American Bar Association

National Security Law Report

Volume 20, Number 4 STANDING COMMITTEE ON LAW AND NATIONAL SECURITY August 1999

Deputy Secretary of Defense Dr. John J. Hamre Challenges Standing Committee to Lead Debate on Homeland Defense

Edited by William E. Conner

On April 29, 1999, the Standing Committee was treated to the thoughtful remarks of Deputy Secretary of Defense Dr. John J. Hamre on the often-overlooked topic of U.S. homeland defense. Dr. Hamre challenged the Standing Committee to heighten awareness of the need for homeland defense and to seek out opportunities for serious discussion of these issues.

Dr. Hamre set the context of his challenge with the observation that any discussion of homeland defense elicits a negative visceral reaction from many Americans. He believes they are frightened of the Department of Defense (DoD) actively preparing the United States to defend itself from a terrorist attack. Dr. Hamre emphasizes, however, that homeland defense is simply too important an issue for DoD to set aside, although DoD must remain very sensitive to the proper role of the military in homeland defense.

The United States does not have ready reserves of law enforcement personnel to call upon in a crisis. Rather, we maintain civil response capabilities for routine day to day operations. As a result, during a time of crisis, exceptional resources from the federal government must augment local law enforcement capabilities. DoD is the only organization that has the ability to mobilize resources for such

Continued on page 4

Inside

02 LtCol Charlie **Williamson** on *Cyberdefense*
03 Cindy **Cohn** on *U.S. v. Bernstein*
03 John **Harrelson** reports on *HASC Hearing on Security at the DoE*
10 Andy **Johnston** & Jeehye **Yun** on *Privacy*
11 Greg **Hoglund** on *E-Commerce*
14 David **Tubbs** on *Exploits*

What's a Pound of Your Information Worth? Constructs for Collaboration and Consistency

by LtCol Perry G. Luzwick, U.S. Air Force

> *Some day on the corporate balance sheet there will be an entry which reads "Information;" for in most cases the information is more valuable than the hardware which processes it.*
>
> *Grace Murray Hopper*
> *Admiral, U.S. Navy (Ret)*

Introduction

Headlines and titles tell us we are in the Information Age, we are using the Information Highway, and we are in a knowledge-based economy. Information must be important. The number one issue facing corporate America and the federal government is how to value information beyond subjective estimates, changing it from an intangible to a tangible asset. This leads directly to an approach for protecting information because certain types of information are worth more than others. Value, or perceived value, drives resource allocation. But if information is important, why aren't there national accounting standards for it? How should a corporation value information? Can there be more than one value? What information is critical enough to require deadly force by law enforcement or the military? Articles have been published on the value of information by accountants, economists, psychologists, artificial intelligence researchers, knowledge management experts, and others, but quantitative approaches still elude us. Until a national standard is established, information will have simultaneous multiple values.

The Information Environment (IE)

The IE is comprised of several interrelated areas. Information moves across information infrastructures to support information-based processes. Information as used

Continued on page 6

Emerging Issues in Cyberdefense

by LtCol Charlie Williamson, U.S. Air Force

Threats to America's computer infrastructure have never been greater. Focused, but relatively harmless, web page hacks and unfocused, but highly disruptive, viruses and worms like Melissa and ExploreZip have become front-page stories. Americans in all walks of life are starting to see the reality of the threat that the Department of Defense has been facing for years. While these challenges have been handled, the growing threat to DoD is more serious and may need a fresh look at the law.

The DoD has more than 2.1 million computers, 10,000 local area networks, and was the target of more than 250,000 *detected* intrusion attempts last year. Cyber attacks offer the capability to exploit sensitive databases, affect transportation systems, and degrade military capabilities with almost complete anonymity from almost anywhere in the world. DoD's vulnerability was demonstrated in 1997 and 1998 in exercises and real world crises. While the military services and defense agencies vigorously addressed network security, they lacked a good means to assess when an attack crossed organizational boundaries and how they should coordinate a strategic defense. All of this led Secretary of Defense (SECDEF) William Cohen to create the Joint Task Force - Computer Network Defense (JTF-CND).

Located with the Defense Information Systems Agency (DISA), the JTF takes advantage of intrusion detection capabilities in the unified commands, military services, and defense agencies. The JTF receives data from these intrusion detection sources, and with data gathered from off-line analysis, fuses it with information about ongoing operational missions, and intelligence and technical data. With this correlated information, the JTF assesses the impact to network operations and military operations, identifies courses of action that will restore the network, coordinates with appropriate DoD or non-DoD organizations, prepares a plan to execute and, with approval, executes that order.

The JTF-CND commander, Air Force Major General John H. Campbell, is also the vice-director of DISA. As the JTF-CND commander, he reports to the SECDEF through the Chairman of the Joint Chiefs of Staff. He has directive authority over assigned forces designated by Service components for execution of the CND mission, and coordinates with and supports commanders of combatant commands.

Senior leaders agree that eventually this mission should be assigned to a unified command. The 1999 Unified Command Plan will assign the CND mission to U.S. Space Command, effective October 1, 1999, subject to Presidential approval. The JTF provides an interim operational capability until U.S. Space Command can assume the mission.

How is this important to national security law? The world is potentially entering a new age, with information supplanting industry just as industry supplanted agriculture as the world's dominant economic force. At the very least, the world is doing business in dramatically new ways whose impacts are not always apparent. When cultures experience tectonic shifts, laws and lawyers are needed more.

E-mail and Internet access have become common features in millions of homes and businesses. Users want privacy and uninterrupted operations. At the same time, the number and severity of hacking incidents is increasing dramatically. Will users continue to rely on law enforcement or will they feel driven to take self-protective "hack-back" measures that may cause them to unwittingly violate the Computer Fraud and Abuse Act (18 U.S.C. §1030)? The Internet is already a sort of "Wild West." Making it safe for its good citizens may require empowering "Sheriffs" and the "U.S. Cavalry" in new ways. This issue raises many questions.

Some questions affect the JTF's law enforcement cell and technical arms. For instance, the Electronic Communication Privacy Act amended the 1968 federal wiretap law to make it clear that intercepting computer communications is a crime. However, it also allowed providers of electronic communication services to monitor their systems for health and security. Should it be amended to clarify the

Continued on page 5

The ABA National Security Law Report
<http://www.abanet.org/natsecurity/>

The *National Security Law Report* (*N.S.L.R.*) contains articles concerning the law relating to the security of our Nation and associated topics. The *N.S.L.R.* is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise.

