

"The only Password you should share."



The Legal Aspects of PKI

By Robert W. Daniels, Esq. • rdaniels@bbn.com

Introduction

The technology known as public key infrastructure, or PKI, and the digital signatures PKI introduces into business transactions, have become the solution du jour in many technology, business, and government circles. As is frequently the case, the technology of PKI and digital signatures is way out in front of the necessary legal and policy underpinnings. Some fundamental questions asked about PKI include: "are PKI-enabled transactions valid?" "Are there any applicable state or Federal laws governing PKI-enabled transactions?" "Who is liable if something goes wrong with a PKI-enabled transaction?" This article will introduce some of a PKI implementation's legal and policy issues.

"Maybe"

The first PKI related question asked by many non-lawyers is "are the transactions that use PKI and digital signatures legally binding?" This is the kind of question that lawyers love because it allows us to provide our favorite answer "maybe." There is general agreement among most lawyers in the field that the question of digital signature legality, even absent any specific law addressing the question, can be answered in the affirmative. Although not a single case addressing the question has made it to trial (yet), most attorneys practicing in the field would agree that existing laws addressing regular paper based transactions also are applicable to the world of PKI and digital signatures.

Numerous individual states have addressed the issues of PKI and digital signatures. However, those laws are applicable within the confines of the individual state only. Unfortunately, in some cases, there are substantial differences between laws in some states. This has left business executives (and their attorneys) scratching their heads trying to determine which law applies when a transaction involves parties subject to divergent digital signature laws.

Should the Feds get involved?

Considering the level of activity at the state level, many lawyers in the PKI field question the need for any Federal legislation. Opponents of Federal entry into the PKI arena contend that such legislation may have the unintended consequence of stifling technological innovation by seemingly favoring one technology over another. These opponents

also point out that the state attempts at legislation should be left alone as the states are a laboratory of sorts where differing approaches to legislation are tried and results can be compared. In response to such concerns, most legislators involved with PKI legislation attempt to draft bills that are technologically neutral. Currently there are no US Federal laws that address PKI or digital signatures directly. There have been numerous bills introduced into both houses of Congress, but thus far none has been enacted into law.

While Federal intervention may not be desirable, some sort of uniformity is necessary. There is a group that is currently developing model state laws related to PKI, electronic commerce, and digital signatures. The National Council of Commissioners on Uniform State Laws (www.nccusl.org) has addressed complex and sometimes controversial legal issues and has prepared model legislation to guide individual state legislatures. NCCUSL is perhaps best known for its role in the development of the Uniform Commercial Code. NCCUSL's first attempt at drafting law which would apply to digital signatures and PKI implementations is the Uniform Computer Information Transactions Act (http://www.law.upenn.edu/bll/ulc/ucita/ucita_99.htm), was adopted by NCCUSL on July 29, 1999.

Continued on page 4.

INSIDE THIS ISSUE

LEGAL ASPECTS OF PKI	1
PRESIDENT'S LETTER	2
ISSA AWARDS	4
WEB PARTNERSHIP	5
BOARD PROFILE	6
INDUSTRY CALENDAR	7
CHAPTERS	8
AUDITING YOUR FIREWALL SETUP	9
ISSA CHAPTER LISTING	11
NEW ISSA OFFICERS	12

PRESIDENT'S LETTER



Dear Fellow Members,

This month has been one of the busiest months I have seen in a long time.

Y2K turned out to be a great exercise in total preparedness and as predicted, the attention was quickly turned to the Information Security arena. On February 15th, I joined more than 20 other information security professionals and internet executives who were invited to the White House to talk about Information Security with the President. The focused attention from the White House was phenomenal. The attendees included Attorney General Janet Reno, National Security Advisor Sandy Berger, White House Chief of Staff John Podesta, National Security Council's Richard Clarke and Secretary of Commerce Bill Daley, and others. Much of the discussion centered on what role, if any, the government should play in infrastructure protection. ISSA is a co-signer of a document that outlines a set of basic principles to which all the attendees agreed.

Two days later I was invited back to DC as part of an advisory panel discussing various aspects of the President's proposal to establish an Institute for Information Infrastructure Protection. The primary focus is to look at R&D surrounding Information Security. It is very rewarding to see how the various aspects of government are forging partnerships with private sector security representatives on both the commercial and academic fronts.

On the subject of trust, the Federal Critical Infrastructure Assurance Office, led by John Tritak, has done a tremendous job in working with the private sector to build an alliance in the Partnership for Critical Infrastructure Security (PCIS). On February 22nd, we held the follow up meeting to our December 8th meeting during which Secretary Daley and representatives of more than 80 companies agreed to begin formalizing the partnership. GREAT STUFF!!

Now on to some specific ISSA internal issues. Samantha Thomas, our Director of Marketing, who has done a tremendous job had to give up her position on the board as her "real job" demanded more of her time. I want to thank her for her service to the organization and look forward to working with her through her regional chapter. It was no easy task to replace her, but Kurt Young of American Century has agreed to fill this all important position. I have asked two other distinguished professionals to serve as special advisors to the president in the areas of Computer Crime and advanced security technology research. Scott Charney, former Chief of Computer Crime and Intellectual Property for the Department of Justice, who is now with Price, Waterhouse-Coopers, has agreed to function in the advisory role around computer crime and how it affects the information security profession. Also Tom Talleur, former Director of Advanced Technology Programs for the NASA Inspector General, now with KPMG, has signed on to advise on advanced technologies.

