



THE OPSEC INDICATOR

Volume X

Spring 2000

"Meeting The Challenges of a Changing World"

Testimony of Convicted Computer Hacker Highlights Security Vulnerabilities

A Look Into the Mind of the Adversary

The main goal of Operations Security (OPSEC) is to "get into the mind of the adversary." The following testimony of Kevin Mitnick, a convicted computer hacker recently released from jail was given to the Senate Governmental Affairs Committee hearing on "Cyber Attack: Is The Government Safe?" It provides a unique opportunity to do learn how the mind of a computer adversary works.

Testimony

"Honorable Chairperson Thompson, Distinguished Senators, and Members of the Committee:

My name is Kevin Mitnick. I appear before you today to discuss your efforts to create legislation that will ensure the future security and reliability of information systems owned and operated by, or on behalf of, the Federal government.

I am primarily self-taught. My hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security, and to learn more about how computer systems and telecommunication systems work.

In 1985, I graduated cum laude in Computer Systems and Programming from a technical college in Los Angeles, California, and went on to successfully complete a post-graduate

project in designing enhanced security applications that ran on top of a computer's operating system. That post-graduate project may have been one of the earliest examples of "hire the hacker." The school's administrators realized I was hacking into their computers in ways that they couldn't prevent, and so they asked me to design security enhancements that would stop others' unauthorized access.

I have 20 years experience circumventing information security measures, and can report that I have successfully compromised all systems that I targeted for unauthorized access save one. I have two years experience as a private investigator, and my responsibilities included locating people and their assets using social engineering techniques.

My experience and success at accessing, and obtaining information from computer systems first drew national attention when I obtained user manuals for the COSMOS computer systems (Computer Systems for Mainframe Operations) used by Pacific Bell.

Ten years later, the novel "Cyberpunk" was published in 1991, which purported to be a "true" accounting of my actions that resulted in my arrest on Federal charges in 1988. One of the authors of that novel went on to write similarly fictionalized "reports" about me for the New York Times, including a cover story that appeared July 4, 1994. That largely fictitious story labeled me, without reason, justification, or proof, as the "world's most wanted cybercriminal." Subsequent media reports distorted that claim into the false claim that I was the first hacker on the FBI's "Ten Most Wanted" list. That false exaggeration was most recently repeated during my appearance on CNN's "Burden of Proof" program on February 10, 2000. Michael White of the Associated Press researched this issue with the FBI, and FBI representatives denied ever including me on their "Ten Most Wanted" list.

I have gained unauthorized access to computer systems at some of the

(continued on page 12)

Inside This Issue:

Director's Message	3
Worldwide Threats.....	4
Malady of Midway.....	6
California, Here We Come!.....	9

IOSS Offers New OP 390

by John Glorioso
IOSS Staff

Neither rain, nor sleet, nor even a blizzard could prevent the Program Development Team (PDT) from presenting the newly revised course, **"Program Development for OPSEC Managers."**

The success of the program resulted from the energy, enthusiasm, experience, and participation of the OPSEC manager throughout the training.

The OP 390 course is designed to provide the OPSEC manager, whether new or experienced, with the knowledge and skill to develop or improve an OPSEC program.

The training focuses on Operations Security as a systematic process. The instructional journey begins with the realization that there are no barriers to establishing a successful OPSEC program. As the training progresses, each module addresses specific information needed by the OPSEC manager to build the infrastructure for his own organization's OPSEC program.

The training is reserved for OPSEC managers or coordinators from government entities or government contractors.

Participants should attend an OPSEC fundamentals course and OP 380, "OPSEC for Practitioners" prior to attending OP 390. Under certain circumstances, these requirements may be waived by the IOSS course manager.

Each attendee must submit their organization's strategic plan, organi-

zation chart, and their OPSEC policy to the course manager. These are necessary for the students to apply the course content to their organization's requirements. If these materials are not available, the course manager should be contacted prior to attending.

The pilot course demonstrated that the optimum class size is 16 individuals. The course is a hand-on approach to mastering the tools required to become an effective OPSEC manager.

For further information regarding OP 390, contact John Glorioso, Program Development coordinator and the course moderator at the IOSS on (301) 982-0323.



Program Development Team

OP 390 is just one of the initiative of the IOSS' Program Development Team. After an initial analysis of services, the IOSS provides a PDT to assist customers in developing or streamlining their OPSEC programs. The PDT serves government agencies or private organizations who are just starting an OPSEC program or need to invigorate one.

It is truly an interagency group with members from the National Security Agency, the General Services Administration and the Commerce Department.

Initially, the PDT gives customers guidance on how to break down barriers when beginning an OPSEC program. The PDT also provides insights on marketing, developing a working group, and creating OPSEC training within an organization. The team will

assist in any endeavor needed to help OPSEC managers form and implement an effective and dynamic OPSEC program.

The assistance offered by the PDT includes working with program managers at their facilities, holding work sessions at the IOSS, responding to any questions and assisting OPSEC program managers in any way possible.