To receive the *N.S.L.R.*, contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; FAX (202) 662-1032; or natsecurity@abanet.org. Comments or original articles should be sent to: Gary Sharp, 28 Bridgeport Circle, Stafford, VA 22554-1776; or WGSharp@aol.com.

What's A Nice Girl Like You Doing Challenging the U.S. Government's Cryptography Regulations?

by Cindy A. Cohn

A recent article in Newsweek began: "You would think the U.S. government would have little to fear from Dan Bernstein, John Gilmore and Cindy Cohn."[1] While I can't speak for Dan or John, this statement certainly rings true for me.

I never pictured myself as one who would challenge or threaten U.S. national security. Yet at the same time, before my involvement with the *Bernstein* case, I never imagined that the U.S. government would be determined to implement and defend a scheme as plainly unconstitutional and irrational as the current encryption regulations. Or, that it would do so claiming a "national security" concern that is, to quote the U.S. District Court, "based upon a belief that terrorists can't type."[2] The Court was quoting a National Academy of Sciences report, specifically recognizing that existing encryption export regulations do not control encryption software written on paper even though the same information in any electronic format is regulated as a threat to national security.

For the last five years, I have served as lead counsel[3] in a case entitled *Bernstein v. U.S. Dept. of Justice, et al.* This case challenges the U.S. government's encryption regulations on several grounds, chiefly that they are a prior restraint on speech in violation of the First Amendment to the U.S. Constitution.

The regulations require U.S. cryptographers and others, including companies that wish to sell cryptography, to submit their computer programs to a government bureaucrat for review and "case by case" licensing. The regulations give no specific criteria for the agency's licensing decisions, no time limit for those decisions and no judicial review of those decisions. As a result, the record in the case is replete with examples of situations in which the agency has exercised its discretion erratically, irrationally, and, in some cases, has simply refused to make a decision, leaving a person in limbo indefinitely.

The regulations license encryption software in electronic form regardless of the fact that it is already available abroad, regardless of the fact that it can be freely exported on paper and then simply scanned or typed into a computer, and regardless of the fact that it is exported for

Continued on page 5

PFIAB Chairman Testifies Before the HASC on Security at the U.S. Department of Energy

Edited by John K. Harrelson

The Honorable Warren B. Rudman, Chairman of the President's Foreign Intelligence Advisory Board (PFIAB), testified before the House Armed Services Committee (HASC) on Thursday, June 24, 1999. This is a summary of Chairman Rudman's evaluation on the state of security at the Department of Energy (DoE).

On March 18, 1999, President Clinton requested that the PFIAB report on the security threat at DoE's weapons labs and the adequacy of the measures that have been taken to address it. Chairman Rudman formed a Special Investigative Panel and produced a report three months later entitled "Science at its Best, Security at its Worst." As the PFIAB Chairman, former member of the Senate Select Committee on Intelligence, and former Attorney General of New Hampshire, Chairman Rudman was well qualified to review the security threat facing DoE and the United States. On June 24, 1999, Chairman Rudman reviewed the findings of the Special Investigative Panel for the full committee of the HASC.

Chairman Rudman began his presentation by labeling the DoE as unorganized, poorly managed, and in need of a dramatic change. He went on to say that the department must be "streamlined" in order to handle the significant job of securing the nation's nuclear technology. He also clarified the seriousness of the problems existing within DoE by comparing the topic at hand to the cliché "if it ain't broke, don't fix it." Chairman Rudman concluded, however, that DoE is so broke that it is beyond fixing, and that it must be replaced. He declared that it is not about security, but about management and the ability to hold everyone within the divisions of DoE accountable.

Chairman Rudman asserted that one of the main issues is the physical and personnel design structure of DoE. Using visual aides, he displayed the physical distance between the "bureaucracy" in DoE and the laboratories and lower-level personnel offices. He believes that Congress and the President of the United States must restructure DoE to make the interpersonal relationships more efficient and institutionalized. He proposed that the problems within the department must be addressed in an "all or none" fashion, and that this can only be achieved by the immediate supervisors in each division that have the ability to relate personnel problems and ideas to top officials.

Continued on page 10

Dr. Hamre on Homeland Defense . . .

Continued from page 1

undertakings. The recent NATO summit in Washington, D.C. was a prime example of such successful cooperation between local and federal organizations.

A major challenge facing the United States, Dr. Hamre believes, is a serious terrorist attack with no warning that will test our response capability to the limit. Dr. Hamre reported that last year there were more than 100 alleged terrorist threats nationwide, although the vast majority were hoaxes. At some point one of them will be real, yet Dr. Hamre notes that many Americans still seem more fearful of military intervention than of an actual terrorist attack. Dr. Hamre believes that, paradoxically, the most serious threat to civil liberties will occur if the United States does nothing to prepare for the day such an attack occurs, leaving the President with only one option: martial law.

Digital camera compliments of THREE OAKS CAPITAL, LLC

Deputy SecDef John Hamre responds to questions after the end of his remarks on homeland defense.

Dr. Hamre detailed four principles that help define the military's proper role in homeland defense. First, DoD will not tolerate a situation which permits ambiguity over who has authority to do what, when, and with whom. Thus, he stated, there must be an unequivocal chain of authority and accountability for DoD's actions in a domestic crisis.

Second, DoD will never seek any other role than that of a *supporting* role to local law enforcement. During the recent NATO summit, DoD troops were under the tactical control of the Attorney General. The Secretary of Defense only had the power to veto deployment. He did not exercise direct control or have power to authorize any action. Dr. Hamre emphasized that DoD does not want to be in a situation where the military poses a threat to American civil liberties.

Third, DoD only intends to buy equipment and take action which are largely related to DoD's statutory warfighting mission, however, much of its equipment is applicable to a domestic crisis. For example, Dr. Hamre explained that DoD is the only organization that can set up a barrier nursing station for 10,000 casualties in two days, or can perform thoracic surgery in a chemical environment, or provide a block-by-block dispersal analysis within minutes of an Anthrax outbreak.

Fourth, DoD's domestic capabilities must be grounded in the National Guard and reserve units. During conflict abroad, Dr. Hamre explained that active military units are forward deployed while our reserves reinforce and support. In a domestic crisis, however, the situation is reversed. Currently, DoD responds to civil emergencies via the Director of Military Support who is subordinate to the Army Chief of Staff. Although this is the foundation that DoD will build upon, Dr. Hamre said that the need exists to establish a joint task force for the type of long term, detailed contingency planning that a domestic crisis requires. Over the next several months, a plan for this joint task force will be studied and recommended to the President.

In response to questions, Dr. Hamre, clarified that DoD is always the second responder, not the first responder in homeland defense. Dr. Hamre believes that a logical dividing line for determining whether DoD involvement is appropriate, as opposed to other federal resources, is whether the emergency requires mobilizing assets. If so, then it is probably DoD's role. If not, then it is likely another federal agency's responsibility. DoD is the only federal agency that can mobilize a large number of personnel and assets quickly. Dr. Hamre said that DoD is developing a network which will make available various types of emergency response equipment for purchase by local law enforcement and emergency response services.

Dr. Hamre concluded by observing that the nature of the end of the 20th century is such that there are materials that could fall into in the hands of a few which would have catastrophic results for many. Such catastrophic terrorism may be chemical, biological, or nuclear. Thus, a very small number of people could make war on the United States. Such acts may cross the line between terrorism and warfare, and DoD is actively preparing for its role in the federal government's mission of homeland defense.

Bill Conner is a former Navy intelligence officer who is now an attorney in private practice in Virginia.

Cindy Cohn on *Bernstein* . . .

Continued from page 3

academic, scientific or nonmilitary commercial purposes rather than for any purpose intended to hurt U.S. national security. On May 6, 1999, the 9th Circuit Court of Appeals agreed that the licensing scheme, on its face, is unconstitutional for failing to contain the necessary procedural safeguards to ensure that an agency does not act in a discretionary manner to prevent the publication of protected expression. The case is expected to be appealed by the government to the U.S. Supreme Court.

So how did a nice girl from Iowa end up challenging the U.S. government's encryption regulations and, at least so far, winning? In 1990, I was a young attorney learning the ropes of a general civil litigation practice. At the same time, I was trying to continue my work in international human rights. I had spent the year before as an intern at the U.N. Centre for Human Rights in Geneva, Switzerland. During my time at the U.N. it became clear that one of the greatest impediments to the realization of human rights and democracy worldwide was the difficulty in getting solid, verifiable information about abuses out of repressive regions of the world. All too often those who tried were later threatened, arrested or disappeared.

Upon my return to the United States, I met a number of computer programmers who were using the Internet. One of them was John Gilmore. I learned from them the great possibilities of this new network of networks to seamlessly and cheaply link individuals, corporations and organizations around the world. Along with opportunities for commerce, friendship and family relationships, we began discussing the political and legal possibilities the Internet would create. While most people I know learned how to use the Internet simply to communicate with their loved ones living far away than for any other single reason, I saw a tremendous opportunity for human rights and democracy activists to work together on the Internet to put pressure on the repressive regimes of the world. Finally, information could flow easily and privately out of repressed areas to the rest of the world. I also saw how the Internet could help with political organizing here at home.

Then in 1994, John asked me if I would help with a lawsuit the Electronic Frontier Foundation was considering. He told me about a mathematics doctoral student at U.C. Berkeley who had written a computer program that did cryptography. This student, Dan Bernstein, wanted to publish his program on the Internet in a Usenet newsgroup forum called "sci.crypt" where such scientific exchanges were common. The government told Dan that his encryption product was too strong to receive an export license and that if he posted his computer program to the Internet without a license he would go to jail as an arms dealer.

Dan was also told a number of other things that demonstrated the irrational discretion granted by the scheme. For instance, he was told that he could not publish even a description of his program written in English with mathematical equations. He was also told that he could go to jail for putting his program in a U.S. library where foreigners might see it. After we sued, and the lawyers began looking over the shoulders of the agency, the government backed down from those assertions.

Continued on page 9

LtCol Williamson on Cyberdefense . . .

Continued from page 2

scope of what providers can monitor and when they can turn over information to law enforcement or is that issue better resolved in a lawsuit by a user who felt a provider went too far?

Other questions affect counterintelligence. Most intelligence oversight rules were written for a different era. In the past, foreign agents generally had to be physically present in the United States to carry on their craft. They risked discovery while using a miniature camera to photograph hundreds of pages. Their only electronic cloak was the telephone. Today, foreign agents can grab data greater in volume than the Encyclopedia Britannica in seconds. They can hide in another country behind spoofed Internet communication protocols that allow them to anonymously jump through several countries before hitting a U.S. computer. If detected, they can instantly disappear and use different tools through different routes. In addition, the difference between a computer program used for espionage and a program used for attack can be just a few lines of code. A foreign agents' new agility means counterintelligence operators need to be able to react quickly, but current oversight rules use relatively slow processes designed for times when information did not move at the speed of light. How can rules be structured to scrupulously protect the legitimate privacy of U.S. persons while also providing sufficient flexibility and speed to effectively respond?

These are just a few of the questions the JTF-CND and its partners face as servants of the U.S. public. Tough questions will need to be answered for the U.S. military to fulfill its constitutional responsibility to help "insure domestic tranquility [and] provide for the common defence." The JTF-CND with its partners in DoD and federal law enforcement intend to face the challenge head on.

LtCol Williamson is the Staff Judge Advocate for DoD's Joint Task Force for Computer Network Defense.

LtCol Luzwick on the Value of Information . . .

Continued from page 1

here means data, information, knowledge, and wisdom—the classic hierarchy. No doubt horrific to purists, there is no one good word to describe all four concepts together. All four exist within the corporation. Rather than argue about definitions and which is more important, the issue is how to value the intangible essence of information, be it data, information, knowledge, or wisdom. At any given time, one could be of greater value than the others. The tacit knowledge of employees is the most difficult resource to quantify and value.

Information infrastructure is the media within which we store, process, and transmit information. Examples are people, computers, fiber optic cable, lasers, telephones, and satellites. Examples of information-based processes are the established ways to obtain and exchange information. This includes people to people (*e.g.*, telephone conversations and office meetings), electronic commerce/electronic data interchange (EC/EDI), data mining, batch processing, and surfing the Web.