Lots of great things happening and I hope I get a chance to meet many of you at the annual conference in Orlando.

Sincerely,

Howard A. Schmidt
ISSA President

ISSA[®] 1999-00

Officers & Directors

President

Howard A. Schmidt
Microsoft Corporation
howards@microsoft.com

Vice President

Bill Betts, CISSP, CPP
CompuSec
billbetts@home.com

Treasurer

Rebecca DeWeese
Columbia University
rd171@columbia.edu

Director of Operations

David Cullinane, CISSP, CPP, CBCP
Sun Life of Canada
David_Cullinane@Sunlife.com

Director of Membership/Chapter Relations

Edward Norris, CISSP
GTE Laboratories
enorris@gte.com

Director of Communications

Richard Mosher, CISSP, CBCP
Ernst & Young
Richard.Mosher@ey.com

Director of Marketing/Public Relations

Kurt Young, CISA
American Century Investments
kurt_young@americancentury.com

Chairman of the Board

Pat Gilmore, CISSP
Charles Schwab & Co.
Pat.Gilmore@Schwab.com

Executive Director

Mary Krukowski
mbrmktg@issa.org

The ISSA PASSWORD

Publisher

Information Systems Security Association
7044 South 13th St.
Oak Creek, WI 53154
Phone: (800) 370-ISSA or (414) 768-8000
Fax (414) 768-8001
www.issa.org

Board of Directors e-mail:
Issa@issa.org

Editor

Meta L. Levin
LevinM@GTE.net

Managing Editor

Richard Mosher, CISSP, CBCP
Richard.Mosher@ey.com

Graphic Designer

Matthew Jossart
graphics@naspa.net

Legal Aspects of PKI *continued from page 1*

International

There also are international variations in legislation and regulations affecting PKI, digital signatures, and electronic commerce. The United Nations Commission on International Trade Law (www.uncitral.org) is currently considering how to bridge inconsistencies between the laws of different countries so that PKI and electronic commerce may flourish. As was noted before, consistency is as important in the legal treatment of PKI as it is in the technical standards allowing PKI to work.

Liability

The final question, and the one closest to the lawyer's heart is "who is liable when something goes wrong in a PKI-enabled transaction?" This question provides lawyers with the opportunity to use another of our favorite answers... "that depends." The answer is crucial, since PKI and digital signature implementations can result in very large transactions processed with little or no human intervention. Unfortunately "that depends" is probably the only realistic answer at this point in time. Liability becomes clearer if a given PKI implementation has been properly thought-out in advance of installation, and key documents are in place, such as certificate policies, certification practice statements, and agreements covering the appropriate subscribers and end users. Using such publications as the Digital Signature Guidelines, a publication of the Information Security Committee of the American Bar Association, or the CARAT Guidelines, released by the Internet Council of the National Automated Clearing House Association (www.nacha.org), improves the odds that obligation and liability questions have been addressed. Accordingly, those planning to implement a PKI based transaction system must ensure that the necessary documentation is in place before the system is made operational. Otherwise, the results could be legally and financially disastrous.

Clear documentation

Clear documentation of how the PKI operates is an essential tool of any PKI implementation that functions externally to an organization or business. There are varying approaches to the preparation and use of documents such as certification practice statements (CPS). The author has prepared a number of these documents for use in PKI implementations where all of the parties to the PKI were legally bound by a contract or agreement. In these situations the CPS is a tool used to set forth how the PKI operates in clear non-legalistic and non-technical language. It is used as a public information document and is aimed at the users of the PKI, both subscribers and relying parties. However, the role of the CPS can vary, depending on the contractual relationships (or lack thereof) between the parties to the PKI; or if the PKI is used exclusively for internal business or organization purposes. Regardless of the particular implementation, it is wise to draft these documents using clear and straightforward language.

Anyone considering a PKI implementation is well advised to either get the organization's in-house legal staff up to speed on PKI and the applicable law or to hire an outside firm with a good working knowledge of PKI. There are a number of resources available to help lawyers not knowledgeable about PKI. Specifically, Digital Signature Guidelines is very helpful. That publication can be downloaded for free at the ABA website (www.abanet.org). Several law firms also maintain web sites that are a virtual gold mine of PKI related laws for all 50 states and many foreign countries as well. The firm of Baker & McKenzie has two excellent resources at www.bakernet.com/itc and www.bakernet.com/ecommerce. Similarly, the firm of Steptoe & Johnson also has an excellent site at www.steptoe.com


Privacy

Privacy is a concern of many people engaging in Internet based transactions which are enabled by PKI. Of course, one of the advan-

tages of a properly installed and maintained PKI system is strong privacy protection. Nonetheless, those planning a PKI implementation must be aware of state privacy laws and regulations. While there is a Federal Privacy Act, it is only binding on the Federal Government itself. Furthermore, those planning PKI implementations which cross international boundaries must also be aware of the privacy laws in the foreign countries. Some countries take a vastly different approach to personal privacy than that generally taken in the US. Several good resources for privacy related information are the Center for Democracy and Technology (<http://www.cdt.org>) and the Electronic Privacy Information center (<http://www.epic.org>).

Conclusion

This article has only touched the surface of a few of the many legal issues attendant to PKI implementations. There are numerous other issues that space limitations precluded from the discussion. Legal issues attendant to PKI implementations are not insurmountable. Many of the questions posed in this article are similar to questions that lawyers deal with every day in the paper-based transaction world. The intent of the article was to give those without a formal legal background a feeling for the types of questions that they should be asking if they are planning a PKI implementation.

There are a number of consulting organizations and law firms that are familiar with the legal issues attendant to PKI and digital signatures. So don't let the fear of legal complications stop implementation of a PKI based solution to business problems. Rather, bring legal counsel into the planning process early on so that those questions are considered and resolved before the project goes live. 

Robert W. Daniels, Esq., is a Senior Consultant with the PKI consulting group of GTE Professional Services and a former Deputy Chair of the Federal PKI Steering Committee. He is a member of the American and Michigan Bar Associations and a graduate of the Thomas M. Cooley Law School. He was a contributor to the Digital Signature Guidelines and CARAT Guidelines discussed in the article.

This article was written in the author's personal capacity and does not necessarily reflect the views of his employer or of the professional organizations of which he is a member. The author wishes to thank John Tomaszewski, Esq. for his editorial assistance.

ISSA Awards

ISSA named Nena Young, an Information Security Policy Analyst with the Texas Department of Information Resources, its Information Security Professional of the Year during ceremonies at the Joint Computer Security Conference in Orlando, FL. A dozen other professionals also were honored for various contributions during the ceremonies.

Young, a Certified Recovery Planner and a Certified Business Continuity Planner, is the ISSA Capital of Texas Chapter treasurer, and was honored for her contributions to her profession and ISSA. She also is treasurer of the ACP Capital of Texas chapter and often brings the two together for joint programs, especially the Contingency Planning and Information Security (ConSec) conference in Austin, TX, for which she served as the chair in 1999. Under her leadership the 1999 conference was the most successful to date.

Continued on page 8

Special Announcement - ISSA Web Partnership

The ISSA International Board is pleased to announce a special benefit for our members in partnership with E-Certify. E-Certify will provide free to all ISSA members a digital ID certificate that can be used for secure e-mail and to simplify the ISSA web site sign-on process. These certificates eliminate the need for members to continually sign back on to the ISSA web site, <http://www.issa.org/>. All current and future members of ISSA are eligible to receive a free certificate.

The digital certificate can be obtained by first signing on to the 'Members Only' section of the ISSA web site. Then follow the steps below: Follow the links to the certificate generator.

Enter your member ID number.

The member number will be validated against the organization records, and you will then receive an e-mail with a PIN number.

Use the PIN number with your member ID number to sign back on to the certificate generator and request a certificate.

You will receive the certificate and can install it for later use.

Once you have installed your certificate, the web site sign-on process no longer will require you to login on daily. Instead, the certificate will be used to validate your access. This certificate will be good through the end of 2000, and will have to be renewed at the first of next year. E-Certify will provide the same functionality for use of Chapters on their own Web sites.

We thank E-Certify for its contribution, and look forward to a rewarding partnership with them. E-Certify is a trusted Internet solutions provider that offers security consulting for networks and applications, secure applications development and managed services.. The Company focuses on a standards-based product and services model, offering corporations the latest security technologies, including authentication, authorization, certificate infrastructures, PKI, firewalls, VPNs, and monitoring. E-Certify has regional offices and hosting facilities throughout the US and Canada. More information is available on the Web at www.e-certify.com.

Find your vulnerable modems ---
before the enemy does!

PhoneSweep™ Telephone Scanner

- * Dials up to 1000 numbers/hour
- * Controls 1-8 modems
- * Brute force attacks
- * In use World Wide
- * Runs on Windows 95/98/NT
- * Integrated SQL (ODBC)
- * Detailed reports

Identifies
200+ remote access
systems, including
pcANYWHERE,
CarbonCopy, ReachOut
Windows NT RAS
Citrix WinFrame, Cisco,
UNIX (28 versions)
Bay Networks, Annex
Audix, BLAST
VAX/VMS
...and 166 more

**Sandstorm
Enterprises, Inc.**
www.sandstorm.net
+1 617-426-5056

PO Box 381548, Cambridge, MA 02138

Instructions for access to the new ISSA web site

To sign on to ISSA's international web site (<http://www.issa.org>) to obtain a certificate or in place of using a certificate, you will need your User-ID, Member-ID and a password. This information is on your ISSA renewal notice.

Your member ID (MID) number. Please note that your MID is also being printed on your Password label to help you remember it. Look for the "MID nnnn" above your name on the label.

Your site user-ID (UID). This is an assigned ID which can, in the future, also serve as an Internet e-mail ID through the TEL server if you need one.

Your initial password to the site will be the same as your user-ID. When you sign on for the first time, you will be asked to change your password. Please do so to protect your access.

Re-Validation

Your access to the web site will be validated for the current session when you first sign-on to the protected area. Permission to access the site will be stored in a cookie on your computer, so that you will not have to re-enter the validation information when you return to the site later. The cookie will not store your actual access information, and it will expire at midnight the same day. You will then have to re-validate your access the next time you enter the site.

Alternatively, you can obtain an X.509 certificates as described above and use it to access the site. Once you have your certificate, you can click on the "Certificate" authentication button rather than entering the UID, MID and password. Until you get your certificate, keep your member ID and your site user-ID handy, and come visit us to see what is available"

BOARD PROFILE

Bill Betts Vice President

For Bill Betts, fun means learning new things. That is how he ended up in InfoSec. About five years ago he was living in Cupertino, CA and trying to figure out what he wanted to do with his life. A college catalog provided the direction. There was a class in computer science that sounded interesting, so Betts took it.

"For so many years I did the same thing over and over again," he said. "Moving to California was kind of a catalyst to do something new."



"Our challenge is to make sure the core services are the best that they can be."