The OPSEC Indicator



Published Quarterly by

The Interagency OPSEC
Support Staff

6411 Ivy lane
Greenbelt, Maryland
20770-1405

Thomas P. Mauriello
Director

Lynne M. Yates
Editor

Telephone
(301) 982-0323
FAX
(301) 982-2913

This is a U.S. Government
Publication

*Contents are not necessarily the
views of, or endorsed by, any
government agency.*

Director's Message



Since the establishment of the U.S. Security Policy Board (SPB), the IOSS has participated in the Training and Professional Development Committee (TPDC).

The mission of the TPDC is to take a strategic look at the entire security community and recommend to the SPB standardization and coordination of security training, education and awareness programs, and to achieve efficiency in the development and delivery of such training.

The TPDC goal is to institute effective, customer-oriented professional development and training programs responsive to the needs of the government.

I am happy to report that in February 2000, I was nominated and elected to be the new TPDC Chair for the next year. I am excited by this challenge,

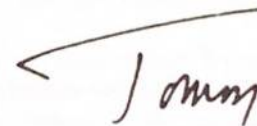
especially because the TPDC has been tasked to develop a plan of action to address three recommendations made by the August 24, 1999 "Report by the Joint Security Commission II."

The issues identified in these recommendations are as follows: the ongoing effort to create and implement core national training for both government and industry security officers; the chartering of a government-wide security awareness program; and the establishment of funding to create security training and awareness projects and research initiatives to be executed by designated departments and agencies.

In simple language, the TPDC is looking at what skills and training the future security professional needs to satisfy the challenges of the new millennium, and how are we going to get there in an efficient, coordinated man-

ner. OPSEC certainly has a role in this regard and we look forward to the opportunity to participate in this effort. More to report on this in future messages.

I look forward to seeing you all at the National OPSEC Conference and Exhibition in Monterey, California from June 5-9. Don't forget to register!



Updates on Courses and Symposia

by Lynne Clark
IOSS Staff



The new courses introduced this fiscal year, "**Counterintelligence and OPSEC**" and "**The Practical Applications Workshop**" have received rave reviews from attendees.

The courses will be offered three more times this fiscal year and there are still openings available. If interested, contact the new IOSS registrar, Margaret Telfer, in Greenbelt, on (301) 982-2438.

The new "**Web Content Security**" course is now available for presenta-

tion "on the road." This course is a must for all who develop or work with web pages. Those interested in having the course brought to your facility and tailored for your personnel, should contact Tami Cook at the IOSS.

The staff has begun working on a new course focusing on "Threat Research." More information will be available in upcoming editions of *The OPSEC Indicator*.

The **European Regional Symposium** will occur in Fall 2000. Prelimi-

nary plans are still under way—the IOSS would like to hold the symposium in Germany in either November or December.

Initially, the symposium was to be this summer, but because many individuals are reassigned during the summer months, it was advisable to wait until late fall.

More information on this will follow in the next edition of this newsletter.

Global Realities, Domestic Concerns

by Tom Harig
IOSS Staff

As America stands on the threshold of a new century, its power and influence are unmatched in the world. Yet, paradoxically, in some instances the threat to its citizens is growing, despite the lessening of Cold War tensions.

This is the picture that the Director of Central Intelligence, George J. Tenet, painted during his annual testimony before the Senate Select Committee on Intelligence on February 2.

Technology Magnifies the Threat

Tenet's remarks emphasized how technology, especially information technology, has "enabled, driven, or magnified" the threat to American citizens.

He reviewed transnational issues and regional issues of vital concern to national security. He discussed how the general advance of science and technology throughout the world has also increased the potential for the proliferation of weapons of mass destruction.

Despite the nuclear capability of China and Russia, mechanisms exist to contain this threat. He noted that the missile threat to the United States from other countries is emerging, but the threat to US interests and forces overseas is "here and now."

Hostile Nations

North Korea, Iraq, and Iran—to name just a few countries that regard the United States with extreme hostility—are all pursuing weapons of mass destruction and the means with which to deliver them, thus complicating and increasing the cost of US planning and intervention; at the same time, these countries improve their deterrence capability, enhance their

prestige, and improve their ability to engage in coercive diplomacy.

Moreover, Tenet added, the ability of the Intelligence Community to give adequate warning to policymakers is slipping.

This is in no way due to a lack of effort of intelligence collectors and analysts, but rather to four main factors: increased proficiency on the part



of our adversaries in the use of denial and deception techniques; the growing availability of dual-use technologies that makes it easier for proliferators to obtain required materials; the growing capacity of countries to import talent to help them overcome technical barriers to proliferation; and the accelerating pace of technological progress that makes information and technology easier to obtain than ever before.

It is an uphill struggle for the Intelligence Community to make progress against these challenges but, he warned, "the hill is getting steeper every year."

Osama bin Laden

In the fight against international ter-

rorism, the number one adversary remains Osama bin Laden, who has not abandoned plans to strike against American interests. Despite what Tenet called "well-publicized interruptions" of his activities, bin Laden still retains the capacity to strike without additional warning.