Breakdowns in the IE

Bad things happen, such as floods, hurricanes, and earthquakes; power surges and sags; and fires. Disgruntled employees can steal, manipulate, or destroy information. Crackers work their way through the electronic sieve of protection mechanisms (*e.g.*, firewalls and intrusion detection devices) into information assets.

PriceWaterhouseCoopers (PWC), the Computer Security Institute (CSI), the FBI, and others have conducted surveys asking participants if they experienced information technology (IT) breaches. Thirty-three to 45 per cent replied they were attacked and suffered monetary losses; some losses were quite large. The number saying they were attacked is no doubt higher. Many attacks are sophisticated and not readily detected. Companies are reluctant to report computer crimes because of potential shareholder law suits and customer loss of confidence and leaving for the competition.

Sound disaster recovery and contingency operating plans are essential. For every minute information systems are not up and fully running, revenues, profits, and shareholder value are being lost. The last thing a general counsel needs is a law suit from unhappy shareholders who are suing for millions because the corporation did not follow best practices to protect information. One problem is that commercial off the shelf (COTS) hardware and software is very difficult to protect. Another concern is firewalls, intrusion detection devices, and passwords are not enough. The state of the art in information assurance (IA) is against script kiddies and moderately skilled hackers. What about the competition, drug cartels, and hostile nation states who are significantly better funded? There isn't a firewall or intrusion detection device on the market which cannot be penetrated or bypassed. Password dictionaries can cover almost any entire language, and there are very specific dictionaries (*e.g.*, sports, Star Trek, or historic dates and events).

Value of Information

The corporation must take proactive measures to protect business operations and the bottom line. The corporation could self-insure – in other words eat a loss. Such a decision needs to be made in the presence of hard facts, not a gut feeling. Does the corporation and its individual business units know how much profit they make per year? Per quarter? Per month? Per day? Per hour? Per minute? Is the information protected? How do you know the information has not been stolen or altered? If transactions at Citibank cannot be accomplished, tens of millions of dollars of business can be lost, and that doesn't count the ill will of customers and permanent loss of future business to competitors.

How does a corporation know what information to acquire, retain, protect, and dispose? Laws and practices cover some, product line and consumer base others. What information is more valuable? It depends on the time and context sensitivities of the situation. Figure 1 is a three dimensional approach for determining the perceived value of information. The corporation's business units produce information elements. At any given time, it's possible to determine the importance of specific information. In the absence of national accounting standards for information as a tangible asset, qualitative approaches are necessary.

From a contextual perspective, the information is of either tactical, operational, or strategic nature. From a time perspective, the information is either routine, important, or critical. Keeping the categories to a small number is essential, otherwise subjectivity will creep in and result in a rating that is either under- or overinflated. At any given time, selecting an information element, its contextual perspective, and its time perspective will result in the perceived value of that information element. The way to differentiate between identical ratings is to add a weighting to the information elements. That unique information in time and context will then be rated relative to other information elements. Does this produce a tangible dollar figure? No. Does it help value intangibles? Absolutely. Can there be more than one perceived value at the same time? Possibly, when two or more people view the contextual and time perspectives differently. A policy can be written to achieve common understanding.

A valuation of information would help prosecutors in computer crime cases. The jury must be convinced there was a loss. What is information in a database worth? A simple approach is it took people (their compensation) and IT assets to acquire, process, store, and maintain. Is there a competitive or national security advantage? What's the cost to replace the information, and the cost of lost business/profits or national security?

Here's an example of perceived value. The Department of Defense sends a roll-on/roll-off (RORO) ship with 100 M1A1 Abrams main battle tanks to South Korea. The ship encounters bad weather in the North Pacific, suffers damage from mechanical problems and cargo which became unsecured, takes on water, and sinks. The nation bemoans the loss of life, Military Sea Lift Command calculates sealift shortfall workarounds, and Materiel Command orders more tanks. The value of the tanks, ship, and loss of life can be accurately calculated by traditional accounting methods. Change the scenario. North Korean actions indicate probable conflict. The United States wishes to show its resolve and support for an ally, so it sends a RORO with 100 M1A1s to meet activated Army and Marine Corps Reservists airlifted to South Korea. The ship sinks. What is the value of the tanks? The perceived value is definitely higher than the accounting value. What is the value of the information the ship sunk to the North Koreans?

Precision is required to derive the perceived value of information because business decisions to focus finite resources on products and services will be based on those perceptions. How granular is the information? How much will it cost to acquire more information? What are the costs of an information-based process? Have performance measures of effectiveness (MOEs) for information been developed (*e.g.*, leading indicators and goals such as expected sales or reduced development time)? Can incremental change and rate of change toward those goals be quantified and measured against indicators such as the corporation's or industry's last quarter's and year's sales, market share, and profits? What are information development and reuse costs? What is the perishability of the information? What is the individual, regional, and enterprise-wide effect of the information? Have unique MOEs been developed, like return on time? From which budget will the money come? What are the trade-offs? Could better return be achieved elsewhere? What extra business will be generated?

Whether or not information is a tangible or intangible asset, the fact remains the Internet, intranets, extranets, virtual private networks, and electronic commerce all exist to do one thing: move information. Those corporations that leverage information the most effectively will lead their industries. Wal-Mart is a prime example.

Multi-Dimensional Approach for Determining the Perceived Value of Information

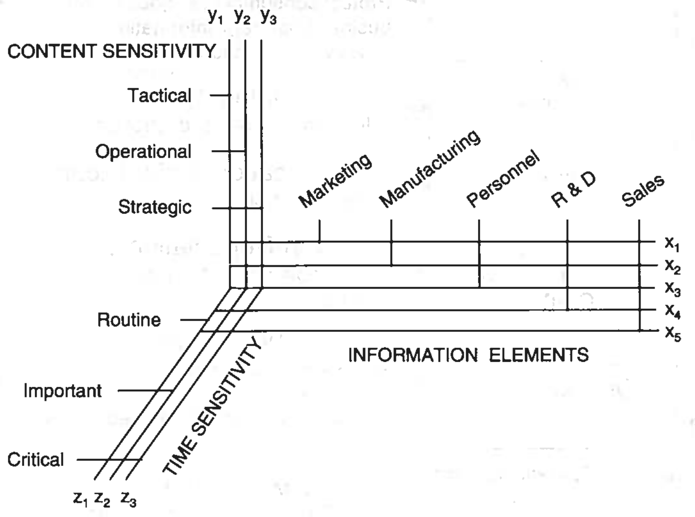

Figure 1

So how does your corporation or law firm value information? Should all information be equally protected? Some information is more valuable than others. Protection measures need to be added as the value of the information increases. How much should a corporation spend to protect its information with firewalls, shielding, intrusion detection devices, personnel checks, motion sensors, encryption, training, anti-virus software, and so on?

Protecting the Information Environment

The electronic genie is out of the bottle and cannot be put back in. Malicious attacks can be mounted, either externally or internally, to steal, alter, or destroy information, disrupt or destroy information infrastructure, and to disrupt information-based processes. A rigorous approach needs to be used to determine a rational laydown of IA products and services, which will be tailored for each corporation. Figure 2 depicts a process to determine a rational laydown of IA mechanisms. Leading it off are validated requirements. A streamlined process to request, analyze, prioritize, and fund them should be in place.

The analysis is based on the parameters developed. The example in the model uses three, but many more ought to be employed. System administrators should know the vulnerabilities of their networks, systems, and applications. Threats can be identified by the Computer Emergency Response Team Coordination Center (CERT\CC) at Carnegie-Mellon University, the National Infrastructure Protection Center (NIPC), IA companies, and others. There is not a one-to-one relationship between threat and vulnerability. The intersection of the two is risk, and, assuming consequence management indicates the need, that's what the corporation needs to protect against.

Another parameter is value. The cost to obtain and replace information can be calculated. The corporation's leading and lagging indicators and MOEs can be used to determine profits. Knowing profits and costs can lead to questions like "What is the value of not having the information?"

The third parameter uses the contextual and time perspectives of the perceived value of information to determine the effect on operations.

Risk management is important, because there isn't enough time or money to eliminate risk. People say, "Well, that's an 80 percent solution." Eighty percent of what?

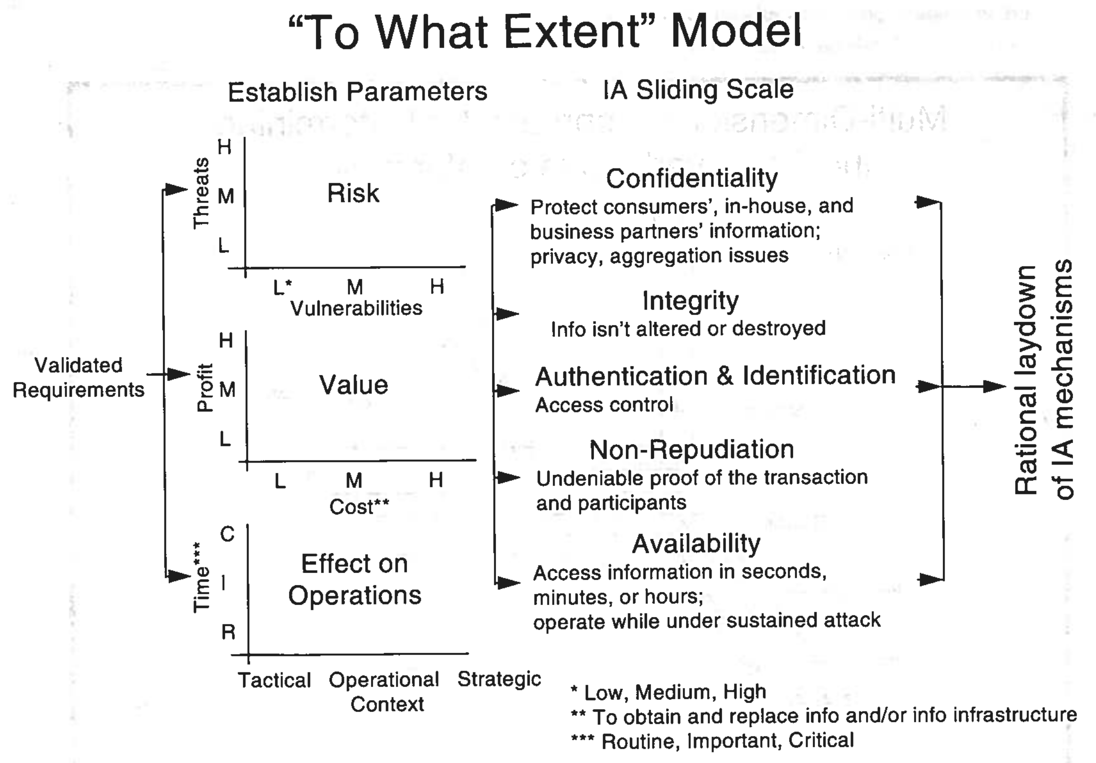
"To What Extent" Model
Establish Parameters
IA Sliding Scale
Validated Requirements
Threats
H
M
L
Risk
L*
M
H
Vulnerabilities
Profit
H
M
L
Value
L
M
H
Cost**
Time***
C
I
R
Effect on Operations
Tactical
Operational
Strategic
Context
Confidentiality
Protect consumers', in-house, and business partners' information; privacy, aggregation issues
Integrity
Info isn't altered or destroyed
Authentication & Identification
Access control
Non-Repudiation
Undeniable proof of the transaction and participants
Availability
Access information in seconds, minutes, or hours; operate while under sustained attack
Rational laydown of IA mechanisms
* Low, Medium, High
** To obtain and replace info and/or info infrastructure
*** Routine, Important, Critical

Figure 2

Configuration management records are not accurate, so there is no complete and reliable baseline of fielded IE products and services. There's no real-time auto-discovery or mapping of the IE to keep track of dynamic changes in hardware, software, information, and physical assets, thus preventing just-in-time IT and IA insertion and abandonment strategies. There's no system for identification of friend or foe on the network such as IFF/SIF (Identification Friend or Foe/Strategic Identification Feature), which the military uses for airspace battle management. Finally, no accounting standards for the value of information and no rigorous, quantitative cost benefit analyses or trade-off analyses and MOE result in subjective conclusions.

The IA sliding scale is applied to all the parameters. Confidentiality, integrity, authentication and identification, non-repudiation, and availability are, in this example, applied to risk, value, and effect on operations. The summation of these variables is used to determine the rational laydown of IA mechanisms.