A veteran of 15 years in criminal justice and security, it was no surprise that he immediately was attracted to InfoSec. Before heading for California, Betts had done private security work, managing security forces for A&P Foods in Edison, LI and in Pennsylvania, and for Rickle Home Centers. Originally from New Jersey, he had spent most of his life on the East Coast. After a friend asked him to do some consulting work on a rape case, he went into business for himself. All was well for a while, but about the time he was getting tired of the security business and looking for something new, his father, who had moved to California in 1983, needed some help. Betts and his wife headed for the West Coast. While there, his wife applied for and got a teaching job in San Jose. So, they decided to stay.

One computer course built on another. He found that it was interesting to marry the two professional pieces of his life: computers and criminal justice. As he realized how fast the industry was moving, he decided to focus on computer forensics.

"It goes with my investigative background," he said. "I like to investigate and pull together all the information, then talk to the suspect. I like looking at how people react to my questions. It's verbal judo."

Betts also likes the varied work and the fact that the field constantly is changing.

Betts' introduction to ISSA was part of that drive to learn new things. He was taking an "Introduction to Computer Security" class and asked his instructor what professional associations he could contact to learn more about the field. The instructor recommended ISSA and Betts began attending San Francisco Chapter meetings. At first the lingo was foreign, but Betts stuck with it and learned a lot.

That push to learn more and more extended to his CISSP certification. He started getting together with others who were working toward the rating, but did much of the work on his own by going to the library and studying two hours a day.

"Then I prayed," he said. "I stood up and raised my hands and said, 'God, please, this one time.' It took about six hours for the test and I was done a half hour early."

Needless to say, he passed.

In the meantime he was becoming more active in the San Francisco ISSA chapter. The chapter president decided not to run for re-election, and Betts suddenly found himself vying for the job. He won and surrounded himself with a group of dynamic chapter members who helped reshape the format, including an ongoing mid-year seminar that has grown steadily.

Before he knew it then ISSA president Pat Gilmore, a member of the San Francisco Chapter, was encouraging him to run for the open ISSA Vice President slot.

"She kind of pushed the issue," he said. "One of the reasons I decided to run was that she said she would support me."

He did. She did. Betts is now vice president.

Betts' major goal is to make certain ISSA is providing basic services to members, as well as good support for local chapters. It's those core services that Betts sees as ISSA's bridge to the future.

"We had some financial problems in the past and Pat's board found a way out for us," he said. "Now we are lucky to be in a position where we are able to move forward. Our challenge is to make sure the core services are the best that they can be."

In his spare time, Betts coaches his 14 year old daughter's soccer team, and is an active member of the Alameda County Search and Rescue Team. His 18 year old son shares his interest in backpacking and camping, and father and son go out together as much as possible. The two also recently took the engine out of his son's car and rebuilt it, a project his son would like to tackle again.

"It was kind of fun working together," he said. "I could turn them down and say I am busy, but it is an opportunity to do something they'll remember. Plus I need to do something completely different than computer security sometimes."

In the end it is back to computer security, though.

ISSA Membership Update Form

Name _____

Member # _____ Chapter _____

Address _____

City, State, ZIP _____

Country _____

Email _____

Phone _____

FAX _____

Please send to:

ISSA Headquarters

7044 South 13 St.
Oak Creek WI 53154

FAX to (414) 768-8001 or
www.issa.org/members

and follow the Member Update link



INDUSTRY CALENDAR

Computer Security Institute

April 3-4, 2000

**Introduction to Computer and Network Security
Facilitated Risk Analysis for Business and Security
Intrusion Techniques and Countermeasure**

April 5-6, 2000

**Securing E-Business: A Technical Guide to Implementing PKI
How to Develop Information Security Policies and Procedures
Secure Migration to Windows 2000**

Location: New Orleans, LA

April 25-26, 2000

Essential Skills for the Computer Incident Response Team

April 27-28, 2000

Forensic Investigation: Tools and Techniques

Location: Cincinnati, OH

April 25-26, 2000

Introduction to Computer and Network Security

April 27-28, 2000

How to Create and Sustain a Quality Security Awareness Program

Location: Gaithersburg, MD

June 10-12, 2000

**Introduction to Computer and Network Security
How to Conduct a Network Vulnerability Assessment
Essential Skills for the Computer Incident Response Team
Windows NT Security: Assess, Penetrate and Secure
Securing E-Business: A Technical Guide to Implementing PKI**

June 12-14, 2000

NetSec 2000 - Technical Dimensions in Network Security

June 15-16, 2000

How to Create and Sustain a Quality Security Awareness Program

How to Develop Information Security Policies and Procedures

Comprehensive Intrusion Management

Intrusion Techniques and Countermeasures

Secure Migration to Windows 2000

Advanced Network Security

How to Develop a Winning Security Architecture

Location: San Francisco, CA

Information: www.gocsicom; csi@mfi.com; (415) 905-2626; Fax (415) 905-2218

MIS

April 3-5, 2000

InfoSec World 2000

Location: Orlando, FL

Optional Workshops: April 1, 2, 6, 7

Information: mis@misti.com; (508) 879-7999; fax (508) 872-1153; www.misti.com

SANS Institute

March 21-27, 2000

SANS 2000

Location: Orlando, FL

Information: info@sans.org or (719) 599-4303

Information Security Forum

ISSA, Information Security Institute, InfoWorld

April 3-5, 2000

InfoSec World 2000 Conference and Expo

Location: Orlando, FL

Optional workshops - April 1, 2, & 6, 7, 2000

Information: www.misti.com; mis@misti.com; (508) 879-7999;

Fax (508) 872-1153

Vanguard

May 14-19

14th Annual Vanguard Security Expo 2000

Location: Atlanta, GA

Information: (888) 547-EXPO; Fax (714) 939-0273;

www.vipexpo.com;

180 S. Anita Dr., Orange, CA 92868

New York Metro Chapter

May 23 - 24, 2000

Computer Security for the 21st Century

Location: New York, NY

Information: George Dolicker, gjpd@lucent.com or

(914) 232-2373



Special Thanks to our ISSA sponsors:

Gold Sponsors:

ISS

Tumbleweed Communications Corp.

Silver Sponsors:

ICSA.NET

Vanguard Integrity Professionals





CHAPTERS

New York Metro Chapter

Not too many years ago the New York Metro Chapter was struggling, just a shadow of its current self. Now it is a thriving organization, with well attended meetings, vendor sponsors, a web site, a newsletter, and is the sponsor of several well regarded conferences each year.

"It has grown a lot in the last three to five years," said former board member Aileen MacGahan.

Former chapter president Rebecca DeWeese, now ISSA treasurer, noted that when she took office in 1994, there were about 95 members. The number now stands at around 200. It began growing in 1992 with the institution of an annual one day conference, the brainchild of member and former president, George D. Hertzberg. He recruited DeWeese to work on the conference, the path toward more chapter involvement for many members.

"The chapter wasn't very large at the time and there wasn't a lot of enthusiasm," DeWeese remembered. "Then membership took off."

After the third year, the conference expanded to one full day, plus a half day of tutorials. Last year it ran as a full two day event. It has attracted new chapter members not only because of its quality, but because of its pricing structure. It costs less to join the chapter and attend than it would if a non-member just attended the conference. Some of the members who joined this way have become active in the chapter. This year's conference is headed by Noel Zakin and is set for May 2000.

Many credit current president Jim Duffy, who took office three years ago, with ideas that sparked the chapter's most recent growth. MacGahan and others note he had "a lot of good ideas" and pushed to have many of them implemented. There are other factors in the growth, too. There are many InfoSec professionals in the New York City metropolitan area, and as the profession has grown, so have the numbers, as well as the need for professional associations where people can exchange information and get an education.

A schedule of regular meetings is posted for the year, both through the chapter newsletter and on its web site (www.nymissa.org). Meetings usually begin about 2 p.m. and end by 4 p.m., and the location is near a train station, something important in New York City. A typical meeting usually involves one or more speakers or a panel discussion, as well as time for networking. Continuing education credits are available.

Vendor sponsorship at the chapter level is one of the ideas for which Duffy can take the credit, both DeWeese and MacGahan said.

"It improved the financial condition of the chapter," MacGahan said. "The corporate sponsors also knock themselves out to find ways to get involved."

One of the benefits is a regular meeting place. In addition, sponsors often help with speakers and other meeting necessities, even light refreshments. Sponsor names are listed on the web site, as well as in the newsletter and on the chapter's letterhead.

The chapter also organizes and runs two special one day professional development sessions, which are free to current members. The most recent was held in mid-January and included technical presentations, as well as a vendor exhibits.

The chapter is run by a 15 member board of directors. There also is a six member executive advisory board charged with advising the governing board about educational programs, membership growth, scholarship and the Fitzgerald Award, which is presented by the chapter annually.

Presided over by Ron Petrucci, who also is in charge of the newsletter, the web site has been up for a little more than a year. It provides

news about the chapter, a meeting schedule, board members and contact information, links to ISSA, chapter sponsors, other InfoSec related links, as well as the International Information Systems Security Certification Consortium, Inc. (ISC²).

The chapter has come a long way in the last five years and members expect it to continue to grow.

UPCOMING CHAPTER MEETINGS

Password now prints news of upcoming chapter meetings. Deadlines are: May-June issue, April 14 (mail date May 26); July-August issue, June 9 (mail date July 28); September-October issue, August 11 (mail date September 22); and November-December issue, October 13 (mail date November 24). Please e-mail information, including meeting date, location, topic, and contact for more information to Meta Levin, Password Editor, levinm@gte.net.

New York Metro Chapter Wednesday, April 12, 2000

Location: Penn Club

Topic: E-mail (external): Privacy/ Confidentiality, Virus Protection, Content Filtering

Speakers: To be announced

Wednesday, June 21, 2000

Location: To be announced

Topic: Internet Update; picnic

Information: www.nymissa.org

Phoenix Chapter Tuesday, April 4, 2000

Location: A.G. Communications Systems

Topic: To be announced

Information: Cindy Donaldson (480) 813-9119

ISSA Awards *Continued from page 4*

Five InfoSec professionals were inducted into the ISSA Hall of Fame in recognition for their contributions to the advancement of the information security profession. They are: Donn Parker, CISSP; Harold F. Tipton, CISSP; William H. Murray, CISSP; Scott Charney, and Sandra Lambert, CISSP, CDP, and CISA. Another seven were honored as members of the ISSA Honor Roll for meritorious conduct and contribution to the advancement of the association. They include Donald L. Evans, FLMI; Gerald L. Kovacich, CISSP, CFE, ISO, CPP; Harold F. Tipton, CISSP; William H. Murray, CISSP; Richard W. Owen, Jr., CISSP, and James Duffy, CISSP.