In fact, it has been noted that his group and others are placing "increased emphasis" on developing surrogates to carry out their operations, further complicating U.S. efforts to detect and neutralize attacks.

Osama bin Laden's network stretches across Europe and Asia, weaving an alliance among radical Sunni Muslims worldwide. Although terrorist groups like bin Laden's rely on conventional weapons to perpetrate acts of violence, Tenet stated there was evidence that groups are seeking chemical, biological, and radiological agents.

Tenet noted that terrorists have also joined the information revolution, using computerized files, E-mail, and encryption to support their operations.

Buying Time

Tenet quite bluntly warned the committee that, despite the success of the United States in thwarting terrorist acts, it has only succeeded in buying time against an increasingly dangerous threat because the root causes of terrorism—poverty, alienation, and ethnic hatreds—are not easily overcome. Ultimately "constant vigilance and timely intelligence are our best weapons," he said.

Tenet was pessimistic about another international threat: that of the narcotics epidemic that has touched millions of American lives. He noted, "Narcotics production is likely to rise

dramatically in the next few years and worldwide trafficking involves more diverse and sophisticated groups.”

Although coca production (for cocaine) has declined in Peru and Bolivia, it has increased in Colombia, and on the other side of the world, there has been a “dramatic increase” in opium production in Afghanistan.

Organized Crime

Tenet also touched on the issue of international organized crime, pointing out that it has become a “serious international security issue,” victimizing not only individuals, but also undermining the political and economic development of entire countries.

Information Warfare

Lastly, Tenet discussed the threat of information warfare, a phenomenon

that barely existed a decade ago. Since the United States relies more than ever on the unimpeded and secure flow of information for its defense and economic health, any adversary that develops a capability to interrupt or stop it wields a powerful weapon.

A number of states are interested in information operations and information warfare as a means to counter the U.S. military superiority.

Tenet described the potential impact such a weapon would have: it can affect the daily lives of American citizens across the country: by degrading the national infrastructure; it provides a “force projection” capability to nations that never had it before; and it will be a basic capability of modern military and intelligence services around the world in the near future.

Tenet went on to discuss regional issues such as what to expect from Russia in the post-Yeltsin era, the unrest in the Caucasus and Central Asia, political turbulence in the Middle East, instability in the Balkans, the enigma of North Korea, and the emergence of China as the world’s “fastest rising power,” and developments in East Asia.

He summarized his testimony by noting that although we are arguably the world’s most powerful nation, this fact does not bestow invulnerability and we must take care to be on guard.

To read Tenet's complete statement, go to the CIA Web site at www.cia.gov and click on "Speeches and Testimony."



Dragontalk

The IOSS has been fortunate in acquiring the services of two highly qualified individuals to assist in our efforts.

George Stephan joins the IOSS as a Senior OPSEC Analyst. George has had a long and distinguished career in the OPSEC field.

George graduated from the U.S. Naval Academy and served for several years in Navy and Marine Corps positions afloat and ashore.

George has more than 21 years of OPSEC experience, having been the command OPSEC officer for the former Strategic Air Command and most recently with Commander of U.S.

Forces in the Pacific.

He has extensive experience in all aspects of OPSEC, particularly in plans, and military operations. George developed and taught the first OP 380, OPSEC Practitioner's Course and compiled an OPSEC Practitioner's Handbook providing detail instruction in training, planning, surveys and OPSEC analysis.

Margaret Telfer is the new Training manager assigned to the IOSS team. As a senior associate for McNeil Technologies, she comes to the staff with a diverse background in both the private and Federal arenas.

Margaret has over 16 years in the security and intelligence fields with the U.S. Army (active and reserve) where her experience included counterintelligence, tactical intelligence and civil affairs.

She began her training management career in 1991 with Lockheed Martin Energy Systems where she helped establish one of the most comprehensive training management systems in the Department of Energy.

Before joining the McNeil staff, Margaret was a regional security operations manager for Pinkerton Security.

She is a certified National Cryptologic School instructor and will be responsible for the scheduling and administrative duties for all IOSS training.

Welcome George and Margaret!

"Victory Disease" Will Prove Fatal for OPSECers Lessons Learned From the Battle of Midway

by Patrick D. Weadon
IOSS Staff

It is said that history is written by the victors. This may be true, but it is always instructive to hear the story from the adversary's point of view.

Thirteen years after the famed Battle of Midway, which marked the end of the Japanese Empire's advance across the Pacific, Mitsou Fuchida, a former captain in the Japanese Imperial Navy was questioned extensively concerning the Imperial Navy's planning regarding the battle. His thoughts, along with those of his compatriot, Masatake Okumiya, are included in the informative book "Midway, The Battle That Doomed Japan."

Fuchida's remarks are most poignant when he summarizes what went wrong in the planning done by the Japanese Imperial Staff. Like many unsuccessful operations, Japan's failure at the tiny Pacific atoll known as Midway was not due to a lack of logistics or training, but rather to a set of assumptions—none of which were based in reality.

The Virus Spreads

"By the time of the Midway battle, arrogance had reached a point where it permeated the thinking and actions of officers and men in the fighting services. This malady has been aptly called "victory disease." The spread of the virus was so great that its effects were found on every level of the planning and execution of the Midway operation."

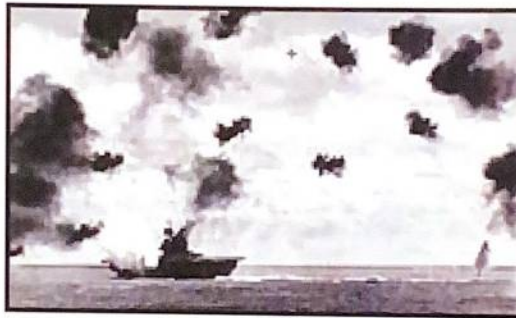
The war had gone so well for Japan up to the spring of 1942 that their Midway planners seemed to work entirely

on the basis of what the enemy *would probably do* rather than what he might possibly do or was capable of doing.

Battle Advantages

Consider for a moment Japan's advantages prior to the battle. The Imperial Fleet sortied with 4 carriers, the Akagi, Kaga, Hiryu, and Soryu, carrying a total of 261 aircraft.

The pilots of the Imperial Navy



The U.S.S Yorktown under Japanese attack.

were highly experienced, battle hardened veterans of a brilliant eastward march across the Pacific beginning at Pearl Harbor, and for which there appeared to be no end in sight.

Admiral Yamamoto, the architect of the many brilliant victories, promised that after the outbreak of war with the United States he would "run wild for a year," and run wild he did.

In the spring of 1942, one did not have to be Lord Nelson to be aware that one more major defeat would leave the Hawaiian Islands and perhaps even California open to Japanese Invasion. (Note: Most historians agree that it would have been difficult for the Japanese to launch a formal attack on the U.S. mainland, however at the

time it was seen by many as a serious possibility).

It is little wonder that the Imperial staff had what Fuchida termed "victory disease." In hindsight, it was logical for them to feel confident about their chances of putting a quick end to any formal opposition in the Pacific.

Conversely, on the U.S. side, the situation was less than promising. Admiral Nimitz, Yamamoto's American counterpart had only three carriers to meet one of the most impressive armadas of all time.

In fact, he barely had three. The Enterprise and Hornet were ready to fight, however the Yorktown, barely seaworthy, had been badly damaged at the battle of the Coral Sea and needed approximately 90 days worth of repairs.

Nimitz informed the dock crews that they had two days to get the ship ready for battle.

Miraculously, the carrier was somehow made ready, but even more troubling to Nimitz was the fact that many of the pilots flying the 233 aircraft were "rookies."

In fact, the Hornet aircrews had never been in combat. (The carrier situation was so dire that the United States asked Great Britain to loan the Navy a carrier from the Indian Ocean—the request was denied.) Nimitz' crippled fleet sortied to a point north of Midway and waited.

Messages Intercepted

Unknown to Yamamoto, U.S. Naval Intelligence intercepted several messages indicating that Midway would be Japan's next objective.

The Japanese messages mentioned the objective "AF" over and over. Nimitz, not sure if Midway was the target, had fake messages sent in the clear indicating that Midway's water filtration system was completely out

of operation. Later that week another message was intercepted from Japanese Naval communications "AF needs water." Armed with this information, Nimitz was able to lay a formidable trap.

Early Moments

The early moments of the battle did not go well for the Americans. Despite finding the Japanese fleet, dozens of torpedo attacks failed to find their mark. However, at 10:20 a.m., on June 4th, Navy dive-bombers arrived on the scene. Due to the earlier torpedo attacks, the Japanese fighters were at sea level, leaving the dive-bombers virtually unopposed.

To make matters worse for the Japanese, when the dive-bombers appeared, the flight decks were covered with bombs and torpedoes. In a matter of moments, the Akagi, Kaga and Soryu were all burning and sinking to the bottom of the sea.

OPSEC Lessons

So what are we to make of the miracle at Midway? What does the battle teach us about OPSEC? Well for one, it clearly shows how "victory disease" can cripple even the most well-prepared organization.

The American command (which prior to Pearl Harbor failed to even consider the possibility that Japan could be a worthy adversary) finally woke up and realized what was at stake. Unlike Pearl Harbor and the host of disasters that followed, nothing was left to chance.

Some still say the American Navy was "lucky" at Midway. But as the old adage goes "the harder you prepare the luckier you get." Nimitz and his staff had indeed worked hard and learned to *think like their adversaries*. In the end this was the key.

Other Cases

In conclusion, victory disease has always been with us. The English King Harold came down with a bad case of it in 1066 when he underestimated the ability of William the Conqueror to bring his armies across the channel.

The commander of the Hessians at Trenton in 1776 also suffered from its effects on Christmas Eve 1776, when he assumed that George Washington and his army were destitute and could not possibly attack his position.