Suggestions for Continued Study

The risk of information loss is real. Corporations need to be proactive in protecting their information-based assets. Even the most acknowledged experts (*e.g.*, Karl Erik Sveiby) have stated placing hard figures on intellectual assets is not meaningful. That may be true because the time and contextual perspectives can shift frequently, thereby altering the perceived value, but it also can lead to efficient resource allocation. Still, the traditional accounting methods are insufficient, as shown by Paul Strassmann. Aggregated information also needs to be considered; standard data labeling and automated reclassification of information would be useful. Rigorous MOEs need to be developed. A crack team of accounting, operations research, industrial psychology, statistics, and economics subject matter experts should be able to develop sound methods, formulae, and MOE. With values derived through rigorous methods, information can then be carried on the books as an asset.

LtCol Luzwick serves as the Military Assistant to the Principal Deputy Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. ABA

Cindy Cohn on *Bernstein* . . .

Continued from page 5

My initial reaction to the government's position was to ask something like, "what does the program do, blow up the Pentagon?" "No," John Gilmore replied, "it just keeps messages secret." He explained that cryptography was the technology that allows people to have envelopes in cyberspace. Without it, e-mail is just like a postcard, open for anyone to read in transit or when stored. "Sounds like a First Amendment problem to me." From there we spent over a year researching the legal issues and the regulations, gathering evidence and planning. We then filed the lawsuit and have spent the last four years steadily winning the case, with the likely ending point at the Supreme Court.

I took this case and have pursued it in part because it is clear that without cryptography, not only will the Internet's promise to industry be unfulfilled, but its promise to those struggling for basic human rights, democracy and freedom will also be left behind. If the repressive governments, criminals or political parties can read the e-mails of those who oppose them, then quite literally, lives and democracies are in danger. The Watergate scandal in the United States demonstrates the ongoing temptation for political rivals to learn each other's strategies even in a more healthy democracy. And, while I would like to believe that key "recovery" (or whatever euphemism is currently in vogue) could be deployed in such a way as to ensure that only good governments, good individuals, and good politicians could read e-mails of others, the work of the world's most preeminent cryptographers agree that this isn't possible.[4] And, their position is confirmed by simple common sense. No system can separate legitimate users from illegitimate ones. Or, as a friend of mine observed, you cannot build a "good-cop" shaped door into a house and not also let bad cops and bad guys in.

So I still don't quite know why the U.S. government considers me such a threat. All I'm trying to do is bring a little sanity to this issue – first, in the form of a regulatory scheme that meets the U.S. Constitutional requirements, and second through enabling the wide deployment of a technology that may help to make the world a little more just.

[1] Steven Levy, *Courting a Crypto Win*, NEWSWEEK, May 17, 1999, at 85.

[2] Bernstein v. Dept. of Justice, 945 F. Supp. 1279, 1296 n.10 (1997).

[3] Co-counsel on the case are Lien Tien of Berkeley, CA; Shari Steele of the Electronic Frontier Foundation; Ed Ross of Steefel, Levitt and Weiss of San Francisco, CA; Elizabeth Pritzker and James Wheaton of the First Amendment Project of Oakland, CA; Robert Corn-Revere of Hogan & Hartson of Washington, D.C.; and, Sheri Byrne of Thelen, Reid and Priest of San Francisco, CA.

[4] Abelson, Anderson, Bellorin, Benaloh, Blaze, Diffie, Gilmore, Neumann, Rivest, Schiller & Schneier, *The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption,* Center for Democracy & Technology, May 1997.

Cindy Cohn is lead counsel on Bernstein v. Department of Justice, et al. ABA

Chairman Rudman on Security at DoE . . .

Continued from page 3

The most significant issue the Chairman focused on was the presence of "arrogance" among the laboratory staff within DoE. While he recognized that these nuclear physicists and scientists were some of the most intelligent in the world, Chairman Rudman stated that because they are so bright they do not appreciate being told how to do their own jobs. This often results in the laboratory staff ignoring the requests and orders of the upper-level staff. Chairman Rudman noted that this arrogance significantly contributes to the lack of organization and dialogue between the laboratories and senior officials.

In his analysis of the current security problem, Chairman Rudman assured the HASC that the physical security of the labs, *i.e.*, the guns, gates, and guards, is strong, while emphasizing that the major problem is the arrogance that exists within DoE. Chairman Rudman elaborated on the "arrogance" issue by referring to DoE as "leaderless" and that its staffing is "dysfunctional" because no one listens to orders and because there is no authority. While the Chairman of the Committee, Mr. Spense, admitted that fundamental change is necessary and long overdue, others such as Mr. Skelton seemed to be concerned by Chairman Rudman's statements that DoE cannot change itself.

The central points that Chairman Rudman stressed in advocating the creation of a semiautonomous agency within DoE was the importance of accountability, authority, and the field personnel having more jurisdiction and a stronger working relationship with upper-level officials within the department. He stated that he has great respect for Secretary Richardson and his staff, which consists of highly qualified individuals, but that they are working in a "dysfunctional" organization.

John Harrelson is a summer intern with the Standing Committee and a junior at Trinity College. ABA

On August 5, 1999, the HASC issued a press release announcing that the House and Senate conference committee on the National Defense Authorization Act for FY 2000 reached an agreement on legislation to reorganize DoE to streamline management and strengthen counterintelligence and security. This legislation marks the first major reorganization of DoE since its creation two decades ago. It essentially implements the recommendations of the PFIAB report by creating a semiautonomous agency - the National Nuclear Security Administration (NNSA) - within DoE. The head of the NNSA will work for and report directly to the Secretary of Energy. – Editor. ABA

Privacy in the 21st Century

by Andy Johnston and Jeehye Yun

> *That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been necessary from time to time to define anew the exact nature and extent of such protection.*
>
> *Samuel D. Warren and Louis D. Bandeis*[1]

The following article examines the privacy concerns raised in an 1890 Harvard Law Review article by Warren and Brandeis. They asserted a "right" to control personal information implicit in common law in response to the concerns raised by the information technology of the late 19th century.

We consider the changes in concepts such as "publication" between the late 19th and 20th centuries, in light of the changes in information technology. We then examine the implications of current technologies for the control and disclosure of personal information and explore the inherent conflict between the benefits of a vast, universally available and rapidly changing electronic medium and the control of personal information.