Ernst and Young was named the Outstanding Organization of the Year, and the Capitol of Texas chapter, Ronald E. Helsley, president, was honored as the Chapter of the Year. The New York Metro chapter garnered the Web Site of the Year award. Wilfred Camillieri is the Webmaster.

Eight new chapters received their gavels: Alamo, The Carolinas, Connecticut, Phoenix, Detroit, Puget Sound, Silicon Valley, and South Florida.

AUDITING YOUR FIREWALL SETUP

By Lance Spitzner • lspitz@ksni.net

You've just finished implementing your new, shiny firewall. Or perhaps you've just inherited several new firewalls with the company merger. Either way, you want to know if they were properly implemented. Will your firewalls keep the barbarians out there at bay? Does it meet your expectations? This paper is designed to be a guide on how to audit your firewall and your firewall rulebase. Examples provided here are based on Check Point FireWall-1, but should apply to most firewalls.

Where to Start

I will address two situations:

You have certain expectations of what your firewall can or cannot do and you want to validate those expectations; or

You do not know what to expect, so you need to audit your firewall to learn more.

I will not cover how to audit or "hack" a network nor which firewall is better than others. Each firewall has its own advantages and disadvantages. What is going to make or break you is not choosing the best firewall, but implementing it correctly. Even the most experienced users can make mistakes, especially when rulebases grow into hundreds of rules.

Setting Expectations

First we have to define what we expect. What do we want our firewall to do? Most of you should already have this defined in the form of a security policy. Make sure you understand these expectations before you verify your firewall setup. That way, when you are done with the process, you can compare the results to your expectations. Some of you may not know what to expect. Maybe you are new to the company and need to assess the situation. Or perhaps your company has just merged and you have assumed responsibility of several new networks. Regardless, try to define some goals before you start.

The Methodology

There are two parts to auditing your firewall setup. First, you want to test the firewall itself. As a critical system in your security plan, you want to ensure this is secure. Second, you want to test the rulebase. What traffic can pass through the firewall? The whole purpose of the firewall is traffic control.

The Firewall.

You want to ensure that your firewall is secure; that no one from the outside or the inside can access or modify your firewall. First, you want to ensure it is physically secured with controlled access. Once someone has physical access, the game is over. Next, the operating system itself

should be fully armored. I recommend you review an armoring checklist specifically designed for your operating system, then ensure the operating system fully complies with it. You can find more information about armoring and checklists here for linux (<http://www.enteract.com/~lspitz/linux.html>), solaris (<http://www.enteract.com/~lspitz/armoring.html>), or NT (<http://www.enteract.com/~lspitz/nt.html>). The next step is to port scan your firewall, from both your internal network and the Internet, scanning for icmp, udp and tcp. We want to identify, what, if any ports are open on your firewall. On most properly configured firewalls, you should find no open ports, you should not even be able to ping it.

A properly armored firewall should have few services to start with. Once the firewall is running, no ports should be exposed unless absolutely necessary. Many of you CheckPoint FireWall-1 users will get a nasty surprise when you find several ports open, such as 256, 257, and 258. These ports are for administration, open by default in the control properties (<http://www.enteract.com/~lspitz/validate2.jpg>). I highly recommend that you disable them. ICMP also is open by default. I recommend you disable this, too. If ICMP is open, your network can easily be mapped from the Internet. If you need these ports or services to administer your firewall, then set up a rule that limits what source IPs can connect to them. To secure your firewall deny access whenever possible. Every rulebase should have a lockdown rule at the beginning that denies any traffic to the firewall. That way your firewall is "sealed" from the world. If you need access to the firewall, have the rule go before the lockdown rule (<http://www.enteract.com/~lspitz/lockdown.html>). All other rules should go after the lockdown rule. Many people consider this a "ghosting" rule, thinking it hides the firewall. It doesn't. It protects your firewall, ensuring that whatever other rules you put in later, your firewall will still be protected. For example, in the demo rulebase (<http://www.enteract.com/~lspitz/lockdown.html>), if you put rule #3 first, now everyone on your internal network has full access to your firewall. The lockdown rule, when placed first, protects you against that. The whole purpose of scanning your firewall is to ensure that you have not accidentally exposed your firewall to unauthorized users. To learn more about rulebase design, check out Building Your Firewall Rulebase (<http://www.enteract.com/~lspitz/rules.html>).

The Rulebase

Once you have audited your firewall, audit your rulebase. The goal is to ensure that the firewall is enforcing what you expect it to. This is done by scanning every network segment from every other network segment. You want to validate that the firewall is accepting only the traffic that you allow. Many firewalls have several network segments, such as

Continued on page 10

AUDITING YOUR FIREWALL SETUP *Continued from page 9*

protected DMZs. Make sure you validate your rulebase by scanning from every one of these segments. I recommend you place a system on your DMZ and attempt to penetrate your internal network, as your DMZ is highly vulnerable. This simulates a compromise of one of your DMZ systems (such as a DNS or webserver), and affirms that your internal network is still protected by the firewall. Remember, your firewall rulebase should deny everything, except what is specifically allowed. The fewer services you accept and the fewer rules you have, the more secure your environment. If during your audit you are not sure if a service should be blocked, block it. If no one complains, then it was not needed.

Authentication / Encryption:

Also test authentication and encryption. Often firewalls are expected to authenticate users to access a resource. FW-1 has several different authentication options, be sure to test them. For example, if you expect users to be authenticated before they access your website, confirm this for yourself. Try accessing the website without authenticating and see what happens. It is easy to make a mistake when you implement a rulebase. What you thought was password protected may be wide open to the world. Apply the same test for encryption. If you have resources that should only be accessed while encrypted, test them out by attempting to access them without encryption. Also, run a sniffer such as snoop (<http://www.enteract.com/~lspitz/snoop.html>) or tcpdump during the test. Make sure your data is actually being encrypted.

Additional Services:

Firewalls today can work with third party software for additional services. For example, virus scanning in email or web content filtering. If you are using any of these third party services with your firewall, you should test them. For example, for virus scanning, send an infected email through the firewall to ensure your virus scanning is working. If it does not, you will need to review your configuration and resolve the problem. Be sure to re-test the configuration to ensure the fix works.

Digging Deeper:

Once you have identified available resources, you can begin to dig deeper. You've determined what the firewall allows through, now what threat does that pose? This is where things become fuzzy, where auditing your firewall setup can become auditing your network. You are no longer auditing your firewall, but auditing the resources behind the firewall. This information will be important to you. The goal is to determine what potential vulnerabilities exist for the accessible resources. I recommend reviewing each accessible resource to identify what vulnerabilities exist. For example, you determine that the firewall allows http access, in your case to several IIS web servers. Now you have to determine what threats that poses. Or, you identify a system running ftpd, in your case wu-ftpd 2.4.2 VR17 (in this case, upgrade to the latest version). If a vulnerability exists, you either have to fix the vulnerability, or

decide if the risk is worth the service. One of the best resources for identifying vulnerabilities (both Unix and NT) is Bugtraq's vulnerability database at securityfocus.com. I highly recommend you review this database for every resource you have accessible. There are also a variety of tools that will help you identify what vulnerabilities exist. Find several tools you feel the most comfortable with and use them.

Logging:

After you have verified your firewall and rulebase, review the firewall logs. Did the firewall detect all of your scans, did it set off the expected alerts? What traffic did it log and how? If your firewall did not detect most of this activity, something is wrong, you need to be able to see this information. Reviewing the rule base will give you a better understanding of what to look for in the future when auditing your logs. For FW-1, I always recommend Track Long. If you are going to log the rule, log it long so you get all the information. For more information on logs

and alerts with FW-1, check out Intrusion Detection for FW-1 (<http://www.enteract.com/~lspitz/intrusion.html>).

The Tools

Now comes the fun stuff: the tools. One of the best tools for auditing your firewall and firewall rulebase is a good port scanner. As you saw, the biggest priority is identifying what resources are accessible.

Once you have identified what resources can be accessed with your port scanner, you can dig deeper. As discussed above, there are a variety of methods and tools to digging deeper. All of these tools are shareware/freeware, so no excuses. Here are several of my favorites:

ONE OF THE BEST TOOLS FOR AUDITING YOUR FIREWALL AND FIREWALL RULEBASE IS A GOOD PORT SCANNER

Saint (runs on Unix)	Updated version of SATAN, excellent all purpose vulnerability scanner.
Nessus (runs on Unix, client can run on 95/NT)	Similar to SAINT, excellent vulnerability database.
Whisker (runs on anything that has PERL)	Searches websites for vulnerabilities
Firewalk (runs on Unix)	Determine what ports firewall allows through.
NetBIOS Auditing Tool (runs on Unix and 95/NT)	NetBIOS Scanning tool
Winfingerprint (runs on 95/NT)	Enumerates NetBIOS Shares, Users, Groups, and Services
legion (runs on 95/NT)	From the guys at Rhino9, scans for smb shares
Sam Spade (runs on 95/NT)	Similar to WS Ping ProPack, but with some different goodies

Continued on page 12



ISSA CHAPTERS

ALAMO

Contact: William Tompkins, CISSP, CRP, CBCP
UT Health Science CTR • 210-567-2308
tompkins@uthscsa.edu

BALTIMORE

Contact: John Walsh • Allfirst Bank
410-244-4631 • john.p.walsh@allfirst.com

CAPITAL OF TEXAS

Contact: Mike Hamilton, CISSP
Texas Railroad Commission
512-463-7178 • mike.hamilton@rre.state.tx.us

CAROLINAS

Contact: Mark Hughes • Intl. Network Serv.
704-379-1970 • mark_hughes@ins.com

CENTRAL OHIO

Contact: Mark Douglas • Nationwide Insurance
614-249-0825 • douglam1@nationwide.com

CENTRAL PLAINS

Contact: Craig Schiller
Bombardier Aerospace Lear Jet
316-946-7314 • CRAIG.SCHILLER@LEARJET.COM

CHICAGO

Contact: Steve Hunt • Giga Information Group
847-685-6154 • steve.hunt@issa-chicago.org

COLORADO SPRINGS

Contact: George Proeller • Litton PRC
719-567-8022 • proelleg@jnt.osd.mil

CONNECTICUT

Contact: Peter Vogt
203-431-4037 • peter.vogt@e_certify.com

DELAWARE VALLEY

Contact: Brent Frampton • The Vanguard Group
610-669-0684 • Brent_Frampton@vanguard.com

DETROIT

Roger Younglove
734-269-2684 • roger_younglove@ins.com

DENVER

Contact: Jeffrey Ott • Ernst & Young LLP
303-454-6784 • Jeffrey.ott@ey.com

GREATER CINCINNATI

Contact: Terri Dean
VA Med Center • 513-861-3100, Ext. 4410
Terri.Dean@med.va.gov