Santa Anna, the commander of the Mexican forces at San Jacinto (the crucial battle of the Texas Revolution) proved to have one of the worst cases in history, when he ordered his 2,500 troops to take a siesta shortly before being attacked by a ragtag Texas Army led by Sam Houston. The entire battle was over in less than an hour.

In more recent times, victory disease has broken out at places like Dien Bien Phu, where a modern French army was forced to surrender to the forces of the Viet Minh in the early 1950's—and tragically at Mogadishu, in the 1990's, when a small contingent of U.S. Army Rangers were sent on a mission to find the Somali war lord Mohammed Adid. The group was not accompanied by armor or artillery—they were ambushed and killed by an angry mob.

The Goal of OPSEC

The goal of the OPSEC community is to find new and innovative ways to protect critical information. In addition, everything possible should be done to put in place a mindset that *never takes anything for granted*. If we can mentally vaccinate ourselves against overconfidence we will have the ability to save lives and to ensure future victories over our adversaries, whoever they may be.

From the Editor

As the Editor of *The OPSEC Indicator*, I would like to extend an invitation to all of you in the OPSEC and government communities to submit articles for publication.

The primary mission of the Inter-agency OPSEC Support Staff is to support U.S. government departments and agencies and government contractors with a national security mission.

The goal of this publication is to present items of interest and address the concerns of individuals from these organizations.

Many subscribers to this newsletter are OPSEC program managers or OPSEC professionals with vast experience and knowledge. Perhaps some of you may wish to share some success or "war" stories that carry a potent OPSEC message.

Anyone may submit articles by mail or via E-mail to ioss@radi-um.nesc.mil or by fax to (301) 982-2913. Submissions to *The OPSEC Indicator* are subject to editing for space, clarity and classification.

For additional information, please contact me at the IOSS. I look forward to working with all of you in the future!

Lynne Yates



Mark Your Calendar

**2000 National OPSEC
Conference &
Exhibition**

*June 6 - 9, 2000
Hyatt Regency Monterey
Naval Postgraduate School
Monterey, California*

*Preconference Seminars -
June 5, 2000*

*Join us in Monterey for a week
of outstanding briefings, work-
shops, and exhibits.*



For more information contact:
McNeil Technologies, Inc.
Phone: 410-553-6465
Fax: 410-553-9275
E-mail: [opsecconf@
mcneiltechmd.com](mailto:opsecconf@mcneiltechmd.com)



Join us in Monterey!

The National Conference and Exhibition is fast approaching. We will be at a wonderful facility in Monterey. Speakers are working on dynamic presentations and the management staff is going all out to make the event an enjoyable one. A tentative schedule is listed below - *the schedule may change* due to last minute conflicts. One of the highlights will be the National OPSEC Awards Luncheon on Tuesday. If you haven't received a flyer in the mail, please call the IOSS or visit the website at www.ioss.gov for registration and up-to-date schedule information — or call the McNeil Technologies staff at (410) 553-6465 for additional information.

Preliminary National OPSEC Conference and Exhibition 2000 Schedule					
Monday — June 5, 2000 — Preconference Seminars					
NPGS Engineer's Aud.		Windjammer	Spyglass	Big Sur	Cypress
0800-1430	Threat Research	OP 300	Web Security	CI and OPSEC	Open Source Research
1445-1630	Mining The Internet				
Tuesday — June 6, 2000 — Conference and Exhibits					
Regency Grand Ballroom					
0800 - 0815	Welcome from Director NSA				
0815 - 0900	Protecting Commercially Sensitive Information in the World's Largest Aerospace Company				
Monterey Grand Ballroom					
0930-1100	National OPSEC Awards Ceremony				
1100-1200	Awards Luncheon				
1215-1315	Awards Luncheon Speaker				
Big Sur		Windjammer	Cypress		Spyglass
1345-1445	Critical Information The Last Mile	Antiterrorism	Proprietary Issues	What's A Pound of Your Info Worth?	
1500-1630	Commercial Comms Vulnerabilities	Technology Collection Trends	Competitive Intelligence & Corporate Espionage	Web Security Roundtable	
1630-1830	Reception/Exhibits Grand Opening				

Wednesday — June 7, 2000 — Conference and Exhibits

	Big Sur	Cypress	Regency IV-V	Windjammer	Spyglass
0800-0900	Law & Disorder	National Infrastructure Protection Ctr.	What's a Pound of Information Worth?	FUNDamentals of Running a Successful OPSEC Program	Motivation Through Communication
0915-1045	Technology Collection Trends	Analytical Risk Management	Competitive Intelligence & Corporate Espionage		
1100-1200	OPSEC & Industry	Economic Espionage	Antiterrorism	Managed Access Procedures	IOSS & OPS
1200-1330	LUNCH (Box Lunches in the Regency Main Ballroom)				
1330-1430	Extranet for Security	The Mind Has No Firewall	Information Assurance: Implication for OPSEC	OPSEC Surveys Workshop	Computer Security
1445-1545	FINCEN	Situational Awareness Training	OPSEC & Law Enforcement in the U.S.		

