id=8451
2. Cisco Systems, Inc. (2008, June). How Robots are Improving the Quality of Healthcare—Automatically. Retrieved July 1, 2008, Web site: http://governmentsecurity.bitpipe.com/detail/RES/1213908574_134.html
3. Blackwell, Gerry (2004, September). The Wireless I.V. Retrieved July 31, 2008, Web site: http://www.wi-fiplanet.com/columns/article.php/3402721
4. Wikipedia.org (2008, July). OSI Model. Retrieved 2 August 2008, Web site: http://en.wikipedia.org/wiki/OSI_model
5. Manion, Art (2008, February). Vulnerability Note VU#106678. Retrieved August 2, 2008, Web site: http://www.kb.cert.org/vuls/id/106678
6. Dubie, Denise (2002, March). Wi-Fi @ Work. Retrieved August 10, 2008, Web site: http://www.networkworld.com/wifi/2002/sideonline.html
7. Havenstein, Heather (2005, May). Wireless Leaders & Laggards: Health Care. Retrieved November 30, 2008, Web site: http://www.computerworld.com/mobiletopics/mobile/story/0,10801,101711,00.html




© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

8. Siles, Raul et al. (2008, November 8). WPA/TKIP ChopChop Attack. Retrieved November 13, 2008, from RaDaJo Web site: http://radajo.blogspot.com/2008/11/wpatkip-chopchop-attack.html
9. Harris, Shon (2003). CISSP Certification All-in-One Exam Guide, Second Edition. Emeryville, CA: McGraw-Hill/Osborne
10. Cache, Johnny (2006, November). Broadcom Wireless Driver Probe Response SSID Overflow. Retrieved August 2, 2008, Web site: http://projects.info-pull.com/mokb/MOKB-11-11-2006.html
11. Kaspersky, Kris (2008). Remote Code Execution Through Intel CPU Bugs (Presentation Abstract). Retrieved November 14, 2008, Web site: http://conference.hitb.org/hitbsecconf2008kl/?page_id=214
12. Author unknown (2007). X86-64 Architecture Guide. Retrieved November 14, 2008, Web site: http://web.mit.edu/6.035/www/handouts-2007/x86-64-architecture-guide.html
13. Rosiello, A. (2004). The Basics of Shellcoding, 1.0, Retrieved December 21, 2008, from http://www.infosecwriters.com/text_resources/pdf/basics_of_shellcoding.pdf
14. Author unknown (2007). Stack (defined). Retrieved December 20, 2008, from http://wiki.osdev.org/Stack
15. CNET reviews. Retrieved June 16, 2008, Web site: http://reviews.cnet.com/computer-printers/?sa=1000036&filter=500196_3809360_



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Wireless at the hospital and the threats they face

16. HP – Understanding the Network Configuration Page. Retrieved June 16, 2008, Web site: http://h10025.www1.hp.com/ewfrf/wc/document?docname=c00033101&lc=en&cc=us&printable=no&rule=804&dlc=&product=305980
17. hevnsnt (2008, April). The WiFi Predator. Retrieved June 29, 2008, Web site: http://www.i-hacked.com/content/view/261/42/
18. Siles, Raul (2003, December). WVE-2006-0073. Retrieved August 10, 2008, Web site: http://www.wirelessve.org/entries/show/WVE-2006-0073
19. Nash, Jim (2004, December). Startup Markets Wireless-Security Paint. Retrieved August 10, 2008, Web site: http://www.informationweek.com/news/management/showArticle.jhtml?articleID=56200676



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 19th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |