A Free Publication on Information Security from Security Horizon, Inc.

the security journal

"Common Sense Security for Common Businesses"

Making good choices for the future...

Where do we go from here?

Second Anniversary Edition

Volume 9 - Fall 2004 Edition

Security Horizon

5350 Tomah Drive
Suite 3500
Colorado Springs, CO
80918
http://www.securityhorizon.com

Editor in Chief: Russ Rogers
Layout Editor: Michele Fincher

The *Security Journal* is always looking for quality writers for this publication. If you're interested in submitting an article for an upcoming edition of The Security Journal, please contact Russ Rogers at russr@securityhorizon.com.

Special thanks go out to Ping Look from **Look Designs** for the creation of the new Security Horizon logo and the new cover masthead images for The Security Journal.

For more information on Look Designs:
www.republicofping.com
design@republicofping.com

For more information on Security Horizon, please visit our web site or email us at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is headquartered in Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents:

Upcoming Black Hat® Events

Black Hat Singapore 2004
Training: October 11-12

Black Hat Japan 2004
Briefings: October 14-15

Black Hat Europe 2005
Briefings & Training:
March 29-April 1

Black Hat USA 2005
Briefings & Training:
July 25-28

For more information, please go to
www.blackhat.com

Notes From the Editor

Russ Rogers
CISSP, CISM
Editor in Chief

Have you ever noticed how people just seem to get very comfortable in their existence? My dad used to warn me 'not to get stuck in a rut'. To him it meant that I needed to try a lot of different things and find one that I really enjoyed doing so that when I went off to college, I'd be a success. Honestly, at the time, I never really understood what he meant or how particularly far reaching that statement was. That one statement actually touches on facets of my world that I would have never considered before. Today, I look across the span of humanity and it's fairly easy to see how we've fallen into a day-to-day haze, where only the thought of a tropical vacation seems to break us from the norm.

Well, folks, the same thing is happening in law enforcement and information security. Consider the forensics and incident response methodologies used within law enforcement. How much have they really changed over the last five years? In contrast, how much has technology changed in that same five year time span? If an individual is not in an industry that requires constant update and evolution, then their minds lose their edge.

The key here is that the folks that want into your system love research and development. They genuinely enjoy the puzzle associated with breaking things or making them perform actions that were never originally intended. This, in turn, leads to the evolution of technologies that are more mature and robust at breaking into systems than those products intended to protect our systems.

Now, don't get me wrong. There are some great products starting to come out on the marketplace, but to some degree our challenge comes when we try to think outside the box. Most of the technological advances of today are simply extensions of previous technologies. For instance, we progressed from technologies that allow us to *sniff* network traffic and see everything on the line to the creation of technologies that *sniff* for us and tell us when something unusual occurs; these are called Intrusion Detection Systems, or IDS. From here we've added the capabilities of earlier firewall products to block that network traffic when we decide we don't like it. The point I'm trying to make is that our defensive mindset is based on a path from our previous technologies. That's not truly thinking outside the box, it's a derivative mindset.

But Hackers, both good and bad, do not think along those same lines and that's where we, as security professionals, get ourselves into hot water. We're fighting a war that pits our intellectual content against someone else's. We have rules, both legal and ethical, that control our actions. They do not. And they're in a constant state of technological innovation, whereas many modern information security product and application companies are 'in it for the money'. That's not intended to be a derisive statement, it's simply the truth.

So, if we have this problem, what's the solution? The solution is growth. The solution is to step past all the things we've done in the past without ignoring the lessons we've learned along the way. We need to adopt the mindset of the traditional hacker, where experimentation, speculation, hypothesis, and testing are a way of life. There are security issues coming down the pipe that will require

Notes From the Editor, cont.

us to think harder and more creatively about the solutions we implement.

This is the first issue of our third year in electronic publication and our readership has grown beyond anything I would have ever imagined when I did the layout for the original. I've asked some very smart people to participate in this issue of the Security Journal because I wanted to make a point that we, as a community, both professionals and laypeople, need to accept what we've done in the past as good, but not necessarily marry ourselves to those ideas as the only means to our end. Think creatively. Consider the possibilities. What potential does the future hold for our technologies? Think like your adversary. Don't be morally offended that someone else is trying to understand what *could be*. It doesn't make them a bad person, nor would it make you a bad person. It's that particular mindset that consistently breaks new ground. Think of it as yoga for your mind.

Peace,
Russ Rogers

Empower your organization with CryptoLex Mobio®.

One device that unifies business processes and enables complete systems integration.

One device that securely accesses all networks and doors, including VPNs and the Internet.

One device that eliminates the need to remember multiple passwords and access codes.

One device that operates remotely, through computers, PDAs and cell phones.

One device that can't be stolen.

One device that can only be used by you.

One solution, less risk.

Mobio is the Power of One™—one ultimate solution to improve business processes, productivity, and information flow by empowering individuals and organizations with secure communication and transaction capabilities. With Mobio, passwords, smart cards and ID tokens are rendered obsolete. Mobio unifies disparate networks, systems and security devices into one complete portable biometric authentication solution.

The Power is Yours.

CryptoLex is actively recruiting four strategic partners for a unique program to begin November 1, 2004. Be the first on your block to unify physical and virtual security with the only authentication device worthy of the task.

All participating organizations will become part of our Security Innovation showcase at the Wireless Mobio official launch in Q1 2005.

Contact

Clovis Najm – VP Sales and Marketing
Mobile: 613.293.7311
Phone: 301.862.5312
Fax: 301.862.5315
www.cryptolex.com
44425 Airport Road - Suite 110
California, Maryland 20619 USA

(CRYPTOLEX)

GSS Security Education Project

By: Greg Miles

The security profession has evolved over the last two decades. The technology available at our fingertips today is scary by comparison even from just five years ago. Many colleges have seen a money making opportunity in creating security related certificate or degree programs.

However, there is not a well defined path for getting future (and even current) security professionals the types of curriculum that will benefit them most from career perspective. There is a trend starting toward certificates, bachelor degree programs, and master's degree programs in computer security. Some are well structured, while others are just an over glorified hacking class.

The purpose of the GSS Security Education Project is two fold: 1) Present ideas and concepts related information security education, and 2) Stimulate discussion around what should we be teaching "up and coming" security professionals and at what point in their education. This project is an effort designed to address the security education needs of the security community. It is not focused on making a security person an expert in every aspect of security, but on giving individuals with the desire to become a security professional a baseline of knowledge necessary to be successful in not only what is taught, but the ability to pursue additional knowledge either through self research or additional training and educations.   The primary idea behind the Security Education Project is to create an open source recommended curriculum that can be adopted by colleges and universities as a as a basis for establishing their security education programs. As a side affect of this effort, the GSS hopes to also incorporate a basic security education program for high school aged individuals interested in computers, networking, and computer security.

As a security professional and an instructor within a security degree program, I see a serious disconnect between what colleges and universities are teaching in their programs and what some believe is needed in the way of understanding the underlying concepts of security in a business or operational environment. Although I strongly agree the best experience is hands-on experience, I do believe that university programs can be better structured to prepare students with the basic skills to prepare to work as a security professional. From my experience I have noticed that security professionals have grown mostly from their job experience, not from formal education. Most security professionals have had technical jobs, technical degrees, or government security experience. The basis of formal credentials for the security professional have primarily been based on certifications (CISSP, Security +, CISA, etc.).

GSS Security Education Project, cont. By: Greg Miles

Goals: This project is meant to provide security professionals with an opportunity to provide their professional input into the evolution of a best practice in security education.

Results: The end result will be an open source curriculum that will be available for any instructor, college or university to review when implementing their security programs. Results of the discussions will be posted on the Global Security Syndicate website. (www.gssyndicate.org)

What is Needed: Volunteers to participate in the discussions and provide input into the best security topics, teaching strategies, and best practices that need to be made available as recommendations for this curriculum.

Greg Miles, Ph.D. CISSP, CISM is a co-founder of both Security Horizon and the Global Security Syndicate.

About the GSS: The Global Security Syndicate (GSS) is a global, not for profit, organization of security professionals and companies (products and services) dedicated to advancing Information Security practices for all levels of business and government agencies by:

- Knowledge sharing through collaborative effort of local community and industry research projects
- Increasing global security awareness and education
- Developing secure strategies and standards to enhance the security lifecycle of security programs and products

For more information, contact Greg Miles at greg@gssyndicate.org, www.gssyndicate.org

GSS

GLOBAL SECURITY SYNDICATE

Why do you think they call it a Master's degree?

Any Master's degree puts you in an elite group. But a Master's from the University of Advancing Technology puts you in a powerful group.

Regardless of your college major, the single best move to make you more valuable is to gain proven understanding and expertise in technology.

The Master's of Science in Technology from UAT will greatly increase your recognition and prepare you for a higher level of leadership. You can customize your program to match your career goals. And, you can finish your Master's in a year and a half – online or on-campus in Tempe.

Master majors such as:

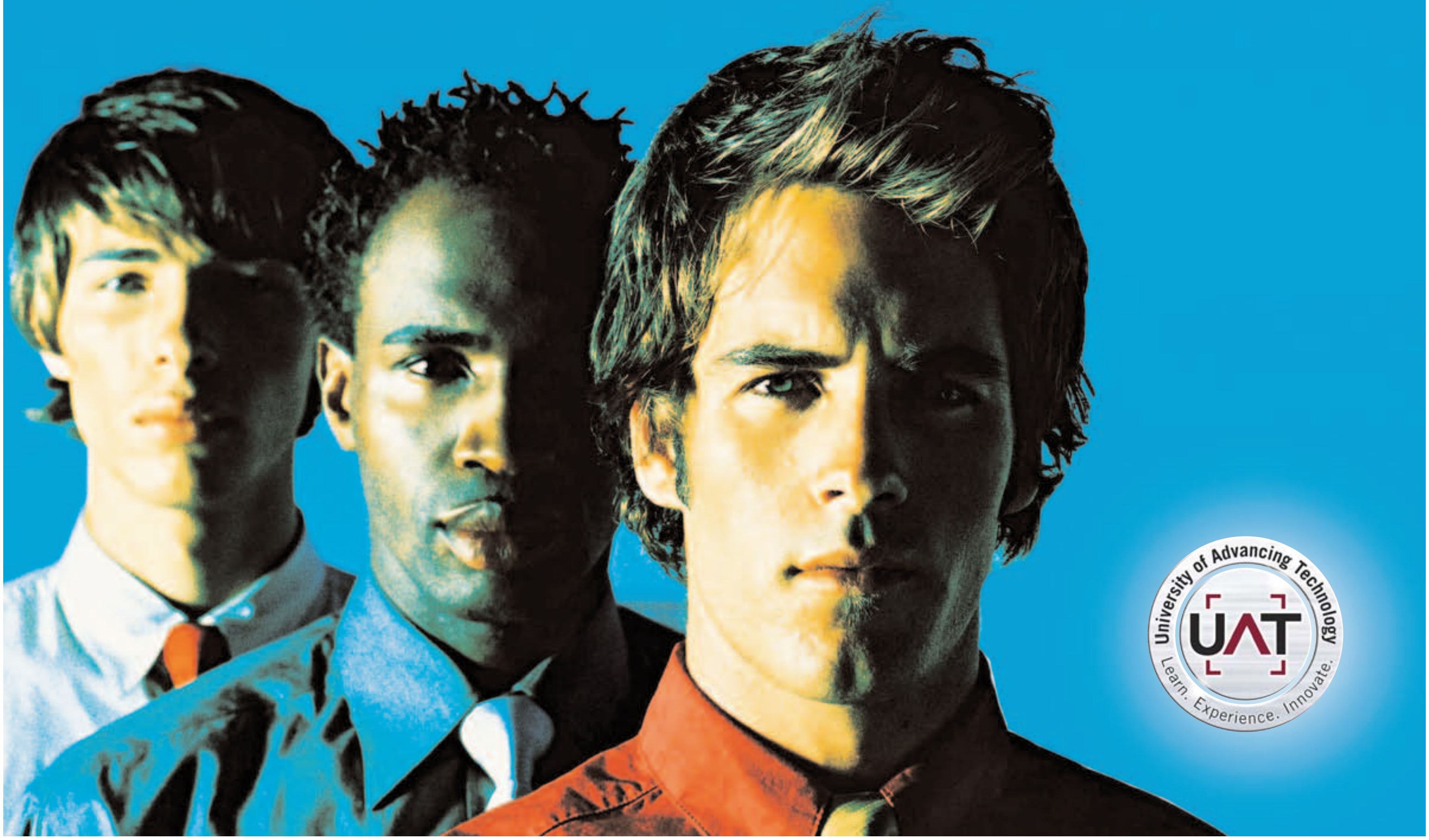
- Artificial Life
- Networking/Security/MIS
- Human Computer Interaction

…or customize your own

Learn more.

2625 W. Baseline Rd. > Tempe, AZ 85283
Phone 800.658.5744 > Fax 602.383.8222

www.uat.edu/masters



University of Advancing Technology
UAT
Learn. Experience. Innovate.

Airjack and WEPlab: Should You Believe the Hype? By: Chris Hurley

WEP is flawed...

Background

A few days ago I was involved in a conversation on the NetStumbler forums about cracking Wired Equivalent Privacy (WEP) keys on 802.11x networks. I have always maintained that even though WEP is flawed, it is strong enough for the home user but should never be used on a commercial or government WLAN. The authors of a two new WEP cracking tools disagreed with my statements citing relatively new methodologies for cracking WEP keys.

WEP is Flawed

Scott Fluhrer, Itsik Mantin, and Adi Shamir initially detailed the flaws in WEP in their paper Weaknesses of the Key Scheduling Algorithm of RC4 (downloads.securityfocus.com/library/rc4_ksaproc.pdf). They discovered that because WEP uses a fixed secret key, weak initialization vectors are sometimes generated to encrypt WEP packets. After enough weak initialization vectors have been captured, the secret key can be cracked. Several tools were released that took advantage of this weakness, the most popular being WEPCrack and AirSnort. The greatest hurdle an attacker had to cracking the WEP key was the amount of traffic that had to be captured in order for a WEP key to be cracked. WEPCrack (and AirSnort) required about 2000 weak initialization vectors to crack the key. Because not every initialization vector is weak, this could take weeks or months to collect depending on the network load.

A New Way

The initial release of WEP cracking tools did not fully realize the potential for cracking WEP keys, in part because all of the potential weak initialization vectors were not taken into account. Dwepcrack by h1kari optimized the attack even further, bringing WEP cracking closer to a realistic attack method. In the summer of 2004, Korek further expanded this with a new statistical attack designed to quickly crack WEP keys and brought it to light on the NetStumbler forums. This attack, called chopping, involves taking a WEP packet and chopping off the last byte. The CRC/ICV is broken so if the last byte is 0, the last four bites should be xored with a certain value. The CRC will become valid again. Retransmit the packet. If it does not get through then if the last byte is 1. This method has been implemented by two relatively new WEP cracking tools, airjack (by Devine) and weplab (by Topo [LB]).

New Tools

In order to test the effectiveness of these tools I set a WEP key on my home access point (Linksys WRV54G) that was generated with a strong passphrase. Both tools claim that the key can be cracked with somewhere around

Airjack and WEPlab, cont. By: Chris Hurley

500,000 unique initialization vectors. This equates to somewhere in the neighborhood of 1.5 million packets.

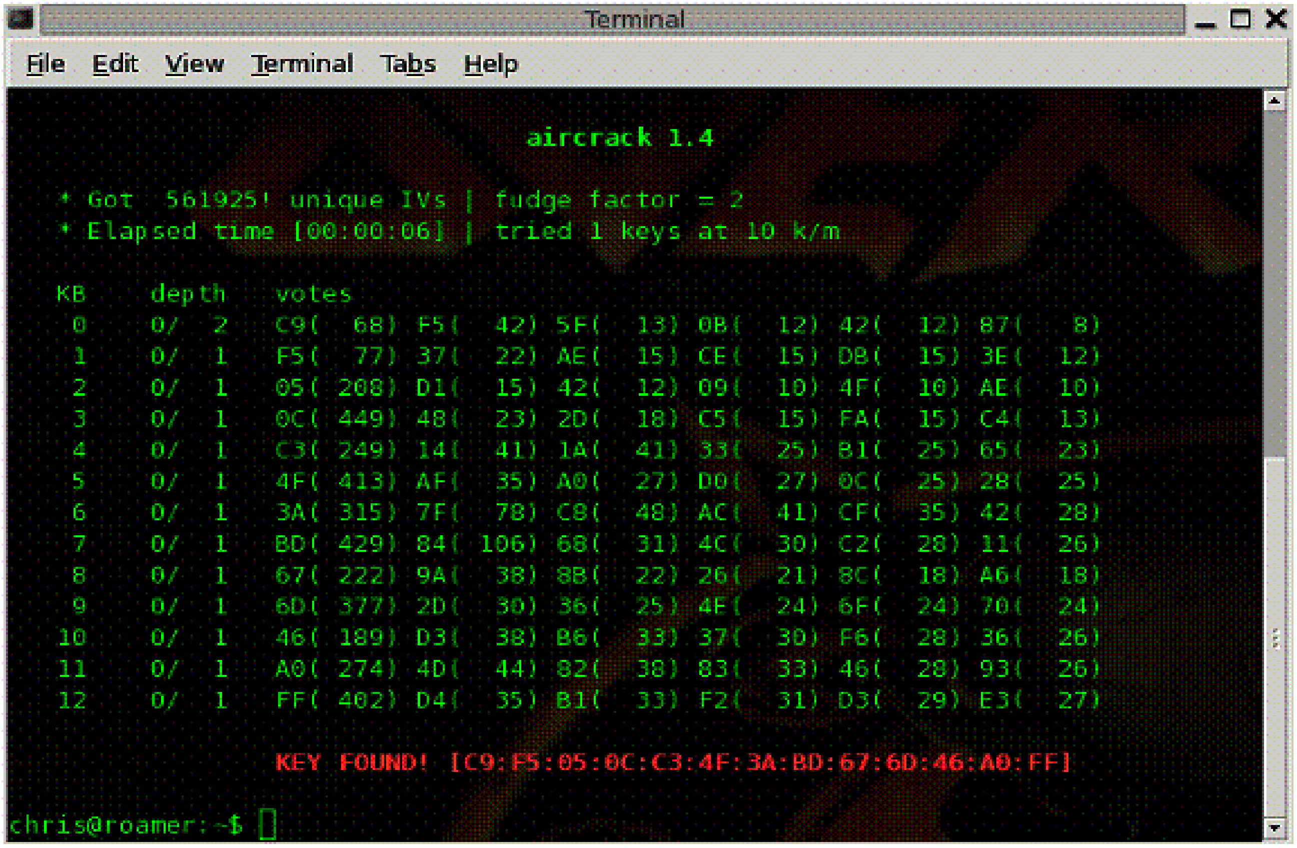
As I started gathering packets (using airodump, which is included with aircrack) I quickly realized that one problem remained. Getting enough packets. Under normal use (which for me is significantly more than the 'average' user) it would have taken me a week or more to gather 500,000 unique initialization vectors. I decided to start adding some traffic to my network. I established several outbound connections (irc, instant messenger, mail, etc) and started downloading large files (Linux iso's from multiple sites). This activity allowed me to quickly increase the amount of time to get 500,000 initialization vectors. In the end, it took about 10 hours to gather enough traffic to try the attacks. An attacker utilizing a replay attack could simulate this type of activity. In a replay attack an attacker captures an AddressResolution Protocol (ARP) packet and repeatedly sends it back to the router/ access point. This will generate additional traffic and can be used to speed up collection.

After my 10 hours it was time to put the tools to the test. First I tried aircrack. Usage of aircrack is pretty simple. The command line argument to run it against my capture file (wlancap.pcap) was simply

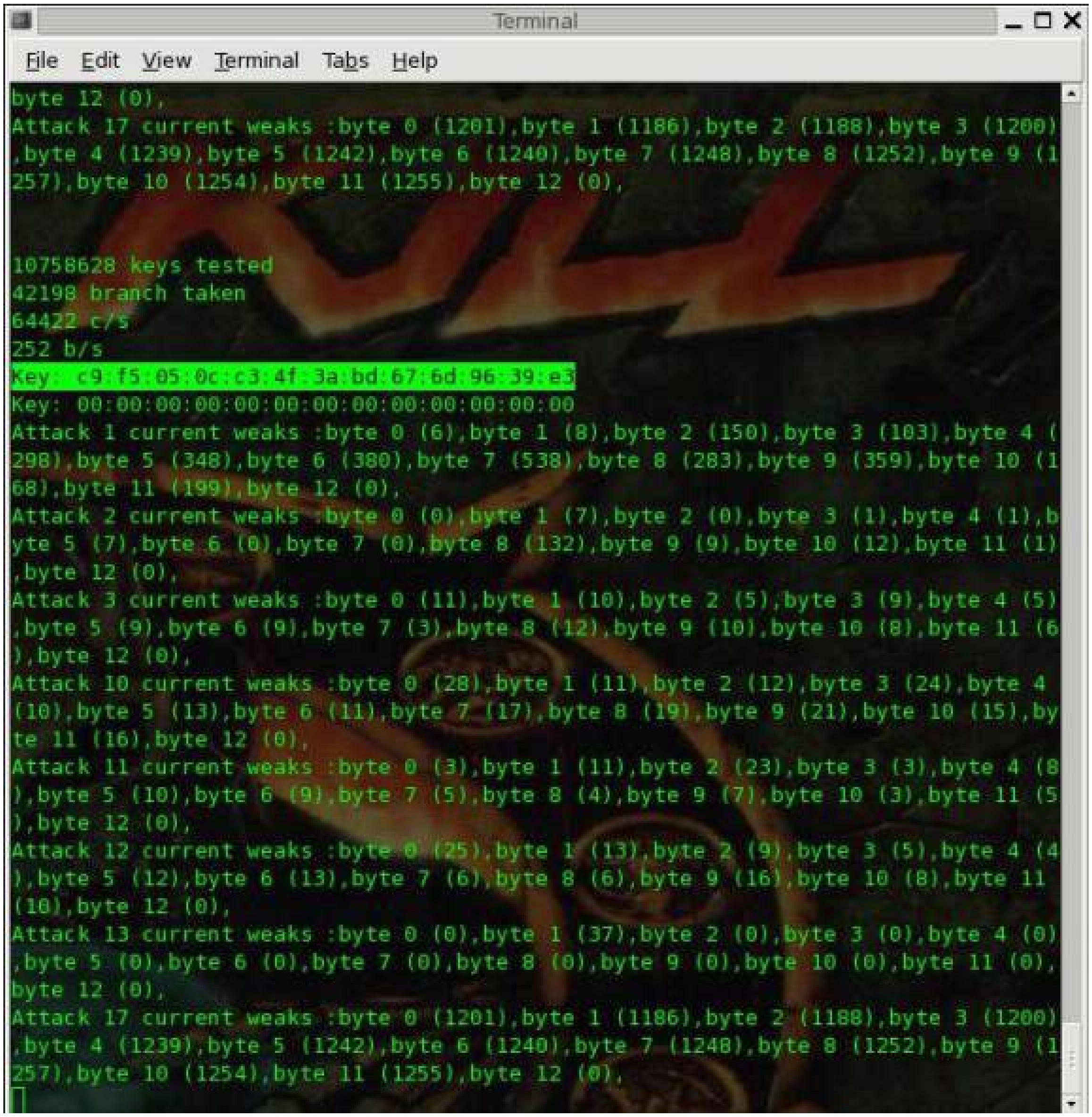
aircrack ./wlancap.pcap

This command attempts to crack the key of the first encrypted network in the capture file (which happened to be mine). It is also possible to specify the BSSID of a specific network with the –b flag.

I expected that it would be able crack the key eventually. I did not expect it to crack the key in 6 seconds!



```
                          aircrack 1.4

   * Got  561925! unique IVs | fudge factor = 2
   * Elapsed time [00:00:06] | tried 1 keys at 10 k/m

   KB     depth    votes
    0     0/  2    C9(  68) F5(  42) 5F(  13) 0B(  12) 42(  12) 87(   8)
    1     0/  1    F5(  77) 37(  22) AE(  15) CE(  15) DB(  15) 3E(  12)
    2     0/  1    05( 208) D1(  15) 42(  12) 09(  10) 4F(  10) AE(  10)
    3     0/  1    0C( 449) 48(  23) 2D(  18) C5(  15) FA(  15) C4(  13)
    4     0/  1    C3( 249) 14(  41) 1A(  41) 33(  25) B1(  25) 65(  23)
    5     0/  1    4F( 413) AF(  35) A0(  27) D0(  27) 0C(  25) 28(  25)
    6     0/  1    3A( 315) 7F(  78) C8(  48) AC(  41) CF(  35) 42(  28)
    7     0/  1    BD( 429) 84( 106) 68(  31) 4C(  30) C2(  28) 11(  26)
    8     0/  1    67( 222) 9A(  38) 8B(  22) 26(  21) 8C(  18) A6(  18)
    9     0/  1    6D( 377) 2D(  30) 36(  25) 4E(  24) 6F(  24) 70(  24)
   10     0/  1    46( 189) D3(  38) B6(  33) 37(  30) F6(  28) 36(  26)
   11     0/  1    A0( 274) 4D(  44) 82(  38) 83(  33) 46(  28) 93(  26)
   12     0/  1    FF( 402) D4(  35) B1(  33) F2(  31) D3(  29) E3(  27)

                   KEY FOUND! [C9:F5:05:0C:C3:4F:3A:BD:67:6D:46:A0:FF]

chris@roamer:~$
```



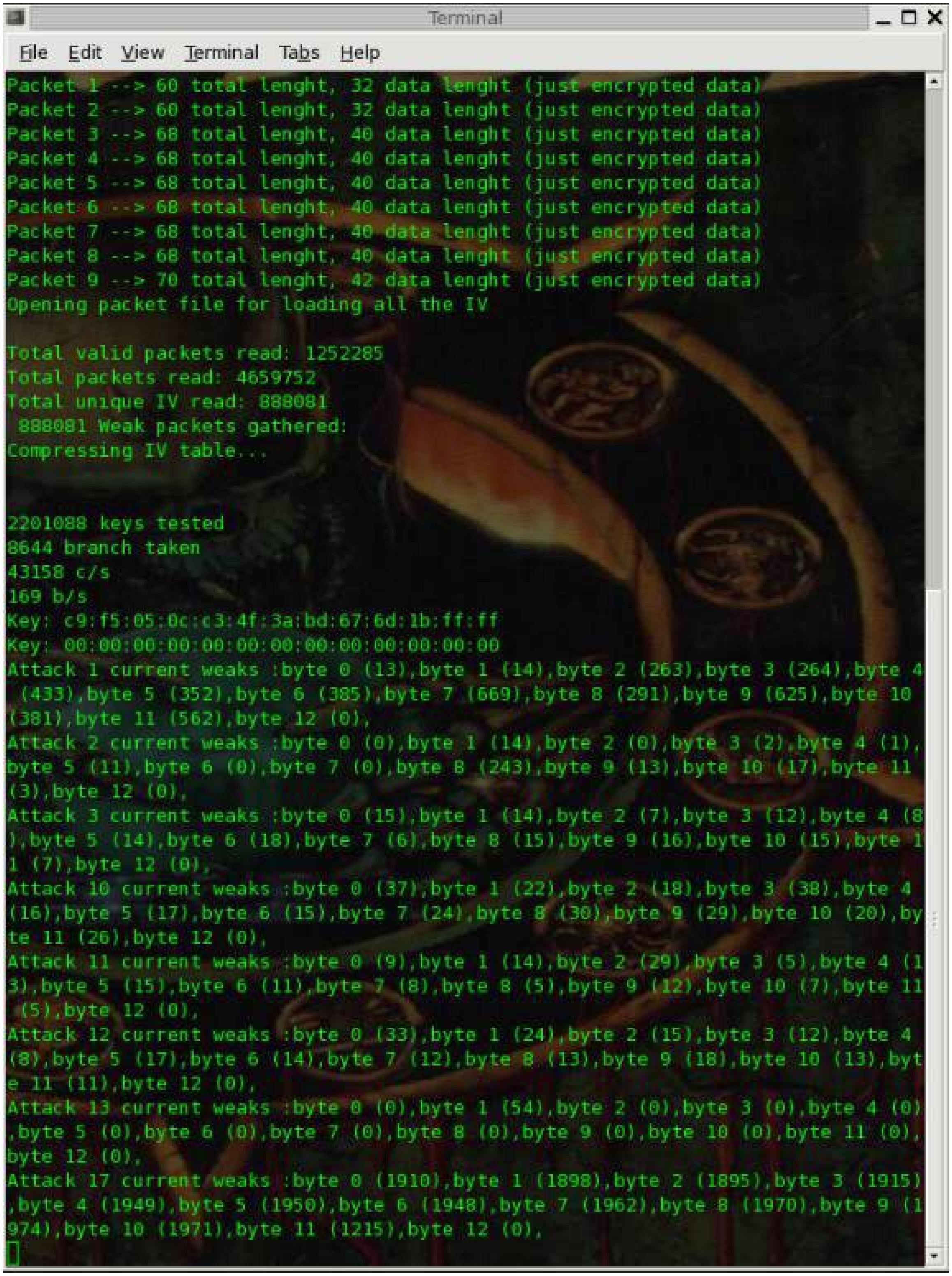
```
byte 12 (0),
Attack 17 current weaks :byte 0 (1201),byte 1 (1186),byte 2 (1188),byte 3 (1200)
,byte 4 (1239),byte 5 (1242),byte 6 (1240),byte 7 (1248),byte 8 (1252),byte 9 (1
257),byte 10 (1254),byte 11 (1255),byte 12 (0),


10758628 keys tested
42198 branch taken
64422 c/s
252 b/s
Key: c9:f5:05:0c:c3:4f:3a:bd:67:6d:96:39:e3
Key: 00:00:00:00:00:00:00:00:00:00:00:00:00
Attack 1 current weaks :byte 0 (6),byte 1 (8),byte 2 (150),byte 3 (103),byte 4 (
298),byte 5 (348),byte 6 (380),byte 7 (538),byte 8 (283),byte 9 (359),byte 10 (1
68),byte 11 (199),byte 12 (0),
Attack 2 current weaks :byte 0 (0),byte 1 (7),byte 2 (0),byte 3 (1),byte 4 (1),b
yte 5 (7),byte 6 (0),byte 7 (0),byte 8 (132),byte 9 (9),byte 10 (12),byte 11 (1)
,byte 12 (0),
Attack 3 current weaks :byte 0 (11),byte 1 (10),byte 2 (5),byte 3 (9),byte 4 (5)
,byte 5 (9),byte 6 (9),byte 7 (3),byte 8 (12),byte 9 (10),byte 10 (8),byte 11 (6
),byte 12 (0),
Attack 10 current weaks :byte 0 (28),byte 1 (11),byte 2 (12),byte 3 (24),byte 4
(10),byte 5 (13),byte 6 (11),byte 7 (17),byte 8 (19),byte 9 (21),byte 10 (15),by
te 11 (16),byte 12 (0),
Attack 11 current weaks :byte 0 (3),byte 1 (11),byte 2 (23),byte 3 (3),byte 4 (8
),byte 5 (10),byte 6 (9),byte 7 (5),byte 8 (4),byte 9 (7),byte 10 (3),byte 11 (5
),byte 12 (0),
Attack 12 current weaks :byte 0 (25),byte 1 (13),byte 2 (9),byte 3 (5),byte 4 (4
),byte 5 (12),byte 6 (13),byte 7 (6),byte 8 (6),byte 9 (16),byte 10 (8),byte 11
(10),byte 12 (0),
Attack 13 current weaks :byte 0 (0),byte 1 (37),byte 2 (0),byte 3 (0),byte 4 (0)
,byte 5 (0),byte 6 (0),byte 7 (0),byte 8 (0),byte 9 (0),byte 10 (0),byte 11 (0),
byte 12 (0),
Attack 17 current weaks :byte 0 (1201),byte 1 (1186),byte 2 (1188),byte 3 (1200)
,byte 4 (1239),byte 5 (1242),byte 6 (1240),byte 7 (1248),byte 8 (1252),byte 9 (1
257),byte 10 (1254),byte 11 (1255),byte 12 (0),
```

Next, I moved to weplab. I initially tried with the same capture file that I had used with aircrack. The command line arguments are not as intuitive with weplab:

weplab -r ./wlancap.pcap -s 3 —perc 100 —key 128 —fcs —debug 1 ./wlancap.pcap

It was unable to crack the WEP key. Weplab came very close, capturing 10 of the 13 Key Bytes almost immediately. But as minutes dragged into hours I decided to capture more packets and try again.

I tried periodically with the same results, the 11th Key Byte was not being cracked successfully. I changed the command line options (particularly the fudge factor and probability) but this didn't help. In fact, with some of the options weplab returned without cracking the key and instructed me to get more packets. After capturing over 888,000 unique initialization vectors, I gave up.



```
Packet 1 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 2 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 3 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 4 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 5 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 6 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 7 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 8 --> 68 total lenght, 40 data lenght (just encrypted data)
Packet 9 --> 70 total lenght, 42 data lenght (just encrypted data)
Opening packet file for loading all the IV

Total valid packets read: 1252285
Total packets read: 4659752
Total unique IV read: 888081
 888081 Weak packets gathered:
Compressing IV table...


2201088 keys tested
8644 branch taken
43158 c/s
169 b/s
Key: c9:f5:05:0c:c3:4f:3a:bd:67:6d:1b:ff:ff
Key: 00:00:00:00:00:00:00:00:00:00:00:00:00
Attack 1 current weaks :byte 0 (13),byte 1 (14),byte 2 (263),byte 3 (264),byte 4
 (433),byte 5 (352),byte 6 (385),byte 7 (669),byte 8 (291),byte 9 (625),byte 10
(381),byte 11 (562),byte 12 (0),
Attack 2 current weaks :byte 0 (0),byte 1 (14),byte 2 (0),byte 3 (2),byte 4 (1),
byte 5 (11),byte 6 (0),byte 7 (0),byte 8 (243),byte 9 (13),byte 10 (17),byte 11
(3),byte 12 (0),
Attack 3 current weaks :byte 0 (15),byte 1 (14),byte 2 (7),byte 3 (12),byte 4 (8
),byte 5 (14),byte 6 (18),byte 7 (6),byte 8 (15),byte 9 (16),byte 10 (15),byte 1
1 (7),byte 12 (0),
Attack 10 current weaks :byte 0 (37),byte 1 (22),byte 2 (18),byte 3 (38),byte 4
(16),byte 5 (17),byte 6 (15),byte 7 (24),byte 8 (30),byte 9 (29),byte 10 (20),by
te 11 (26),byte 12 (0),
Attack 11 current weaks :byte 0 (9),byte 1 (14),byte 2 (29),byte 3 (5),byte 4 (1
3),byte 5 (15),byte 6 (11),byte 7 (8),byte 8 (5),byte 9 (12),byte 10 (7),byte 11
 (5),byte 12 (0),
Attack 12 current weaks :byte 0 (33),byte 1 (24),byte 2 (15),byte 3 (12),byte 4
(8),byte 5 (17),byte 6 (14),byte 7 (12),byte 8 (13),byte 9 (18),byte 10 (13),byt
e 11 (11),byte 12 (0),
Attack 13 current weaks :byte 0 (0),byte 1 (54),byte 2 (0),byte 3 (0),byte 4 (0)
,byte 5 (0),byte 6 (0),byte 7 (0),byte 8 (0),byte 9 (0),byte 10 (0),byte 11 (0),
byte 12 (0),
Attack 17 current weaks :byte 0 (1910),byte 1 (1898),byte 2 (1895),byte 3 (1915)
,byte 4 (1949),byte 5 (1950),byte 6 (1948),byte 7 (1962),byte 8 (1970),byte 9 (1
974),byte 10 (1971),byte 11 (1215),byte 12 (0),
```

All told I generated and captured traffic for over 24 hours. It should be noted that weplab is acknowledged by the author to be in beta at this time, and cracking WEP keys isn't an exact science to begin with, so it may have been possible to get the key by continuing to change the command line options.

Airjack and WEPlab, cont.

By: Chris Hurley

Conclusions

Someone made the statement that these new tools had taken the theoretical and made it practical. I think to a large degree that is a fair statement. However, these tools continue to suffer from the problem of gathering enough packets to crack the key. Since replay attacks can be used by an attacker to generate traffic, it is now possible to crack WEP keys in a relatively short period of time.

If possible, you should use WiFi Protected Access (WPA) on your WLAN. Home users will still find better protection using WEP as a deterrent, but corporate or government networks should not even consider using WEP on their wireless networks, but that has always been the case.

Chris Hurley is a Senior INFOSEC Engineer with Assured Decisions, LLC in Columbia, MD and is the author of “WarDriving: Drive, Detect, Defend” from Syngress Publishing. His experience ranges from Security Engineering and Architecture to vulnerability assessments and penetration testing on both wired and wireless networks. In addition to running the WorldWide WarDrive he organizes the annual DefCon WarDriving contest.

hack
wire
FBI

Biometrics and the Advancement of Computing

By: Clovis Najm

Most people understand the concept of biometrics but are hard-pressed to see practical applications. Why would the average person need a Star Wars-like device to digitally transmit fingerprints, retinal or facial scans to gain access to top security buildings and computers? Recently, biometrics has been thrust into the mainstream via TV shows and movies like *Minority Report* and *I, Robot*. Even though, the general public may not be aware the concept of and practical use for biometrics has been ongoing for decades. Most recently a number of innovative companies have turned their attention to enabling and installing biometrics for everyday use. In a world overrun with identity theft, fraud and security breaches, biometrics may be the silver bullet everyone has been waiting for. But adoption of this technology is slow. This could be partially due to technological limitations, fear of change, perceived cost and implementation challenges, however, the lag of adoption can be overcome with awareness and education around the elements of biometric authentication and the processes involved.

Proof of identity (authentication) is part of our everyday lives and its necessity is growing at a rapid rate. Think of all the cards in your wallet and what each is used for. Think of all the networks those cards access to allow you to get on with the business of living. You need a passport to board a plane. You need a driver's license to legally operate your vehicle. You need an access card to get into your office. You need your bank card to get cash from an ATM while your credit card allows you to make purchases online or over the phone. Most of these authentication "devices" require passwords, access codes and PINs. We are required to remember multiple passwords especially for banking, telephone and Internet transactions. As a society we are now required to operate as a "system" and we must interact with other system to get our business done. Interaction between systems requires some form of authentication. Unfortunately, present-day authentication techniques are riddled with weaknesses and limitations. Most authentication devices are "transferable", which means they can be lost or stolen or hacked or misused. Some might argue that weak authentication is the root cause of the $5 billion identity theft problem in the United States.

Biometrics has the capability to address and overcome the weaknesses inherent in other forms of authentication. Traditionally, we utilize biometrics everyday in the form of face-to-face contact, eye witness testimony, DNA screening, and signing documents and credit card receipts. Biometrics is our most important and powerful form of authentication because it is based on building a trust chain between individuals and organizations. Biometrics is the most definitive proof of identity in a court of law. Traditional biometric processes work extremely well and are heavily relied upon by society as biometric information is "non-transferable" – your physical person can't be stolen. Your proof of identity is absolute. This is a requirement for productive, safe and reasonable human interaction. So, what happens when there is no face-to-face contact? No photo IDs with signatures to verify? How do you prove you are who you say you are? How do you safely and securely interact, transact and authenticate in the world of computing?

Biometrics has been an underutilized human component for computing and online transactions due to one large hurdle - the Internet. Biometrics and the Internet have not yet been connected. The Internet is the largest network in the world; however, Internet technologies are being used to connect multiple sites and systems. We can, therefore, define Internet technologies as shared networking – enabling systems while not being directly connected via cable to a central host. Buildings are being wired with Ethernet and TCP stacks, appliances are manufactured with IP addresses, and wireless technologies linking everyone to a network including the Internet. Business depends on the Internet to operate internally and interact externally.

Expansion is fueled by decreased cost, increased speed of communication, and more efficient information sharing. The cost is substantially lower for shared computing because bandwidth is spread between different applications ensuring optimal use. The Internet enables communications and information sharing to touch every corner of the globe. Essentially, the Internet is becoming a faster more efficient virtual replica of our daily lives. Internet technologies are now able to connect systems and employees to organizations from remote locations. Human interaction for transactions and general business are now conducted online.

Zeros and ones are presently used to authenticate these interconnected systems and their users. This authentication protocol can easily be falsified, copied and transferred at high speed – creating an enormous security problem. The Internet and its technologies are designed for sharing – naturally open for anyone to copy – which creates havoc for authentication systems not designed for unsecured dispersed networks. New systematic identity theft schemes are possible because everything is connected and most network endpoints are typically protected by a simple password. Passwords are universally regarded to be the weakest form of authentication. In such a high risk environment, wouldn't strong biometric authentication be a logical solution?

Currently the answer is a resounding, no. Layer upon layer of complexities exist in the biometric arena that make make implementation virtually impossible. Strong authentication in the physical world requires physical interaction to initiate. Biometrics are different – the challenge becomes how to effectively enable secure personal and digital identification through a network.

People carry their biometric data with them. Therefore, scanning devices require one of two criteria: 1. The individual must have visited the scanner before. 2. Biometric scanners must be networked. The first situation is problematic given the many potential entry points into a network. The second, however, is very possible given shared network environments like the Internet. The practical side of such a deployment, however, is challenging given the size of various biometric scans and the various non-standardized scanning technologies unable to match nonproprietary scans. Given our computing industry has difficulty standardizing database fields; it is difficult to imagine these biometric scanners ever being able to share templates. Or is it?

Biometrics, cont. By: Clovis Najm

The solution could be based on a hybrid technology of biometrics and cryptography. When biometrics are used to authenticate to a system, the interaction between human and system begins to replicate that of the physical world, with enhanced benefits. Personal biometric data could be loaded on a trusted third party server and cryptography could be used to securely match the templates. Cryptography would protect the biometric data in transit enabling two parties to become known from any two networked computers. Finger, facial and retinal scans could all be matched centrally, which would provide biometric confirmation between a person and a system for the purpose of information sharing, communications, and Internet transactions. The process would legally replicate the physical world providing irrefutable biometric proof of fingerprints, retinas, or even capillaries that are just as powerful as an eye witness or personal signature. Unlike many physical interactions or transactions between two people, biometrics can be confirmed by a trusted third party for every authentication attempt. This additional layer of security does not presently exist anywhere in the traditional world of security and authentication.

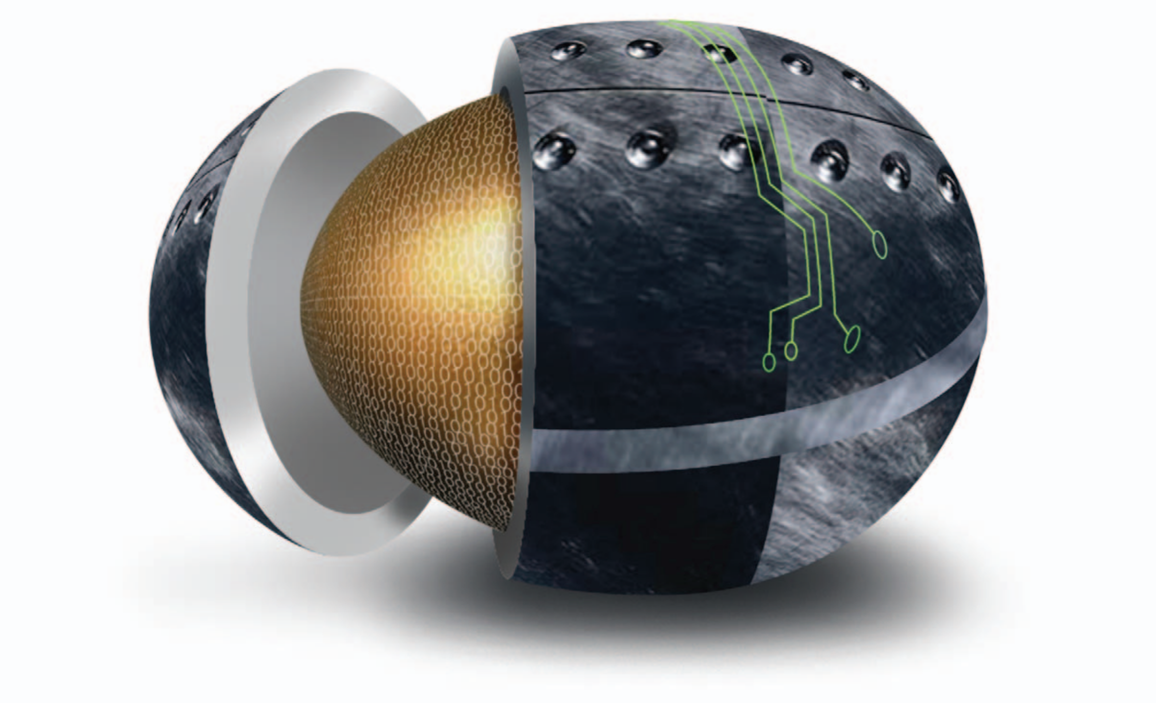
User concerns arise, however, when individuals are asked to believe a “trusted third party server” is protecting their biometric data properly and the data is being shared securely. Every time a person’s biometric data is scanned, individuals feel their biometric data is being taken from them, which evokes reluctance and limited user acceptance. From an organizational standpoint, businesses are accepting liability for becoming a biometric extension of its employees. This is a tall order for any organization. In addition, biometric scanners must be loaded on all network endpoints. An impossible feat at best.

In a world overrun with identity theft, fraud and security breaches, biometrics may be the silver bullet everyone has been waiting for.

But what if it was possible? What advantages would this provide to our world? We could stop worrying about losing our wallets or having our credit cards stolen. Getting a passport replaced in a foreign country would be possible through a vending machine connected to the Internet. If we met someone online, we could quickly trust they are who they say they are. Business relationships would develop at lighting speed as no reference checks would be required. Internet fraud would disappear. Identity theft would be a thing of the past. Access to secure areas and equipment would only be provided to properly authenticated individuals and not to imposters using someone else’s ID card, smart card or password. Biometrics and cryptography hold the key to expanding human interaction in the world of computing. Networks and computers could be utilized in ways we only previously dreamed of.

Clovis Najm is Vice President of Sales at Cryptolex, Inc.

www.cryptolex.com



Protect your assets.

Infosecurity delivers information, education, and networking for a higher level of security.

Protecting your business and its information assets requires confidentiality, availability, integrity and risk mitigation. As the security professional, you are constantly challenged to demonstrate your security plan's effectiveness as the threats and dangers to your enterprise become larger and more complex.

Knowledge sharing, community building.

Interact with many of the thought leaders in the security industry. Debate the issues and latest trends. Discover how to better manage the security strategy that's right for your organization.

All New conference content.

(ISC)^2 has partnered with Infosecurity to bring continuing professional education through the Security Leadership Conference Series, the gold standard in information security education. This year's seven-track program also includes sessions developed by Government Security News, LexisNexis Mealey Conferences, NYMISSA and the Larstan's Black Book on Corporate Security.

Proactively identify, assess and eliminate vulnerabilities.

In an industry that is constantly evolving, this is where you find the tools and technology to keep your information secure. More than 100 top suppliers come to Infosecurity to present the newest hardware, software and services that help you assess and manage risk.

Register today!

Infosecurity 2004 is the only event that brings together an independent, knowledge-based conference, a robust exhibition hall, and high-level networking opportunities all under one roof – in New York City. Come discover, learn and discuss ways to reduce risk and protect your organization's information assets.

For early-bird conference discounts and free exhibition admission, register online at www.infosecurityevent.com. Questions? Call (800) 417-8646, or (203) 840-5690. To Exhibit, please call (203) 840-5387.

infosecurity 2004

December 7-9, 2004 Jacob K. Javits Convention Center, NY.
www.infosecurityevent.com

Premier Education Partner:	Annual Conference:	Annual Chapter Conference:	Global Media Sponsor:	Premier Media Sponsors:	Official Media Sponsors:	Media Supporter:	Global Sponsor:	Gold Sponsor:	Silver Sponsors:	Produced and Managed by:
(ISC)^2®	ISSA Information Systems Security Association	ISSA New York Metro	SC Magazine	CSO The Resource for Security Executives INFOSTOR	GSN Information Storage + Security Journal	Security Horizon	symantec.	AVAYA	Ernst & Young Quality In Everything We Do Protocom Development Systems	Reed Exhibitions

Network Behavior Anomaly Detection

By: Brendan Hannigan

Stopping Zero-Day Attacks, Combating Evolving Security Threats and Addressing Internal Security

As the security industry moves from passive reaction to proactively stopping threats, new technologies provide both opportunity and confusion. Enterprises must deal with an increasing influx of new attacks that slip by perimeter defenses. Although security architectures are built in layers to provide a “defense in depth” approach, zero-day attacks and internal security breaches have become the most challenging threat.

There will always be new security threats. While layered security can mitigate risk from general nuisances, real protection depends on identifying and reacting to any new threat the instant it hits your network. This article will look at Network Behavior Anomaly Detection, a technology recognized by many security experts as the key to combating the plethora of threats that security managers face daily. We’ll evaluate the technology’s ability to provide enterprise-wide security that extends beyond the perimeter and stops subtle blended threats in their tracks.

What Is NBAD? Why Do I Need It?

Continued innovation has created many ways to protect against known threats. We evaluate every new attack that hits, spending valuable time analyzing and creating defenses that protect against major worms, viruses, commonly-known hacking vulnerabilities and other threats. Yet a malicious attacker can change only a few lines of code and the same worm, virus or Trojan will slip right by the reactive signature or patches developed to stop the original. Hackers creatively find new ways to breach traditional signature-based security defenses. Ongoing changes and upgrades in network infrastructures, Web services and new software continue to create vulnerabilities and opportunities for exploitation.

Simply detecting an attack isn’t enough. Network and security administrators really need a means to enforce network behavior so business can move forward. They need to identify potentially malicious activity and contain or resolve it before it can cause damage. NBAD profiles network behavior across the extended enterprise, flags anomalies, isolates the source of the issue or attack, and identifies corrective measures to resolve or mitigate the threat. The net gain comes from faster reaction to breaking threats and shortened time to resolution. That translates into increased uptime and efficiency combined with decreased operational costs and losses.

Network Behavior Anomaly Detection: Surveillance, Analysis & Control

Network Behavior Anomaly Detection (NBAD) technologies model traffic flows, transactions and network activity and analyzes them to learn what normal behavior looks like, including run-rate activity spikes. It detects aberrations—changes in traffic levels, communication patterns or other anomalies that serve as an early warning system for attack or internal misuse of the network. Pinpointing suspicious behavior, NBAD isolates the source of the anomaly and recommends resolution before damage can be caused.

Successful NBAD requires a three-tiered approach of surveillance, analysis and control. Surveillance recognizes malicious activity, catching even the most insidious low-and-slow probes of network defenses without sounding false alarms based on every traffic spike. While firewalls and other appliances provide a limited view at a single point in the network, NBAD surveillance looks across an entire network to ensure that threat analysis and detection is performed enterprise-wide.

Behavioral analysis is the key to understanding and applying what is learned from network surveillance. NBAD technology taps both real-time and historical views of network activity to model the behavior of users, applications, servers and network resources. The latest NBAD technologies include a classification engine that profiles network behavior to identify fluctuations in behavior. It raises an alarm when it perceives potential threats based on deviations from this baseline. NBAD does not rely upon a signature to identify a malicious internal user, or an evolving worm. It understands the dynamic complexities of modern networks, recognizing normal and acceptable behavioral changes as safe. Behavioral analysis identifies everything from the anomalous behavior caused by a new attack or hacking attempt, to internal threats such as insider scans and stealthy attacks. NBAD even recognizes policy violations among network users who use P2P file sharing and instant messaging, as well as any type of network misuse.

The third element, control, empowers security and network professionals to enforce network behavior. Simply identifying an anomaly is not enough; NBAD also identifies corrective measures. New attacks and security threats will continue to hit every network with increasing sophistication—and far greater danger. The control element prioritizes the severity of threats so administrators can address the most critical issues first. Armed with real-time surveillance and analysis, NBAD systems can either flag abnormal activity and give precise steps for hands-on remediation by network and security administrators, or provide automated resolution. It can address different types of activities in different ways, and is flexible enough to enforce network behavior based on unique customer use. After all, some parts of the network are more critical than others, and different types of threats require different approaches to resolution. Advances in NBAD technology put remediation options in the user's hands.

Where Does NBAD Fit In My Security Strategy?

In a crowded security market, every vendor hypes a different technology as the most critical element of a layered security defense. So where does Network Behavior Anomaly Detection fit in your security strategy and network architecture?

NBAD incorporates security event feeds and network traffic flows from your existing infrastructure to ensure that the enterprise infrastructure is fully leveraged. But the most direct value NBAD provides, and the primary reason people choose NBAD systems, is to address the critical flaws left by traditional signature-based technologies—addressing internal security concerns, and stopping subtle blended threats and zero-day attacks.

Network, cont. By: Brendan Hannigan

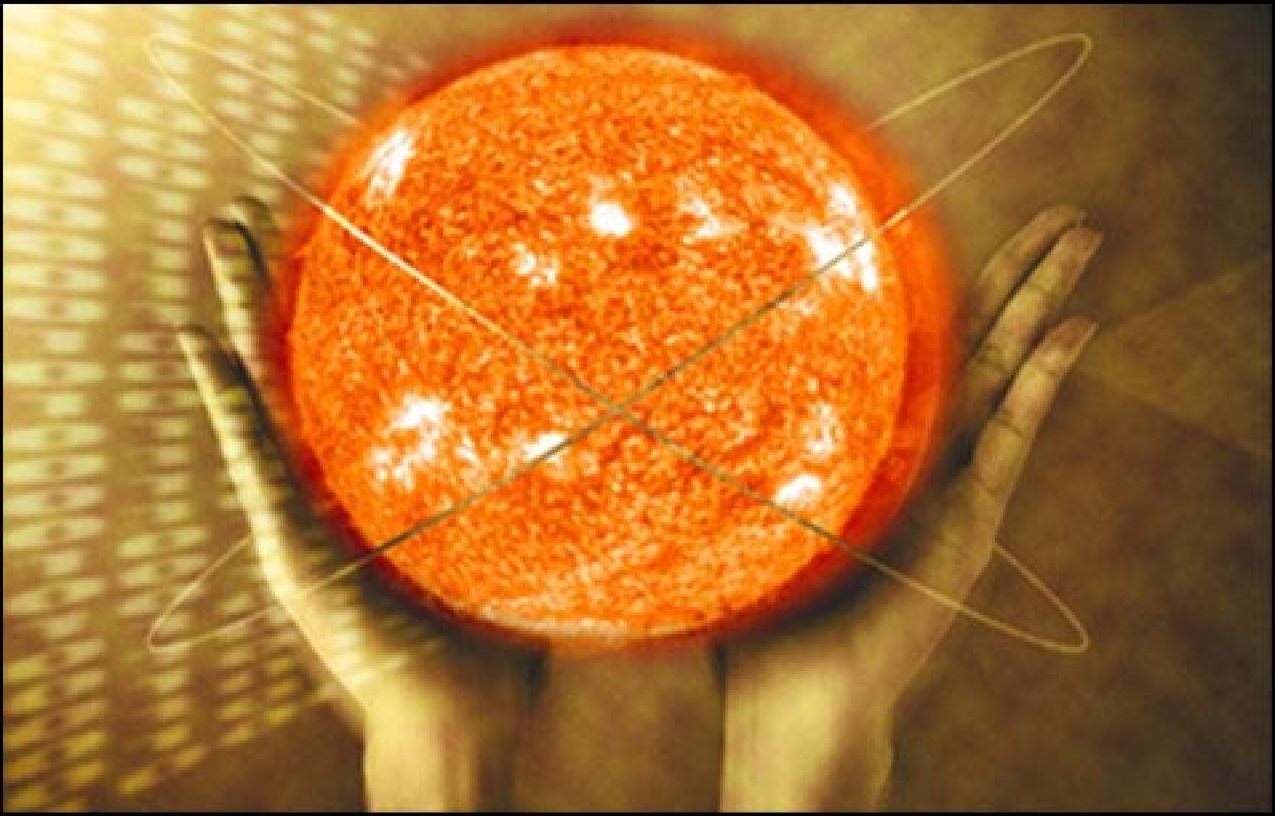
The bulk of ongoing security expenses, and the biggest nightmare for security and network managers, is identifying, reacting to, and cleaning up damage from the “next big attack.” No other technology matches NBAD’s ability to defend against new attacks that are as unpredictable as they are inevitable. NBAD serves as the first responder product for identification, understanding, control and remediation for any new attack.

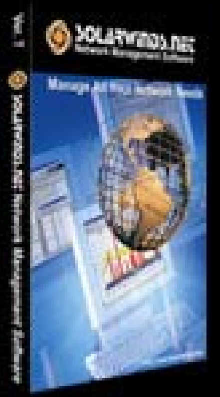
Brendan Hannigan is Executive Vice President of Marketing and Product Engineering at Q1 Labs Inc.

www.q1labs.com

Top 10 Benefits of Network Behavior Anomaly Detection

1. **Stops external threats**—NBAD provides the first (and often only) defense against the proliferation of zero-day, blended and internal threats, without the time delays or alarm overload of signature-based systems. This means identifying and locating worms, Trojans, denial of service, spam, viruses and blended/hybrid threats quickly and providing automated resolution.
2. **Enforces internal policies**—Exposes and locates internal threats so you can stop them quickly and eliminate future problems, whether from violation of internal policies or intentional misuse. Such misuse wastes resources and exposes enterprises to unnecessary legal and security risk.
3. **Ensures regulatory compliance**—Provides monitoring, detection, alerts and audit trails to comply with new regulations and compliance issues that demand IT participation.
4. **Avoids legal risks and liabilities**—Provides the processes and information to protect your organization against risks and liabilities such as lawsuits from illegal file sharing of copyrighted material, lawsuits from accidental disclosure of confidential information, and penalties for non-compliance with regulations.
5. **Improves operational efficiency**— Identifies problems quickly, isolating the source of network bandwidth issues or security threats to speed resolution without additional staff.
6. **Provides an enterprise-wide security system**—Holistic enterprise-wide view of security goes beyond segment-based, perimeter-focused point products.
7. **Secures the “perimeter-free” network**—Protects open, distributed networks from potential threats for the most advanced defense of infrastructures that can’t rely upon perimeter security solutions.
8. **Eliminates breaches from mis-configured systems**—Identifies network mis-configurations quickly and effectively, isolating the source to close vulnerabilities and conduits for hackers.
9. **Provides live window of network activity**—Gives network and security administrators an instant real-time view into network behavior, along with access to terabytes of data. It identifies issues in real-time and archives a complete audit log of activity without costly additional storage requirements.
10. **Combines network and security analysis**—Integrating asset discovery, vulnerability data and observed network profiling provides context-sensitive detection of known events. Pivoting between security and network data simplifies the process of finding, fixing and preventing threats.




SOLARWINDS.NET
Network Management Software

Windows XP Embedded Security, Pt 2 By: Travis L. Schack

This article is part two of an overview of important security issues concerning Windows XP embedded and the critical security functionality it offers for embedded devices.

File System Security

To encrypt data on your embedded disk, you must be using NTFS. NTFS also allows you to control access to directories and files. Some applications, especially legacy applications, only support FAT32. To protect data from local unauthorized access, the following XPe components must be added.

Feature	Required Components
Encryption File System (EFS)	User Interface Core NTFS Primitive: Crypt32 Local Security Authority Subsystem (LSASS)
NT File System (NTFS)	Primitive: Sfc
Windows File Protection	Primitive: Sfc Primitive: Sfcfiles Primitive: Sfcos
Driver Rollback	Add Hardware Control Panel Primitive: Setupapi
System Restore	System Restore Core
Volume Shadow Copy Service	Volume Shadow Copy Service File Sharing

Network Security

Will your embedded device be accessible from the Internet? Does it need to transmit sensitive data over a network securely? Will your embedded device rely on IIS or any other application that needs SSL support? XPe offers IPSec and SSL/TLS support. The following table shows the network security features and the components that must be added to support them.

Feature	Required Components
IPSec	IP Security Services
SSL/TLS	Local Security Authority Subsystem (LSASS) Cryptographic Network Services Primitive: Secur32 Primitive: Crypt32 Primitive: Cryptdll Primitive: Netapi21 Netlogon/Netjoin
Secure RPC	RPC Local Support Primitive: Secure32 Primitive: AuthZ Secure RPC over Kerberos Secure RPC over Negotiate Secure RPC over NTLM Secure RPC over SSL

Windows XP Embedded Security, Pt 2 By: Travis L. Schack

Wireless

Will your embedded device offer some type of wireless service or utilize wireless to function? The only wireless security feature that is supported in XPe is WEP. Today, it is hard to call WEP a security feature without smirking. A risk assessment must be performed to determine if WEP will be a suitable security feature for your wireless device. The author recommends that you consult the wireless security section of your company security policy.

Feature	Required Components
WEP	Primitive: Wzcsvc Wireless Zero Configuration

Internet Connection Security

Will your embedded device need protection from the Internet or from a public accessible network? Need a secure method to remotely manage your device? The following components can be used to assist in securing the network connection of your embedded device.

Feature	Required Components
Internet Connection Firewall	Internet Connection Sharing and Firewall
S/MIME	Mapi32 Libraries Cryptographic Network Services Primitive: Crypt32
WebDAV/WebFolders	Web Folders
HTTPS	Wininet Library Local Security Authority Subsystem (LSASS) Primitive: Secur32 Primitive: Crypt32 Primitive: Cryptdll Primitive: Netapi32 Netlogon/NetJoin
PPTP/L2TP	Dial-up Networking Common Libraries

Windows XP Embedded Security, Pt 2 By: Travis L. Schack

Security Management

Managing and monitoring the security configuration of your device will depend on the location of the device. Will you have to remotely maintain your device? Do you need command-line capabilities for automated scripting of configuration management? How will you perform regular audits on the security configuration? The following components will aid you in your security management tasks.

Feature	Required Components
Certificate Management	Certificate MMC Snap-In Tool
Security Configuration, Analysis	Windows Security Configuration Editor Engine Windows Security Configuration Editor Client Engine Security Accounts Manager Client Security Accounts Manager Server Security Settings Editor Security Configuration Engine Command-Line Utility
IP Security Management	IP Security Tools and User Interface
Group Policy Management	Group Policy Core Administration MMC Snap-In
Local Users and Groups Management	Users Control Panel
Credential Management	Credential Management User Interface Key Manager

Configuration Management

The overall goal of configuration management is to maintain control of systems or applications throughout their life cycle, ensuring that all additions, deletions, or changes occur in an identifiable and controlled environment, and that such changes do not adversely affect any desired properties or functions. It is recommended to utilize a configuration management database for you XPe image to track all components of your final image.

While this might sound like a daunting task, it is even more critical to track this information for XPe than it is for a full install of XP Pro. “Why is that?” you might be asking. One reason is when a critical security patch is released for XP. You know that it will be applicable to your XP Pro installation. What about your XPe image? It is a “componentized” version of XP Pro. How do you know if the components that are affected by the patch are included in your image? The most efficient way to know is by inquiring your configuration management database to check if the patch is applicable to your XPe image.

Implementation

By now, you should have identified business functionalities and security requirements for your embedded system. This phase includes building the XPe image, installing the completed image on the device, configuration, and testing. Application of a security-hardening checklist to both the OS and all applications are performed. To consistently and rapidly apply security settings to XPe, it is recommended to make use of security templates.

Security templates are text-based configuration files that contain system security policy settings, service settings, and file permissions. Templates can be deployed using several methods. Through the console, you can locally apply the template using the Security Configuration and Analysis Microsoft

Management Console (MMC). If your device is part of a domain, you can distribute the template using the Group Policy Editor. You can also use the secedit.exe tool with a customized script to apply the security template.

Guidance to configure your template should come from your security policy. If you do not have a security policy, you can find guidance from one of the following: NIST, Center for Internet Security (CIS), National Security Agency (NSA) and SANS.

Once you have installed and securely configured your XPe system, you should thoroughly test the system. All functions that were identified during the design phase should be thoroughly tested. Additionally, a security assessment should be performed against the system. The system should be tested externally and internally. External testing should be performed using at least two vulnerability scanners. The reason two scanners should be used is that one scanner could identify a vulnerability or weakness that the other scanner missed. Example scanners are Nessus, Newt, Retina, Saint, ISS Internet Scanner, and GFI LANguard Security Scanner. Microsoft offers the Microsoft Baseline Security Analyzer (MBSA) but it does not support XPe. Internal testing should be conducted by comparing a baseline security template with the current system settings using either the MMC or secedit.exe.

Defensive Layering

In 2003, ATM's running Windows XPe were shut down by malicious activity from the Welchia and Blaster worms. These attacks demonstrated the importance of defensive layering of critical systems, keeping systems up-to-date with patches, and the ability to respond to an attack. Host hardening has proven to not be the panacea of security.

Firewall Protection

As mentioned earlier, XPe is bundled with a stateful firewall called Internet Connection Firewall (ICF). In XPe Service Pack 1, ICF is disabled by default. Enabling of ICF can be done two ways: 1) During the initial startup, which offers protection during and after the boot process; 2) Manually after the boot process.

To setup option 1, you have to download the ICFUtil.exe tool, create a custom component with it, and build the component into your XPe image. Once this component has been added to your image, you can use several scripting and programming languages to configure ICF through the ICF API's. Microsoft published an article on this entire process on their website with the title *"Enable Internet Connection Firewall in Windows XP Embedded with Service Pack 1 Images".*

Host hardening has proven to not be the panacea of security...

ICF and <packet filter> were the only firewall options you had to protect your XPe system. On May 17, 2004, Sygate Technologies announced the release of the "first" security solution for XPe systems. Their Security Agent software provides intrusion detection and prevention, a personal firewall, host integrity, and the ability to manage the agent centrally.

Windows XP Embedded Security, Pt 2 By: Travis L. Schack

Anti-Virus Protection

At this time, XPe offers limited protection from viruses and malicious code by using the Enhanced Write Filter (EWF). EWF provides a means for protecting a volume from writes. This allows the system to boot from read-only media. There are two types of EWF: Disk Overlay and RAM Overlay. Disk overlay allows write data to be redirected to a separate partition on the hard disk and can be committed to the protected partition. RAM Overlay allows write data to be redirected to memory. The data is lost once the system is shut down or rebooted.

The impact of a virus that infects a XPe system with user credentials is minimal. After reboot, the virus would have been eliminated from the system. If the virus were to infect the system with admin or system privileges, it would be able to access the protected disk and cause damage. Anti-virus software would have to be used for this protection. At this time, there is not anti-virus software that supports XPe. Additionally, anti-virus vendors have not disclosed which XPe components are needed to run their software on a XPe system.

Operation/Maintenance

Ok, at this point, you have designed, built, secured and tested the XPe system. It is now time to deploy the system into production. How are you, or your customer, going to distribute patches and updates to the system? That depends on how many systems you have and how are they deployed. Is the device deployed in multiple locations? Is there network connectivity to all devices? Will the system be a standalone system? Can you centrally manage your XPe devices?

Patches

Patches are released weekly for newly discovered vulnerabilities and weaknesses in the XP OS. Companies are discovering that it is critical to keep systems up-to-date on patches to increase the survivability of their mission critical systems. Microsoft offers several methods to deploy patches.

The first method uses the Device Update Agent (DUA). DUA is a service that runs on the XPe system called Duagent.exe. This service is scheduled to retrieve updates and configuration tasks, via HTTP (or HTTPS), from a remote or local system. To deploy an update, you first download the QFE update and unpack it. You will find details of which file and registry settings are being updated in the Additional Information section of the QFE release notes. These file and registry settings are used to create a Device Update Program (DUP) script and converted to a program. This converted script is placed on your update server with the updated binaries from the unpacked QFE. When the DUA contacts the server, it recognizes that a new script is there and downloads the updated binaries with the update script. Once downloaded, it executes the commands in the command script to install the update. There is now a tool called

Windows XP Embedded Security, Pt 2 By: Travis L. Schack

DUAScriptGen that will assist you in importing the full list of file and registry changes from a XPe QFE and generate the DUA script file.

The second method offered by Microsoft is to create your own custom patch process through scripts. Depending on your application, this might be an option. For most companies, this will not be an option.

Recently, a third option was made available form Microsoft. SMS 2003 was released and it supports XPe devices. Using the SMS 2003 XPe agent, you have the ability to inventory and update your XPe systems.

SUS does not support updating XPe images. Windows Update (WU)is not supported on XPe either, even though the WU client is in the component database and can be built into your image. Because of the unique nature of XPe, SUS and WU do not support checking relational dependencies between features, files, or registry keys.

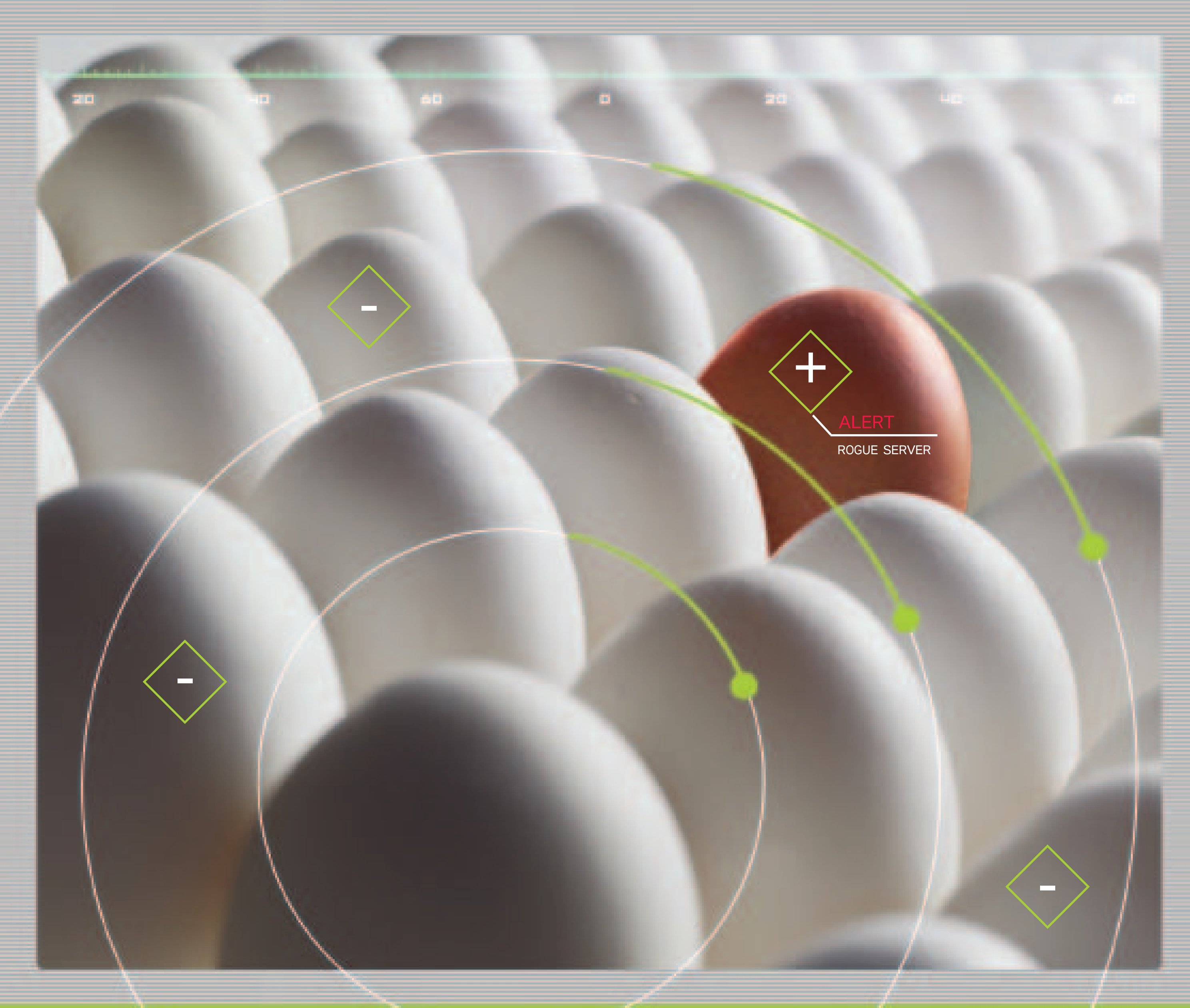
For systems that are standalone, unless they use dialup to receive updates, a service or field technician will have to update the system.

Summary

I realize that this article scratched the surface on designing, implementing and operating a secure XPe system. While the article did not cover application security, like IIS or SQL Server, you should have a good understanding of the types of security features that XPe offers and the components that are needed to support each feature. As more embedded devices are positioned in the industry and become critical components in business infrastructures, it is imperative that security becomes an integral part of the overall system design.

Travis L. Schack*,CISSP, CCNA, is the President of Vitalisec, Inc.*

Contact him at travis@vitalisec.com.



Only QRadar can pinpoint network anomalies in real time.

QRadar™ Security is focused on your network's perimeter. So who's monitoring internal activity that's threatening your network? QRadar maintains 24-hour vigilance to counter these threats. It learns normal behavior, flags irregular activities and their source, then identifies corrective measures. You'll find and fix problems immediately, no matter where they originated. To learn how to reduce downtime and losses while improving operational efficiency, go to www.q1labs.com.

www.q1labs.com | 781-250-5800

Q1 Labs
The nexus of security and networking

Don’t Believe Everything You Hear

By: Joe Grand

A Commentary on Adopting Security Technologies

Waiting for my flight from San Diego to Boston to board, I became curious to what sorts of devices people were using in day-to-day activities. I saw a man leaning against the wall using a Palm-based Kyocera mobile phone. I saw two BlackBerry devices sitting next to each other on a chair like brother and sister. I saw a laptop balancing precariously on the edge of a payphone’s narrow aluminum shelf, connected to the payphone’s data port. I saw airport personnel waving proximity cards in front of doors to gain access to restricted areas. I saw PCs running Windows at each gate, with locked screensavers flashing a message stating “This terminal is for authorized personnel only.”

What I quickly realized is that most users use technology without caring about how it was designed, the security, or even how it works. Why should they? They just want the product to function as they expect. But, for us, as security professionals, we live and breathe security. We design and implement technology and need to make sure it’s secure. This holds true for the consumer market just as it does for the enterprise, government, or military organization. We, as a population, have become so dependent on technology that we often forget the major risks associated with using it.

If you look around, most organizations, including those that are solely dedicated to computer security consulting and those that have dedicated computer security teams, are quick to adopt new technologies based on the recommendations of others or without verifying the claims of the vendor. “Trust us, we’re secure.” is what they’re told, and without blinking an eye, they believe it. Specifying and purchasing products based on your security needs is not a “one size fits all” decision. Nothing is 100% secure, and if someone says their product is, proceed with caution.

Before specifying or purchasing a technology for your network, always ask technical questions to the people that designed the product, not the people who sell the product (unless, of course, they are one in the same). Be cautious of dealing with companies who will not let you interface directly with their engineers. Ask them why they think the product is secure, ask how it was designed, ask how it was tested, ask how they can back up their claims, ask about their security policies and procedures. If they can’t explain any of that, become suspicious.

A further problem is related to the actual design of the products in the first place. Due to a general lack of understanding of secure design practices in the product development industry, many products are protected by “security through obscurity,” improperly implemented security, minimalist security mechanisms, or just sheer luck. Many vendors actually believe their own security claims. “The attacker will never be able to figure out how we encrypt the data,” they say. “Our scientists have created an unbreakable code”.

Don’t Believe Everything You Hear, cont. By: Joe Grand

Vendors and integrators alike need to understand how to design and implement products securely, how to gauge the threats against their products, and how to understand the mindset of an attacker. But, this sort of information can’t be taught in a day, and it most definitely can’t be learned in a day. A crash course in computer security will give you nothing but a false sense of safety.

In a recent engineering industry trade magazine, I saw an advertisement for a pair of DES-encrypted RF modules. The concept was simple: A 56-bit symmetric key was used to encrypt and decrypt the data traveling wirelessly through the air. The problem is that the DES key is stored in a notoriously insecure Serial EEPROM (Electrically Erasable Programmable Read Only Memory) within each module. So, once an attacker determined the location of the crypto keys in memory and retrieved the keys using a standard device programmer, they would be able to clone the module and sniff and decrypt all wireless communications between the two points. This is a perfect example of what can happen if the designers do not understand the potential attack risks.

We need to, by default, never trust a product straight out of the box. Challenge the claims. Scrutinize what you’re told. We must install and test products in a laboratory before implementing them in a real environment. We must get ourselves into the minds of attackers and try to break the product. As security professionals, we will undoubtedly discover problems with technology that most other people would never think of. We’ll look in places that other people don’t even know about. We’ll analyze physical hardware, circuitry, firmware, look for problems in source code, evaluate operational behavior, whatever it takes to make sure we understand the limitations of the technology and how we can best implement it for ourselves or our organization.

We are the security professionals. It’s not the end user’s responsibility to make sure that the products they use are secure. It’s ours. People, especially clients or your fellow employees, rely on us to make sure the products we recommend and implement meet some sort of security baseline. Don’t let them down.

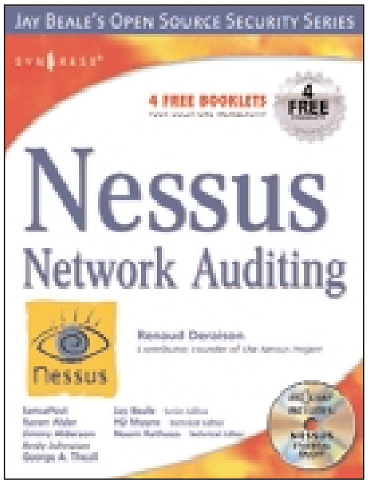
Joe Grand is the President of Grand Idea Studio, Inc., a San Diego-based product development and intellectual property licensing firm, where he specializes in embedded system design, computer security research, and inventing new concepts and technologies. He has testified before the United States Senate Governmental Affairs Committee and is a former member of the legendary hacker collective L0pht Heavy Industries. Joe holds a Bachelor of Science degree in Computer Engineering from Boston University. You may reach him at joe@grandideastudio.com.

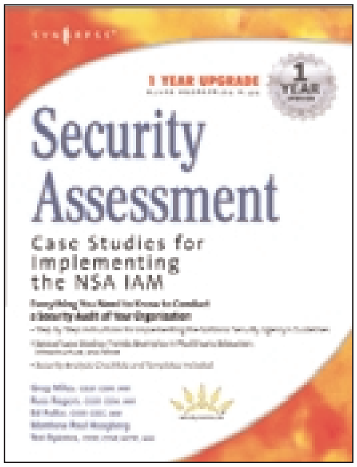
GRAND idea studio

SYNGRESS®

Available from Syngress Publishing Now! New Books by Security Horizon and Russ Rogers!

$49.95 US
$69.95 CAN
544 pp, 7 x 9.1875
ISBN: 1-931836-08-6





$69.95 US
$89.95 CAN
448 pp, 7 x 9.1875
ISBN: 1-932266-96-8

Nessus Network Auditing

Crackers constantly probe machines looking for both old and new vulnerabilities. In order to avoid becoming a casualty of a casual cracker, savvy sys admins audit their own machines before they're probed by hostile outsiders (or even hostile insiders). Nessus is the premier Open Source vulnerability assessment tool, and was recently voted the "most popular" open source security tool of any kind. This is the first book available on Nessus and it is written by the world's premier Nessus developers led by the creator of Nessus, Renaud Deraison.

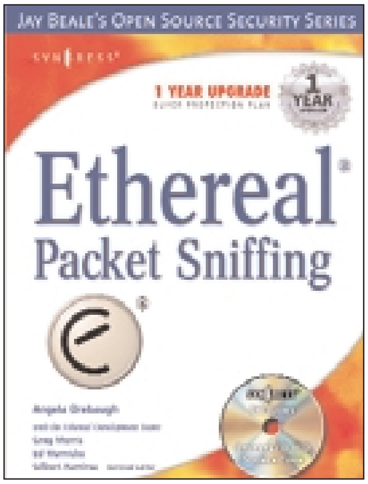
Security Assessment: Case Studies for Implementing the NSA IAM

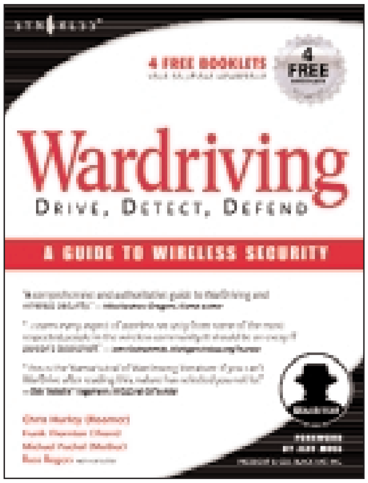
In 1998, the National Security Agency (NSA) Information Assurance Methodology (IAM) was developed to meet the demand for information security (INFOSEC) assessments–a demand that was increasing due to Presidential Decision Directive 63 (PDD-63) while at the same time NSA was downsizing. The NSA sought a way to maximize its resources to assist as many customers as possible and so they created a list of organizations that could perform the same service as the NSA. The NSA quickly realized that this system would not only provide valuable information to consumers–it would also provide a vehicle for standardization of INFOSEC assessments.

Also Available Now from Syngress Publishing:

Ethereal Packet Sniffing
$49.95 US
$69.95 CAN
608 pp, 7 x 9.1875
ISBN: 1-932266-82-8

From the Ethereal Development team, comes the first book ever on Ethereal.





WarDriving: Drive, Detect, Defend
$49.95 US
$69.95 CAN
512 pp, 7 x 9.1875
ISBN: 1-931836-03-5

"A comprehensive and authoritative guide to WarDriving and wireless security."
—Mike Kershaw (Dragorn), Kismet author

Syngress: *The Definition of a Serious Security Library™*

www.syngress.com

Defense in Depth

By: Ed Fuller

WOW, the second anniversary of the Security Journal.

By now as you've been reading these articles you know that there is a lot to accomplish in order to adequately protect your information. All of the topics that have been covered represent facets in a protection schema known as Defense in Depth.

Defense in Depth was first coined by the Department of Defense as part of a strategy to focus Information Assurance protection. Defense in Depth is not a silver bullet to protection, but is a "best practices" strategy that relies on the intelligent application of technologies and techniques to implement and maintain the protection. As with any good risk management approach Defense in Depth recommends that there is always a balance to be achieved. Protection must balance with the cost of the protection; operational considerations must balance with the operational performance. In order to make good decisions on what technologies and techniques to employ in Defense in Depth there are a few things that have to be considered.

Adversaries or Threats. Each organization needs to identify who or what is the threat, what is their reason for attacking (motivation) and possible ways they can attack. Adversaries can be anything from a script kiddy that wants to make a name for them selves in the underground up to and including nation states who want to weaken the country. In between these vastly different threats are things like corporate espionage and criminals who would attack to make a profit at your organization's expense. These are malicious adversaries that are commonly thought of but don't forget the non-malicious threats such as fire, water, power failures and the most prevalent threat, user error.

Once you have identified the threat you can look at what the current protection schema is providing you when you look at Confidentiality, Integrity, and Availability. Think of these as protection services that you are providing for your organization or customer. These services are always based on the concept Protect, Detect, Respond and Sustain. Organizations should expect attacks. You would not be in business if you did not have something important that needs protection. Organizations should employ tools and procedures that allow them to react and recover from attacks.

Protect is based on the hardening or securing of the system and components. In the commonly used Computer Network Defense this is proper implementation of System Configuration Management and Remediation Management. If you don't know what you have and how it is "supposed" to be used, how can you protect the system? If you don't have a defined approach to fixing problems that pop-up, how will you fix things? Unfortunately in many organizations this is an ADHOC process and is why Protect is difficult

Defense in Depth, cont.

By: Ed Fuller

to implement and maintain.

Detect is based on the ability to identify anomalous activity. Simply put this is the implementation of Audit. If you don't monitor what activities are occurring on the network, how will you know if something unusual is occurring? Yes this means that you will have to identify what is normal activity to be able to identify abnormal activity.