Thursday — June 8, 2000 — Conference

0800-0900	Law and Disorder OPSEC on Trial	The Future of OPSEC	Cyber Threat to the Critical Infrastructure	Managed Access Procedures	Information Assurance Implications for OPSEC
0915-1015	OPSEC & Law Enforcement in U.S. Border Patrol	Situational Awareness Training	OPSEC & Industry	Military Contingency OPSEC Planning	Computer Security
1030-1130	National Infrastructure Protection Center	Extranet for Security Professionals	FINCEN		
1130-1300	LUNCH (Box Lunches in the Regency Main Ballroom)				
1200-1245	Working Lunch: Conference Debrief in Regency IV-VI				

Thursday — June 8, 2000 — Conference (continued)

	Big Sur	Cypress	Regency IV-VI	Windjammer	Spyglass
1300-1400	OPSEC and the DD254	Cyber Threat to the Critical Infrastructure	Economic Espionage ANSIR Program	The FUNdamentals of Running a Successful OPSEC Program	OPSEC Surveys Workshop
1415-1545	Competitive Intelligence & Corporate Espionage	Commercial Communications Vulnerabilities	Analytical Risk Management		

Friday — June 9, 2000 — Classified Sessions

	Naval Postgraduate School
0800-0900	Chinese Intelligence Threat
0915-1015	Foreign Interest in Your Website: The Value of OPSEC
1030-1200	Counterintelligence in America
1200-1245	Lunch
1245-1345	Trends in Adversary Denial and Deception
1400-1530	DICE 2000



The OPSEC Professionals Society
will present

Risk Techniques in the Technology Age
May 12

Working Together for Solutions for
A More Secure World
June 27-28

For location, times, and registration information check the OPS webpage at
www.opsec.org

(continued from page 1)

largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

After my arrest in 1995, I spent years as a pretrial detainee without benefit of bail, a bail hearing, and without the ability to see the evidence against me, combined circumstances which are unprecedented in U.S. history according to the research of my defense team.

In March 1999, I pled guilty to wire fraud and computer fraud. I was sentenced to 68 months in Federal prison with 3 years supervised release.

Conditions

The supervised release restrictions imposed on me are the most restrictive conditions ever imposed on an individual in U.S. Federal court, again according to the research of my defense team.

The conditions of supervised release include, but are not limited to, a complete prohibition on the possession or use, for any purpose, of the following: cell phones, computers, any computer software programs, computer peripherals or support equipment, personal information assistants, modems, anything capable of accessing computer networks, and any other electronic equipment presently available or new technology that becomes available that can be converted to, or has as its function, the ability to act as a computer system or to access a computer system, computer network, or telecommunications network.

In addition to these extraordinary conditions, I am prohibited from acting as a consultant or advisor to individuals or groups engaged in any computer-

related activity. I am also prohibited from accessing computers, computer networks, or other forms of wireless communications myself or through third parties.

I was released from Federal prison on January 21, 2000, just 6 weeks ago. I served 59 months and 7 days, after earning 180 days of time off for good behavior. I am permitted to own a land line telephone.

Computer Systems Vulnerabilities

The goal of information security is to protect the integrity, confidentiality, availability and access control to the information. Secure information is protected against tampering, disclo-



sure, and sabotage. The practice of information security reduces the risk associated with loss of trust in the integrity of the information.

Information security is comprised of four primary topics: physical security, network security, computer systems security, and personnel security.

Each of these four topics deserves a complete book, if not several books, to fully document them. My presentation today is intended to provide a brief overview of these topics, and to present my recommendations for the manner in which the Committee may create effective legislation.

Uncontrolled physical access to computer systems and computer net-

works dramatically increases the likelihood that the system can and will suffer unauthorized access.

Hardware may be locked in rooms or buildings, with guards, security cameras, and cypher-controlled doors. The greatest risk to information security in apparently secure hardware environments is represented by employees, or impostors, who appear to possess authorization to the secured space.

Data Security

Government agencies require formal backup procedures to ensure against data loss. Equally stringent requirements must be in place to ensure the integrity and security of those backup files. Intruders who cannot gain access to secure data but who obtain unauthorized access to data backups successfully compromise any security measures that may be in place, and with much less risk of detection.

Network Security

Stand-alone computers are less vulnerable than computers that are connected to any network of any kind. Computers connected to networks typically offer a higher incidence of misconfiguration, or inappropriately enabled services, than computers that are not connected to any network. The hierarchy of network "insecurity" is as follows:

- Stand-alone computer—least vulnerable.
- Computer connected to a LAN, or local area network—more vulnerable.
- Computer and a LAN accessible via dial-up—even more vulnerable.
- Computer and LAN connected to internet—most vulnerable of all.

Unencrypted network communications permit anyone with physical access to the network to use software to monitor all information traveling

over the network, even though it's intended for someone else. Once a network tap is installed, intruders can monitor all network traffic, and install software that enables them to capture, or "sniff," passwords from network transmissions.