HAWAII

Contact: Frank B. Lohman • HMSA
808-948-5611 • Frank_Lohman@hmsa.com

INDIANAPOLIS

Contact: Mark Acton, CISSP • Eli Lilly & Co.
317-276-6222 • maa@lilly.com

KANSAS CITY

Contact: JoAnn Fisher
816-459-5016 • jafisher@farmland.com

LATIN AMERICA

Contact: Antonio Quiones
Hitachi Data Systems • 011-525-662-8799

LAS VEGAS

Contact: Michael McKinzie
877-516-7401 • mmckinzie@miragersorts.com

LOS ANGELES

Contact: Steve Haydostian
Information Security Consultant
818-368-1280 • haydoinc@aol.com

MINNESOTA

Contact: Jayne Logan • 612-761-3878
jayne.logan@dhcmail.com

NASHVILLE

Contact: Brian Tatro
615-599-8133 • btatro@btatro.com

NATIONAL CAPITAL AREA

Contact: Bob Giovagnoni • iDefense
703-914-5485 • rgiovagnoni@idefense.com

NEW ENGLAND (BOSTON)

Contact: David Sawin • Fleet Financial Group
401-275-7737 • david_e_sawin@fleet.com

NEW JERSEY

Contact: Bruce L. Murphy, CISSP
Price Water House Coopers
973-236-5440 • bruce.l.murphy@us.pwcglobal.com

NEW MEXICO

Contact: Nellie L. Ward, CISSP • Sandia National Labs
505-844-6038 • nlward@sandia.gov

NEW YORK METRO

Contact: James E. Duffy, CISSP • People's Bank
203-338-2121 • jeduff@peoples.com

NORTH COAST (CLEVELAND)

Contact: Edward Niam Jr. • Corporate Solutions, Inc.
216-528-0130 • csi@corpsolutionsinc.com

NORTH TEXAS

Contact: John McGraw • EDS
972-605-6949 • john.magraw@EDS.com

ORANGE COUNTY

Contact: Dennis Bittner • CDRP • Auto Club of
So. California
714-850-5310 • Bittner.Dennis@AAA.calif.com

OTTAWA

Contact: Ronald D. Chuchryk
iQuest Glogal Inc.
613-727-1448 • rchuch@fox.nstn.ca

PHOENIX

Contact: Cindy Donaldson • Collins Consulting Grp.
480-813-9119 • cdonaldson@collinscg.com

PITTSBURGH

Contact: Richard E. Archer • KPMG
412-232-1590 • reacher@kpmg.com

SACRAMENTO VALLEY

Contact: Samantha Thomas, CDRP
CalPERS • 916-341-2129
samantha_thomas@calpers.ca.gov

SAN DIEGO

Contact: Dave Lyons Jr. • Callaway Golf
760-930-5474 • DavidL@callawaygolf.com

SAN FRANCISCO BAY

Contact: Anjali Atanacio
Infosec Architect/SBC Dir Operations
415-995-3877 • anjali.atanacio@pbdir.com

PUGET SOUND (SEATTLE)

Contact: Frank Simorjay Best Consulting
425-814-8104 • security@bestnet.com

SIERRA VISTA

Contact: Will Lemons • lemons@fhu.disa.mil

SILICON VALLEY

Contact: Steve Trolan
408-358-7653 • steve@trolan.org

SOUTH FLORIDA

Contact: Dale Peterson • Digital Bond
954-797-9445 • peterson@digitalbond.com

SOUTH TEXAS (HOUSTON-DOWNTOWN)

Contact: Harvey Nusz • Aud Force
713-655-8892 • harvey_nasz@auditforce.com

ST. LOUIS

Contact: Carolyn Boemler
Edward Jones & Co. • 314-515-3474
carolyn.boemler@edwardjones.com

TAMPA BAY

Contact: Matthew Decker
Lucent Network Professional Services
813-289-1001, Ext. 362 • prez@tampaissa.org

TEXAS GULF COAST (HOUSTON-CLEAR LAKE)

Contact: Chris Zinn • GTE Internetworking
281-283-8136 • chris.zinn@csoonline.com

TORONTO

Contact: Keith G. Parsons, CISSP
905-683-9830 • picker@idirect.com

For information on upcoming meeting dates for a particular chapter, please call the person listed as the contact for that chapter.

NOTE: Please send chapter information to:

ISSA Headquarters
7044 S. 13th Street • Oak Creek, WI 53154
(414) 768-8000 • FAX: (414) 768-8001
E-MAIL: issa@issa.org

SystemExperts

P.U. 01/02 '00, pg. 11



New ISSA Officers

Five new ISSA officers were announced at the Joint Computer Security Conference:

President:
Howard Schmidt

Director of Education:
Deb Peinert

Director of Operations:
Richard Mosher

Director of Communications:
Dave Cullinane

Director of Public Relations:
Kurt Young

AUDITING YOUR FIREWALL SETUP *Continued from page 10*

If you want to learn more about auditing tools, I recommend you check out securityfocus.com tool database. To learn more about exploit tools, I recommend you check out technotronic.com exploit tool database.

Conclusion

A firewall is only as good as its implementation. In today's dynamic world of Internet access, it is easy to make mistakes during the implementation process. By auditing your firewall setup, you can ensure that the firewall is enforcing what you expect it to, in a secure manner.

Lance Spitzner enjoys learning by blowing up his Unix systems at home. Before this, he was an officer in the Rapid Deployment Force where he blew up things of a different nature.

ISSA®

ISSA Headquarters
7044 S. 13th Street
Oak Creek, WI 53154

FIRST CLASS
U.S. POSTAGE
PAID
WAUKESHA, WI
PERMIT NO. 125