More than a century ago, Warren and Brandeis proposed that the individual's right to control the nature and extent of the divulgence of unpublished personal information was implied by common law. They argued that this privacy right was distinct from the copyright law that governed the use of the information after publication. The distinction was emphasized because the authors considered the technological advancements in 19th century information technology as a significant threat to the "right to be let alone."

In 1890, the ability to communicate and publish information through a variety of mass outlets (such as newspapers) in a day or two raised serious concerns about privacy issues. In 1999, anyone in the United States who can operate a keyboard has the potential to make any information available around the world in fractions of a second. More ominously, we are highly dependent on information technology for education, entertainment, finance and personal convenience. The providers of these services can store and piece together dozens or hundreds of very small bits of information divulged daily by individuals into extensive individual and group profiles – often without the individual being aware that anything has been divulged at all.

Continued on page 12

The E-Commerce Weak Link

by Greg Hoglund

While encryption protects transactions en route, the e-commerce server remains vulnerable to security attacks.

Transactions are the crux of e-commerce. And achieving secure transactions is the impetus for the growing e-commerce security market. Yet much of today's perceived e-commerce security is anything but secure. Encryption technologies protect data along much of a transaction's electronic journey, but *not* after the data, perhaps your own credit card number, reaches its destination server at the e-commerce site. With alarming frequency, these very servers, which hold your valuable credit card data, are under attack from sophisticated hackers.

The fact is, today's e-commerce sites are only as secure as their weakest link, and this is often a commercial server where valuable information is stored unencrypted. Making these links secure will involve both technology and a set of stronger standards and laws governing e-commerce security.

Limited Security

Encryption is one of the most powerful tools used to secure communications, but there are limits to its effectiveness. Any e-commerce solution must communicate securely with customers. This is usually achieved with Secure Sockets Layer (SSL), a technology capable of encrypting communications between your computer and the server.

While you should never participate in e-commerce activity without encryption, the fact that you are using SSL does not protect you from hackers. SSL cannot ensure the safety of data once it arrives at its destination and is stored unencrypted. While SSL can prevent a hacker from "sniffing" your transaction en route between your computer and the server, it cannot stop a hacker from breaking into the server itself, the weak link.

The reality is that it is a fairly simple task for hackers to break into an e-commerce server. Even if you think a particular e-commerce site is safe, it probably isn't. Many software vendors will tell you their server software is secure, and even if you have installed all of their security patches on your server, it is still not completely safe.

A recent case clearly demonstrates the frailty of server security. A serious remote buffer overflow was discovered in the latest version of IIS – a web server. Estimates are that over 90 percent of the IIS servers on the Internet are vulnerable to this bug, which allows hackers to install any software of their choosing onto the server. They can install Back Orifice or other root-kits into almost any IIS server, and many e-commerce sites use IIS as their web server. Even with SSL, credit card information is not protected once a hacker breaks into the server and steals the database. Not protecting confidential information such as credit card numbers, opens these e-commerce sites up to damaged reputations, angry customers, and lawsuits.

Guarding Against the Known

Host-based security is an absolute requirement for secure e-commerce, and tools such as an intrusion-detection system (IDS) can provide critical notification of an attack. There are two types of IDS: signature-based and anomaly-based.

Signature-based detection presumes prior knowledge of an attacker's method's known as a "signature." The signature contains the nature of the attack, the exploit used and the delivery mechanism, all of which must be known in advance for network based intrusion detection to work.

To obtain this knowledge, the e-commerce provider must monitor public forums and keep abreast of the computer underground's latest exploits. But there are always exploits that are not publicly known or are so fresh that the public is unaware of them. The effectiveness of the signature-based IDS is weakened accordingly.

Weakened, but not useless. There is an entire class of hackers called "script kiddies" who do not develop their own exploits, but download and use publicly available "scripts" that perform well-known exploits for them. Because their exploit methods are documented, a signature-based IDS can protect against them.

But there is another, far more sophisticated class of hackers who discover vulnerabilities on their own. They write the scripts the "script kiddies" use, and they are the real threat to your security and corporate assets.

Detecting System Anomalies

Anomaly-based detection, on the other hand, is particularly powerful because it does not require prior knowledge of an exploit to detect it. Instead, an anomaly-based IDS utilizes known facts about your system. It knows which system calls are being made by your software and it knows which files have been recently altered. It collects and monitors this data. An anomaly-based IDS uses the premise that any attack – no matter how complex – will alter your system in some way. When it detects any deviation from "normal," it alerts the system administrator to investigate the event.

Continued on page 13

Johnston and Yun on Privacy . . .

Continued from page 10

Assuming that people *do* have some right to the disposition of personal information, this article illustrates some of the ways in which information services, operating "transparently" to the user, acquire and collate such data to an extent not usually realized by the public. The term "divulge" is used here to describe the conscious transmission of personal information to another party without the intent of making it available to the general public. The terms "disclose" and "publish" are used to describe the publication of information in the usual sense.

Privacy vs. Commerce

A century ago, information had value if people wanted to pay to read about it. At the dawn of the 21st century, information itself is a commodity. The commercial interest in information collection and analysis is enormous. Since the value of information increases with the ability to store and analyze it with increasing certainty and detail, this commercial interest will continue to increase with advances in the technology. At the same time, the technology allows any individual to become a global information provider with negligible cost and effort.

Behind the Screen

In order to illustrate some aspects of the issue, we describe four ways in which information technology enables service providers to exploit information collection to a far greater extent than a user might expect. Each example involves routine and legal information gathering. Although the information collected from these methods are not necessarily private and in many cases necessary for daily operations, the sum of the collected information allows one to glean unintended private information on the individuals or group of individuals, without their awareness that such information may be gathered. We categorize and define the four gathering methods as:

Passive logging – the collection of information that is of no benefit to the user and usually unrelated to the service being provided, but is common maintenance practice on most computers.

Active logging – the collection of information that is of specific interest to the service provider which is often used to provide more convenient user interactions.

Program mishandling – poor design or bad programming which causes unintended side effects.

Quid pro quo – voluntarily divulged personal information without a clear understanding by the user of the potential scope of its use. In return, the user gains access to goods or services from the provider.

Passive Logging

Computers log internal activities with associated start, duration and end times. Such logging is essential for maintenance and trouble-shooting. The same logs can often be used to glean information about individual usage. An example for this case has actually occurred. A system manager noticed that his logs recorded numerous Internet connections from a competitor called ABC, Inc. to his company, XYZ, Inc. He also noticed records of many e-mail transactions between a high ranking officer of his company and an executive officer from ABC, Inc. Based upon his observations, he guessed that his company was going to be bought out buy a competitor before it was public knowledge.