Dial-in Access

Dial-in access increases vulnerabilities by opening up an access point to anyone who can access ordinary telephone lines. Off-site access increases the risk of intruders gaining access to the network by increasing the accessibility of the network and the remote computer.

Computer systems that are not connected to any network present the most secure computing environment possible. However, even a brief review of stand alone computer systems reveals many ways they may be compromised.

Operating Systems

The operating systems control the functions of the computer: how information is stored, how memory is managed, and how information is displayed—it's the master program of the machine. At its core, the operating system is a group of discrete software programs that have been assembled into a larger program containing millions of lines of code. Large modern day operating systems cannot be thoroughly tested for security anomalies, or "holes," which represent opportunities for unauthorized access.

"Rogue" software applications can be installed surreptitiously, or with the

unwitting help of another. These programs can install a "back door", which usually consists of programming instructions that disable obscure security settings in an operating system and that enable future access without detection; some back door programs even log the passwords used to gain access to the compromised system or systems for future use by the intruder.

Ineffective Passwords

Computer users often choose passwords that are in the dictionary, or that have personal relevance, and are quite predictable. Static, or unchanging, passwords represent another easy method for breaching a computer system—once a password is compromised, the user and the system administrators have no way of knowing the password is known to an intruder.

Dynamic passwords, or non-dictionary passwords are problematic for many users, who write them down and keep them near their computers for easy access—their own, or anyone who breaches physical security of the computer installation.

Uninstalled Software Updates

Out-of-date system software containing known security problems presents an easy target to an intruder. Systems administrators cannot keep systems updated as a result of work overload, competing priorities, or ignorance. The weaknesses of systems are publicized, and out-of-date systems typically offer well-known vulnerabilities for easy access.

Default Installations

Default installations of some operating systems disable many of the built-in security features in a given operating system. In addition, system administrators unintentionally misconfigure systems, or include unnecessary services that may lead to unauthorized access.

Again, these weaknesses are widely publicized within the computing community, and default or misconfigured installations present an easy target.

The most complex element in information security is the people who use the systems in which the information resides.

Weaknesses in personnel security negate the effort and cost of the other three types of security: physical, network, and computer system security.

Social Engineering

Social engineering, or "gagging," is defined as gaining intelligence through deception. Employees are trained to be helpful, and to do what they are told in the workplace. The skilled social engineer will use these traits to his or her advantage as they seek to gain information that will enable them to achieve their objectives.

E-mail Attachments

E-mail attachments may be sent with covert code embedded within. Upon receiving the e-mail, most people will launch the attachment, which can lower the security settings on the target machine without the user's knowledge.

The likelihood of a successful attempt using this method can be increased by following up the e-mail submittal with a telephone call to prompt the person to open the attachment.

Information Security Exploits

Information security exploits are the methods, tactics, and strategies used to breach the integrity, confidentiality, availability or access control of information.

Discovery of compromised information security has several consequences, the most important of which is the decline in the level of trust associated with the compromised information and systems that contain that information.



Examples of typical security exploits follow.

Physical Security Exploits

Using deception or sheer bravado, the intruder can walk into the off site backup storage facility, and ask for the physical data backup by pretending to be from a certain agency.

The intruder can claim that particular backup is necessary to perform a data restoration. Once an intruder has physical possession of the data, the intruder can work with the data as though he possessed superuser, or system administrator privileges.

If an intruder gains physical access to a computer and is able to reboot it, the intruder can gain complete control of the system and bypass all security measures—an extremely powerful exploit, but one that exposes the intruder to great personal risk because they're physically present on the premises.

Network Security Exploits

Physical access to a network enables an intruder to install a tap on the network cable, which can be used to eavesdrop on all network traffic. Eavesdropping enables the intruder to capture passwords as they travel over the network, which will enable full access to the machines whose passwords are compromised.

Network software exists that probes computers for weaknesses. Once one system's weaknesses are revealed and the system is compromised, the intruder can install software (called "sniffer" software) that compromises all systems on the network.

Following that, an intruder can install software that logs the passwords used to access that compromised machine. Users routinely use the same or similar passwords across multiple machines; thus, once one password for one

machine is obtained, then multiple machines can be compromised

Computer System Exploits

Vulnerabilities in programs (e.g., the UNIX program send mail) can be exploited to gain remote access to the target computer. Many system programs contain bugs that enable the intruder to trick the software into behaving in a way other than that which is intended in order to gain unauthorized access rights,



even though the application is a part of the operating system of the computer.

A misconfigured installation on a computer in operation at the Raleigh News and Observer, a paper in Raleigh, North Carolina, demonstrates the problematic aspect of system misconfiguration.

Using the UNIX program "Finger," which enables one to identify the users that are currently logged into a computer system, I created a user name on the computer system I controlled.

The user name I assigned myself matched exactly the user name that existed on the target host. The misconfigured system was set to "trust" any computer on the network, which left the entire network open for unauthorized access.

