



This month we decided to print a "Best of the Hurricane Labs Newsletter" edition, featuring your favorite articles from the past 2 years. These articles were chosen based from the comments we received from our readers throughout time. Whether you find these articles familiar or you missed them the first time around, we hope you will enjoy this month's edition!

Wireless Security Primer: Beyond the Tin Foil Hat from September 2008

By: Lann Martin

Wireless security is hard. Securing a wireless network means starting with some different assumptions than you would with wired. On top of that, 802.11 is still relatively new tech with frequent updates, and learning how it works is often like trying to hit a moving target¹. With that in mind, here is a quick primer on a few of the basic things you absolutely must know to protect your wireless network.

Learn to share

WiFi is a shared medium, meaning everyone can see everything on the network all the time. You should assume an attacker (lets call him Walter) can see all the traffic on your network. Walter can probably see your traffic from the parking lot or even the Starbucks across the street, especially with a high-tech coffee-can-and-usb-adaptor antenna. Wally can also inject packets into your network, spoofing the MAC address to make them look like they are coming from a legitimate user, even if the user is currently connected.

Encryption is not magic

Beyond the fact that encryption does not, on its own, make any network secure (a topic for another day), you should not treat encryption as if it works by magic, and you should know that not all encryption is created equal. As you may know, WEP (the first popular attempt at WiFi encryption) is broken. No matter how complex you make your key, it can easily be cracked

in a few hours or even, with a few tricks and a little luck, in a few minutes.² DO NOT USE WEP.

WPA does not suffer from the same weaknesses as WEP, but it can still be used incorrectly. For WPA using Pre-Shared Keys (sometimes referred to as PSK or WPA-Personal), keys can be cracked offline, meaning that after a few minutes in your parking lot, Walter can go home to his cluster of Linux-infused PS3s and let them work on breaking your encryption while he takes a nap (Walter is a lazy hacker). If you have to use WPA-PSK, you can prevent Walter's cluster from cracking your key in any reasonable amount of time by selecting a long, random password. If you are feeling crazy and insist on using a password that isn't entirely random, be sure to change your wireless SSID to something uncommon to protect against a pre-computed dictionary attack, which can crack a weak password in seconds.³

Paper walls

There are a couple of wireless "security measures" that might give you a warm fuzzy feeling, but provide no real protection against a motivated attacker. Disabling SSID broadcasting prevents the access point from advertising its existence, but it does nothing to hide an active network. The SSID of a network is transmitted with every data packet and is visible even when the data is otherwise encrypted. MAC filtering is a common way to control

access by allowing only certain network devices to connect. However, like the SSID, the MAC address of legitimate clients is transmitted unencrypted with every packet. All Walter has to do (now that he has woken up) is wait for a legitimate client to connect, steal the client's MAC address, and spoof the address to connect with his own computer. Don't think that these measures are totally useless; they would probably prevent your curious neighbor from stealing your bandwidth, but they should not be confused with security.

This article has only covered security at the access point. Look for future articles about securing other aspects of a wireless network.

Upcoming Events

May 1: **Security on a Shoestring Budget**, Hurricane Labs Classroom, Independence, OH

May 22: **Check Point R70 Preview**, Hurricane Labs Classroom, Independence, OH

June 12: **Check Point R70 Preview**, Hurricane Labs Classroom, Independence, OH

Register for any of these events at www.hurricanelabs.com.

1: <http://en.wikipedia.org/wiki/802.11#Protocols>
2: <http://www.aircrack-ng.org/>
3: <http://www.renderlab.net/projects/WPA-tables/>

An increasingly common task that I have found myself working on lately is helping customers to profile their network usage. This typically comes about due to rulebase audits, installation of IDS devices, mysterious bandwidth usage, and application problems, but many other random things have also spawned full-fledge investigations into what is actually happening on the wire. At first it was a bit intimidating because there is so much data floating around on a network, how do you narrow it down into a useful chunk of information that can provide answers? It's all about using the right tools. That and grep/awk...they are your friends. :-) After working on a few of these projects I have grown to enjoy sniffing traffic and helping to solve mysteries of the ether, and I'd like to overview some of the tools that I have been using to accomplish this.

"Sniffing" port

This is perhaps the most valuable tool, which is required to properly use many of the other software tools to their full abilities. Commonly referred to as a Mirrored or SPAN⁴ port, it is a port on a switch that has been configured to have frames from other ports copied to it, so that it effectively sees the same traffic. Generally you can copy anywhere from a single access port through a list of ports, individual VLANs or several, or even just every port on the switch. Some of the tools which benefit most from a Sniffing port include Snort, NTOP, and tcpdump/wireshark.