Respond is the ability to report and react to anomalous activity. This definitely builds off of the Detect. Once you have identified an abnormal activity you must determine if it is malicious or non-malicious. Then what do you do? How and who will the activity be reported to? Are there defined processes for reacting to the abnormal activity?

Sustain is the ability to maintain the proper level of security through a mature process. This is the normal day-to-day activity normally known as Network Management. Network management can be a nightmare for some organizations because they have not implemented Protect, Detect, or Respond. This creates an organization that is continuously in the fire-fighting mode. Dealing with issues over and over again based on what is going wrong today.

As we are all aware to implement these and create a sound Defense In Depth strategy you have to have three things or elements: People, Technology, and Operations. These must be balanced to provide the best coverage for the price and relying too much on one will result in exposure to attacks.

People are the beginning of Information Assurance starting with the senior management. The senior management must have a commitment to protecting the information based on a clear understanding of the threats. Senior management provides the policy and procedures needed for effective Information Assurance. Senior management must provide the resources needed to implement the policies and procedures with clear understanding of roles and responsibilities and personal accountability. Training must be included in this resource assignment for all critical personnel. Having the senior management commitment includes the establishment of both physical and personnel security. This will allow the organization to monitor and control access to facilities, information, and critical elements of the information technology environment.

Technology is available in a variety of components and services. Technology can be used to detect attacks, malicious activity, or even non-malicious activity. But what technology should be used? Every organization should utilize defined policy and processes for technology acquisition. These are normally based on the Information Assurance architecture and standards found in the Security Policy. There should be defined criteria for selection and procurement of products. These products should be implemented with defined and standardized configuration guidance. Prior to implementation there should be a process to assess the risk that could be introduced to the system by implementation of the technology. When you implement technology in the Defense in Depth strategy you should look at the Information Assurance principles that include the following:

- Defense in Multiple Places. Adversaries

Defense in Depth, cont.

By: Ed Fuller

can and will attack from multiple angles. Your organization or customer must employ protection mechanisms at different locations to be resistant to all classes of attack. Defensive locations are called “focus areas” and include; Networks and Infrastructure, Enclave Boundaries, and Computing Environment.

a. Defending the network and infrastructure provides protection of the LAN and WAN by ensuring confidentiality and integrity of the data transmitted.
b. Defending the Enclave Boundaries provides resistance to active network attacks.
c. Defending the Computing Environment provides access controls on hosts and servers to resist the insider or distributed attacks.

- Layered Defenses. There is no single product or service that is a cure all for the inherent weaknesses of the network. Given enough time and resources an adversary will find an exploitable vulnerability. The best method to mitigate this threat is through the use of multiple countermeasures that present different obstacles to the adversary. These countermeasures should include both protection and detection measures. This will increase the risk to the adversary of detection and reduce the adversary’s chance of success. A common example of this in large networks is perimeter firewalls in conjunction with Intrusion Detection and implementation of more granular firewalls and controls on the internal network.

- Specify the Security Robustness. This means understanding the value of what you are protecting and placing appropriate technical controls in the appropriate place. One example of this is the deployment of

strong perimeter defenses and implementation of security templates for the workstations and servers. This makes sense as it is usually operationally effective and suitable to deploy stronger mechanisms at the network boundary than at the user desktop.

- Robust Key Management. Infrastructures are lucrative targets. Deploying robust key management and public key infrastructures, such as PKI or PGP, that support all the Information Assurance technology that is deployed will ensure that you are resistant to attack.

- Event Correlation. Deployed infrastructures should be able to detect intrusions, analyze them and correlate the results to provide enough information to react accordingly. This will allow the "Operations" staff to answer the following questions: Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?

Operations focus on all the activities required in maintaining and sustaining the organization or customer's security posture on a daily basis. This will always include:

- Maintaining the security policy and ensuring that all personnel are aware and following the policy.

- Certifying and accrediting systems to ensure that good Risk Management decisions can be made.

- Managing the security posture by keeping patches and virus definitions and access control lists updated.

- Providing key management services.

- Performing security readiness reviews, commonly call assessments to ensure the controls are functioning correctly.

- Monitoring and reacting to threats or attacks as they occur.

- Recovery and resumption of operations from attacks or non-malicious events such as fire or flooding.

Defense in depth is simply a means of using multiple controls to implement a more complete security posture based on the perceived threats or adversaries. We know that we are not going to achieve a 100% security because that would leave us with 0% usability. For example, we could deny all inbound or outbound connections to the Internet, and in today's computing environment the network usability would suffer greatly. We want to avoid weak links through the balance of People, Technology, and Operations. Each of these are used to maintain the organization or customer's ability to Protect, Detect, Respond, and Sustain their Information Assurance.

Ed Fuller is Senior Vice-President and Chief Operating Officer for Security Horizon, also functioning as the lead instructor for NSA training and assessments. Comments or questions can be sent to ed@securityhorizon.com.

Book Review

By: Brian Martin

Security Warrior

Cyrus Peikari & Anton Chuvakin
Paperback - 581 pages (January, 2004)
$44.95 - O'Reilly ISBN: 0-596-00545-8

Security Warrior is one of the latest books that attempts to cover hacking and security information in a way that appeals to all levels of the field. Most books of this nature will present a wide variety of concepts and technologies that fall under the "security" blanket. These topics usually include an introduction to security, networking, reconnaissance, social engineering, attack and defense. As with most professions, attempting to disclose the ins and outs in a comprehensive manner would take volumes of information and could never be summed up in a single book.

Breaking away from the mold, Security Warrior stands out in a crowd of security books by delving into the world of software cracking through reverse engineering. While this is not a skillset many security personell use or know, it can be a very handy skill to have. Peikari and Chuvakin spend almost one third of the book on reverse engineering by providing detailed explanations, real world examples and even excercises to test your ability to break past software that restricts your access to a program on your own computer. While the skill of reverse engineering is useful, it is also fairly intensive and requires a solid programming knowledge. The extensive use of program source code in the book can get a bit overdone as most people reading the book will already understand it and find no use for it typed out in a book, or find themselves lost after the second line.

The next major section covers the basics of networking and reconnaissance as relates to security testing. After a brief outline of TCP/IP and other protocols that make this big Internet thingy work, they immediately dive into the art of Social Engineering before going back to network recon, OS fingerprinting and hiding your attacks. While this information is all valuable, the sudden turn to Social Engineering in the middle of technical network attacks is disjointed to say the least.

Once you have identified your targets via network recon, the next step is to figure out what specific platform attacks may work for you. Unfortunately, you need to read the chapter on Unix defense before Unix attacks in this book. While the order of the chapters is a minor nuisance, the author's consistancy is a tad annoying. After learning about Unix defense and attack, you then get treated to Windows Client Attacks and Windows Server Attacks. Apparently, the chapter on Windows defense got left on the cutting room floor. Even more odd is the next chapter on SOAP XML Web Services Security followed by the SQL Injection attack chapter. While these are all well written chapters that convey the information very cleanly, the order and choice of topics is very messy.

The last section covers Advanced Defense and goes into audit trails, intrusion detection, honeypots, incident response and forensics. Each chapter receives a good share of attention and falls back into an orderly fashion for dispensing the details of each technology. This material is a solid conclusion to a book that has a place in the security professional's library. For someone just entering the security circle, this book will be a rough start.

Brian Martin is a member of Attrition.org (http://www.attrition.org),a computer security Web site dedicated to the collection, dissemination and distribution of information about the industry for anyone interested in the subject.

What is FISMA?

By: Matthew Hoagberg

With hackers, cyber intruders, and terrorists, it has become increasingly important, now more than ever, to protect our nation's information technology and systems.

To improve our nation's information security posture, Congress approved the E-Government Act of 2002 (E-Gov) which included the Federal Information Security Management Act of 2002 (FISMA). FISMA is Title III of E-Gov that was signed into law (Public Law 107-347) on December 17th, 2002 by President George W. Bush. E-Gov addresses information technology among Federal agencies, standards in Information security, and addresses ways to protect the confidentiality of an individual's information that exists for statistical purposes.

FISMA replaced the Government Information Security Reform Act (GISRA) which was signed into law in November of 2000, as well as building upon the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996. FISMA is built off of GISRA making GISRA's provisions permanent, broader, and stronger, as well as including minimum requirements for information security. In addition to continuing provisions from GISRA, like the role of the Inspectors General (IG), FISMA has directed the National Institute of Standards and Technology (NIST) to continue to develop information security guidance for federal agencies. This guidance will set standards for systems operated by the federal government. FISMA sets the goals for information security and grants the authority of setting guidance for the minimum security settings to NIST. NIST has released Recommended Security Controls for Federal Information Systems. Special Publication 800-53 (SP 800-53) outlines guidance for federal agencies to be able to achieve FISMA compliance. The SP 800-53 will serve as a temporary guide for agencies' information security controls. As agencies gain knowledge and experience through the SP 800-53 they will be able to comment on the publication and provide feedback to NIST. From the agencies feedback, NIST will develop the new Federal Information Processing Standard (FIPS) 200. The FIPS 200 will expand on the FIPS 199 and mandate the minimum security controls for all federal information systems.

Purpose of FISMA

There are six key purposes of FISMA.

1. To provide a comprehensive framework for information security controls;
2. Provide effective management and

oversight of security risks;

3. Provide development and maintenance for controls to protect information systems;
4. Provide an instrument for improved oversight of Federal agency information security;
5. Acknowledge that commercially developed security products can offer advanced solutions; and
6. Give individual agencies the authority and freedom to select commercially developed products.

Purposes 1 through 4 are directly taken from GISRA while 5 and 6 were added to the purposes section acknowledging that commercially developed information security products can offer advanced and effective information security solutions. While acknowledging that individual agencies should select their own specific hardware and software information security solutions from among these commercially developed products.

Requirements of FISMA

Some of the basic requirements to Federal agencies in an effort to better secure federal information and systems are:

- Provide an inventory for all systems within an organization;
- Provide minimum information security for their systems;
- Have a basic security structure that can help provide information security;
- Conduct annual evaluation of security;
- Require the Office of Management and Budget (OMB) to operate a federal incident response center, whose functions include:
  i. technical assistance to federal agencies
  ii. collecting data
  iii. analyzing data;
- Authorize the OMB to oversee the development and implementation of requirements; and

Ensure that information security management processes were integrated with strategic and operational planning.

FISMA also requires government agencies to report on their IT security as compared to the minimum requirement on an annual basis as well as requiring all federal agencies to submit to the best practices for information security. Within the evaluation, the agency must list the possible risks to their information and systems, and work to reduce that risk. Agencies will use a Plan of Action and Milestones (POA&M), a report that identifies vulnerabilities and a plan to eliminate them. The POA&M will be reviewed monthly and turned in quarterly to the IG and agency officials will be held accountable for their security posture.

Obstacles and Challenges of FISMA

Obstacles and challenges that government agencies face are the lack of funding and the lack of staff which not only must continue with daily operation but now must implement new security. This includes maintaining the current risk management and policies. Another issue is a cultural change, which must take place in the way we look at and address IT security, for FISMA to work. As new policies and guidance are created, each organization must determine how they apply to them and how they are going to implement them. Government agencies will be expected to report on their information security posture once a year and will be graded A though F. As well as financial and personnel obstacles, FISMA brings with it new challenges. Agencies must gather, study, and understand their organization's security risks pertaining to their information systems and be able to demonstrate to the IG that they are complying with the new government regulation outlined in FISMA. Agencies must show that they are taking care of the vulnerabilities within the information systems and continually striving to improve their information security.

Conclusion

In conclusion, the Federal government has developed a law that mandates information security. FISMA was designed to keep the individual government agencies not only secure, but accountable for their information security. The agencies then have to be able to defend their security posture with greater reporting requirements. The reporting will show where government agencies are and how they plan to improve their security posture on a yearly basis. FISMA allows the agencies to evaluate all of its bureaus and compare each organization. The FISMA report is a checklist that details the compliance with policies and procedures.

The bottom line is to protect our government assets and to continue to improve the security of our government agencies. I have little doubt that this will bleed over into private businesses creating a country dedicated to security of our information technology.

Matthew Hoagberg is a Security Consultant with Security Horizon. You may contact him at Matt@securityhorizon.com