Personnel Security Exploits

Social Engineering involves tricking or persuading people to reveal informa-

tion or to take certain actions at the behest of the intruder. My work as a private investigator relied heavily on my skills in social engineering. In my successful efforts to social engineer my way into Motorola, I used a three-level social engineering attack to bypass the information security measures then in use.

First I was able to convince Motorola Operations employees to provide me, on repeated occasions, the pass code on their security access device, as well as the static PIN.

The reason this was so extraordinary is that the pass code on their access device changed every 60 seconds: every time I wanted to gain unauthorized access, I had to call the Operations Center and ask for the password in effect for that minute.

The second level involved convincing the employees to enable an account for my use on one of their machines, and the third level involved convincing one of the engineers who was already entitled to access one of the computers to give me his password.

I overcame that engineer's vigorous reluctance to provide the password by convincing him that I was a Motorola employee, and that I was looking at a form that documented the password that he used to access his personal workstation on Motorola's network—despite the fact that he never filled out any such form! Once I gained access to that machine, I obtained Telnet access to the target machine, access which I had sought all along.

Voice Mail and Fax Exploit

This exploit relies on convincing an employee at a large company to enable a voice mailbox: the intruder would call the people who administer the voice mailboxes for the target company and request a mailbox. The pretext would

be that the intruder works for a different division, and would like to retrieve messages without making a toll call.

Once the intruder has access to the voice mail system, the intruder would call the receptionist, represent himself as an employee of the company, and ask that they take messages for him; last but not least, the intruder would request the fax number and ask that incoming faxes be held for pickup.

This sets the stage for the call to the target division of the company. At this point, the intruder would call the target division to initiate the fax exploit with the goal of obtaining the targeted confidential company information.

During that call the intruder would identify himself as an employee of the division whose voice mail and fax systems have just been compromised, he would cite the voice mail box in support of his identity, and would social engineer the target employee into faxing the target information to the compromised fax number located at one of their other offices.

Now the intruder would call the receptionist, tell the receptionist that he's in a business meeting, and ask that the receptionist fax the confidential material "to the hotel." The intruder picks up the fax containing confidential information at the secondary fax, which cannot be traced back to either the intruder or the targeted company.

I used this exploit to successfully compromise ATT's protected network access points routinely. ATT had learned that a system had been compromised by unauthorized entry at a central network access point called "DataKit."

They imposed network access passwords on all DataKits to inhibit unauthorized access. I contacted one of the manager's secretaries and used the Fax Exploit to convince the secretary to fax me the password that enabled access to

a DataKit that controlled dial-up access to ATT's worldwide computer network.

Recommendations

The Voice Mail and Fax Exploit demonstrates the most important element in my testimony today: that verification mechanisms are the weak link in information security, and voice mail and fax are the tools used to verify the authenticity of the credentials presented by someone seeking physical, network, or computer systems access.

The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice.

Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.

The corporate security measures that I breached were created by some of the best and brightest in the business, some of whom may even have been consulted by the committee as you drafted your legislation, Senate Bill S1993. S1993 represents a good first step toward the goal of increasing information security on government computer systems. I have several recommendations that I hope will increase the effectiveness of your bill.

- Each agency perform a thorough risk assessment of the assets they want to protect.

- Perform a cost-benefit analysis to determine if the price to protect those systems represents real value.

- Implement policies, procedures, standards and guidelines consistent with the risk assessment and cost benefit analyses.

- Employee training to recognize sophisticated social engineering attacks is of paramount importance.

- After implementing the policies, procedures, standards and guidelines, create an audit and oversight program that measures compliance throughout the affected government agencies.

- The frequency of those audits ought to be determined consistent with the mission of a particular agency: the more valuable the data, the more frequent the audit process.

- Create a numeric "trust ranking" that quantifies and summarizes the results of the audit and oversight programs described above. The numeric "trust ranking" would provide at-a-glance ranking – a report card, if you will — of the characteristics that comprise the four major categories defined above: physical, network, computer systems, and personnel.

- Effective audit procedures - implemented from the top down - must be part of an appropriate system of rewards and consequences in order to motivate system administrators, personnel managers, and government employees to maintain effective information security consistent with the goals of this committee.

Conclusion

Obviously a brief presentation such as the one I've made today cannot convey adequately the measures needed to implement effective information security measures. I'm happy to answer any questions that may have been left unanswered for any members of the committee."

To read this testimony in addition to and the testimony of other witnesses, visit the Committee on Government Affairs site on the U.S. Senate homepage at www.senate.gov.

Quarterly Quote



Discovery consists of seeing
what everybody else has seen
and thinking what nobody has
thought.

–Albert Szent-Gyorgyi Nagrapolt
1893-1896
Nobel Prize Winning Chemist

Interagency Opsec Support Staff
6411 Ivy Lane
Greenbelt, MD 20770-1405

First Class Mail
Postage and Fees Paid
National Security Agency
Ft. Meade, MD
Permit No. G-712