Snort

A commonly used open source Network Intrusion Detection System, Snort⁵ is excellent for quickly alerting about certain traffic patterns which could indicate malicious activities. It also is

great to rat out people for using things like IM clients, games, Kazaa and other filesharing clients, webmail, or XXX-type materials. During the implementation of new IDS systems we are finding that the initial tuning phase is generally spent trying to understand what legitimate application traffic is causing harmless alerts.

Packet captures

These are easily the most important tools for troubleshooting and analyzing network traffic. Tcpdump⁶ is the most commonly used Linux command-line tool, where Wireshark⁷ (formerly known as Ethereal) is a popular GUI tool for both Windows and Linux. Tcpdump is, for me, a much easier way to capture the relevant data into a dump file for further processing. I can then 'replay' the file using tcpdump, or even import it into Wireshark to more easily follow the traffic for better analysis. Other related tools include netdump⁸, tcptrack⁹, and Check Point's fw monitor tool.¹⁰ The fw monitor command is found on Secure Platform systems and is a very nice upgrade to tcpdump, as it allows you to follow the routing of the traffic over several interfaces, where tcpdump only runs on one interface at a time. One disadvantage I find with fw monitor is that it does not show any ARP information, which is important to see when troubleshooting NAT related issues. Thankfully, Secure Platform also includes tcpdump, which does show ARP information. So between the two it all works out.

Bandwidth usage

This seems to be the most common reason to call us in to snoop a network. Usually people need to figure out: A) What is eating their bandwidth? Is it legitimate traffic or not?; and B) What is

the solution? Should they upgrade the circuit, install QoS, limit internet usage (install a proxy perhaps?), or move servers to remote locations to offload the traffic from the point-to-point. MTRG¹¹ is a commonly used tool for performing generic bandwidth usage graphs. You can monitor all of the interfaces of your networking equipment via SNMP to generate graphs what will show trends in overall usage. To see a more specific output of what is actually happening, NTOP¹² is a great tool. On Debian-based Linux machines it is very easy to install and it will automatically run a webserver that you can connect to, so that you may view the results. It generates graphs to show what type of traffic is flowing, what percentage of the overall usage each service is using, and which hosts are the most chatty (and with which other hosts). I think that everyone should have an NTOP server running on their network, to monitor what is happening and where.

Final thoughts

Your network is like your very own jungle, and to successfully navigate any jungle you need to have the appropriate tools available. I must ask you: How well do you know your jungle? After all, it is yours, so why not map it out to learn the habits of its inhabitants? The tools are readily and freely available. Having a well founded understanding of your network can really help to speed the troubleshooting process for many application issues, as well as help to avoid problems in the future by knowing early on what to expect. You may also discover a change from the norm one day that could indicate some potentially bad stuff, that other mechanisms are not catching. If this happens please let us know, we know some guys who can help. :-)

4: <http://www.cisco.com/warp/public/473/41.html#topic7-1>

5: <http://www.snort.org>

6: <http://www.tcpdump.org/>

7: <http://www.wireshark.org>

8: <http://www.rhythm.cx/~steve/devel/netdumpd/>

9: <http://www.rhythm.cx/~steve/devel/tcptrack/>

10: http://www.checkpoint.com/techsupport/downloads/html/ethereal/fw_monitor_rev1_01.pdf

11: <http://oss.oetiker.ch/mrtg/>

12: <http://www.ntop.org>

Doom and Gloom

or How to Hire the Right Gloomy Security Guy *from May 2008*

By: Bill Mathews

I'm usually the gloomiest guy in the room not outwardly of course but internally. I'm the guy always planning my escape should terrorists or zombies decide to strike whatever building I happen to be in. Make no mistake, I'm far more afraid of zombies than terrorists, I mean zombies are a fact of life. Self-preservation is an instinct we should all possess but many of us do not. When is the last time you worried about how you would escape from a zombie attack? Think about it.

Information Security can be thought of as your method of self-preservation when things go completely wrong. I'm not talking about just the big bad super hackers that are constantly stalking your network, but failures in general. Security people should be multi-disciplinarians and have some knowledge of several fields of IT. This should include development, databases, networks, etc. They should understand and be able to plan for failures of any variety and not just the big zombie attack.

Too many of us have a lot of security specific alphabet soups after our names. However, far too few of us have a deeper understanding of what is necessary to actually defend a network or application. It's one thing to understand the tenets of information security but someone somewhere MUST understand what it takes to make the network run before they can really figure out how to secure

it. Security is more a state of mind than a definable deliverable. It's more a method of thinking about "what if...this happens" and being able to plan for it.

So, what does this all mean? What am I getting at? Fire all the CISSPs? Well sure, it's a start I suppose. More importantly what I'm saying is that when you interview a security person, when you're reviewing your current security person, ask them some important questions. Questions like, "Okay Mr. Security Guy, CISSP. You're on the fourth floor of a building, zombies have surrounded the doors. You have an ax, a shotgun, chewing gum, and some gasoline. How do you escape?" The answer will tell you whether this person has the right frame of mind to really secure a network or is just trying to fool you into believing he does.

Pen Tests as a Learning Experience

from October 2008

By: Steve Benson

There are a lot of different attitudes and expectations clients have for penetration tests. Many people think of a penetration test as quality assurance, expecting the result of the test to be a simple yes or no answer to the question "is this software bug-free?" (or at least security bug-free).

There is a problem with this thought: The penetration tester cannot possibly determine whether any given software is completely free of bugs in a typical penetration test. That would at least require the source code which we (as penetration testers) are rarely given in the typical penetration test. Sometimes further adding to this obscurity are vague error messages or a lack of experience on the penetration tester's part with the application or framework in question.

These conditions often lead penetration testers to report something in between "pass" and "fail". For instance, I'll report that while I was not able to exploit a particular piece of software, it has some suspicious behavior which I recommend changing. I will make such recommendations if I suspect that someone with more time or better knowledge of the application or its surrounding software environment might be able to exploit it.

I think that more bugs can be found and fixed if penetration tests are thought of as education rather than a simple "pass/fail" result. For example, if a vulnerability is found, think about how and why it was exploited. If a recommendation is made about something that we could not exploit, think about what else the pen tester might need to actually exploit the vulnerability and who else might have that. One of the things a penetration test gets you is not only the actual test and report, but the ability to ask questions of someone with a different perspective. Thinking about a penetration test this way can lead to far more improvements than simply the correction of the actual bugs that the test finds.

Links

Website: <http://hurricanelabs.com/>

Blog: <http://blog.hurricanelabs.com/>

Twitter: <http://twitter.com/hurricanelabs>

Facebook: <http://www.facebook.com/pages/Independence-OH/Hurricane-Labs/45588867073?ref=share>

Every month you read this newsletter and hopefully learn something new or interesting about securing your network. But what about physical security? We all know about the badge that gets you in the building and the cameras that can see your computer screen while you're streaming usopen.com to see Tiger win again. I'm talking about the data that walks out the door every night and you only hope will return the next morning...laptops.

Everyday we as network/security administrators trust our users to leave the building with login credentials, customer data, or personnel information. I find it amazing considering we barely trust our user population to put a URL into a browser window. How often do these laptops sit in the car overnight or sit unlocked at Starbucks while John Q. User goes to the restroom? What I find

even more amazing is that we LET THEM do this. It's not that we don't try to keep them from doing these things; but we know it's going to happen and we still let them walk out the door every night. My suggestion, flying tackle them as soon as they hit the front door and wrestle the laptop bag out of their arms...j/k. Something does need to be done though.

The most obvious answer is disk encryption. There are enough encryption products out there that something will work well for you and your situation. I'm sure there will be the normal hassle from the budget people or maybe you'll be forced to convince the Bobs that this is necessary. Have them consider the implications if your data falls into the wrong hands, and don't think that there isn't someone out there who wants it. Trust me, there is.

In addition to encryption, you should beat it into the heads of your users that taking care of these laptops is essential. Don't leave them in your car. Don't leave the screen unlocked and walk out of sight. Use a laptop lock always. These are common sense things that never get done.

If you have questions about encryption, google it or call us. We're all more than willing to help you keep your network secure. The downfalls of not having encryption far outweigh the work/money that it takes to implement it. We are far too reliant on the people who take these laptops home to secure them. In the end, it is not the job of the person who takes the laptop home to secure the data on it (it is their responsibility to keep them safe though). It's your job to keep them secure.



Hurricane Labs
4401 Rockside Road, Suite 310
Independence, Ohio 44131
216-923-1330
www.hurricanelabs.com



What's New? Hurricane Labs has MOVED! Due to the need for more space and future expansion, Hurricane Labs has moved to the 3rd Floor of their current building. Their classroom has also moved to the third floor. Feel free to visit our new space the next time you're in the area. The new suite number is 310!