Active Logging

In addition to the routine logs that any computer system maintains, many Internet services use methods to collect information for purely commercial use. Cookies are a classic example. Cookies are records that web sites store and later read from the user's computer. The information usually involves the patterns of the individual's use of the web site. Web servers are now able to customize information to the individual by using the cookies to target advertising and services to personal preferences. Although this is a great convenience, the web service provider "profiles" the user without the individual being aware that this type of information is being recorded. This type of operation allows customization of sites like <www.my.yahoo.com>.

Program Mishandling

An early electronic service provider distributed a program that a user could use to communicate with the provider. A user of the services would be presented with advertisements for various products. If the user asked for further information about the product advertised, that selection would be recorded in a storage area set aside by the communication software in the user's computer. At the end of the session, the stored information was written to the user's disk. At the beginning of the next session, that particular information would be sent to the service provider who used it to target advertisements to the individual's interests. Unfortunately, when the interface program set aside a storage area, it failed to clear out the contents that other programs stored in that location.

Since the interface program was not careful, it might include personal correspondence, tax information and other data resident on the individual's computer hard drive along with the intended consumer choice data. There was no reason to believe that this information was even seen by the provider, let alone exploited in any fashion. However, the poor design of the interface program raised serious concerns among many subscribers, including one of the authors.

Quid Pro Quo

A common example of voluntarily divulging information is in the super-market's use of magnetic cards that contain private information. These cards are offered "free" in return for filling out a form with personal information. The cards are then presented at the checkout line to provide discounts to the shopper. This mechanism allows the store to track individual preferences such as type of products purchased, price, time and location of the transaction. The supermarket can process this information for marketing purposes. The "free" cards are actually part of a *quid pro quo* in which the shopper exchanges personal information to get the card which can subsequently be leveraged with further information about the time, place and nature of the shopper's purchasing habits.

Conclusions

No malicious intent underlies the technologies described above. In most cases, the technology provides a benefit to both parties in a transaction. However, the consumer who uses the service usually doesn't understand the full value and scope of their contribution in that transaction. The problem of privacy and security is a broad and complex web of technologies, people, policies and law. We must understand the nature of this new medium if we are to exploit it fairly. No approach will be effective unless it is implemented within the framework of a coherent body of law governing the access and use of personal information.

A variety of encryption and authentication technologies are available which could be deployed within such a framework to partially address the privacy issue. However, without a broad understanding of the implications of information technology across many segments of society, no consensus can be reached upon which a framework can be built. More fundamentally, society must be prepared to determine whether and to what extent personal privacy should be considered a "right" in the face of the continuing advances in information technology. These questions were raised more than a century ago. We must now begin to address them as a society.

[1] Samuel D. Warren and Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

Andy Johnston is a Security Specialist and Jeehye Yun is a Team Leader at QUATEAMS, LLC, a Maryland-based full-service technology company specializing in end-to-end solutions. ABA

Hoglund on E-Commerce . . .

Continued from page 11

The second form of anomaly detection involves measuring the communication channels on the network. Normal and regular communications between machines are logged, and any deviation from this pattern can be flagged for further investigation. While this doesn't apply to something like a public web server, it is highly effective on internal networks and attacks carried out by people within the company.

The third form of anomaly-based IDS monitors your software's system calls. Again, deviant patterns of system calls may indicate that a buffer-overflow attack has been executed or that strange arguments have been passed to the software – events usually due to software errors or some form of misuse.

Standards and Solutions

Much of the effort to resolve security gaps will come in the form of standards or laws governing e-commerce. While there are many standards committees directly associated with the Internet, they are able to define standards but not to enforce them. This is unacceptable in particular to the banking and insurance sectors – two industries that need to measure and mitigate risk. For a glimpse into the future of e-commerce security, consider that insurance companies now offer coverage for data-loss and security breaches. Increasingly, insurance companies will not insure an e-commerce solution unless you can prove that you followed sound coding practices. If you cannot prove your software is free of buffer overflows, for example, the insurance will cost considerably more.

Additionally, the legal ramifications for ignoring security will grow. Witness the preparation for Y2K readiness and the proposal of legislation in Congress that would limit liability. The bottom line is that as e-commerce explodes, organizations will have to take security precautions and obtain insurance to guard against lawsuits from investors, business partners and employees to compete effectively. Since security enables the future of e-commerce, more vendors are ensuring security is built into their hardware and many software vendors are going the extra mile to assure the security of their applications. The public, the legal community, and those organizations that provide secure e-commerce will ultimately win the war and set the standards for the future.

Greg Hoglund is a Senior Researcher for Product Development at TRIPWIRE SECURITY SYSTEMS, INC., an Oregon-based software development company specializing in system security and policy compliance applications. ABA

Exploits: How Hackers Hack

by David Tubbs

We are bombarded daily with a series of rather frightening headlines and statistics. It is estimated that computer intrusions will cost private industry more than $20 billion this year. The damage caused by three recent virus attacks – Melissa, Chernobyl, and ExploreZip – has already exceeded $2.5 billion. The Cox Committee and PFIAB investigations strongly criticized the Department of Energy for lax computer security which likely resulted in the loss of sensitive nuclear weapons secrets. The White House announced that Russia may have used computers to steal some of our most sensitive military secrets – to include weapons guidance systems and naval intelligence codes.

In sharp contrast, the media tells us very little about *why* our computer systems are so vulnerable and *how* hackers are able to compromise our computer systems – and until we all have a better understanding of how hackers hack, we will remain a vulnerable society. There are many information gathering techniques and technical exploits that allow non-authorized personnel to gain access to proprietary, sensitive, and classified information systems. This article is intended to provide a brief overview of how a hacker gathers information necessary to compromise your computer and an overview of the most common technical exploits.

Information Gathering Techniques

Perhaps the greatest vulnerability of any computer system is the human element. Most people still use family names or other easy-to-remember passwords, or use more difficult passwords but write them down in an easily accessible location near the computer. While some hackers may attack only by the Internet, a sophisticated and persistent threat dedicated to compromising your computer system will attempt to surveil your system physically and electronically. Information gathered from conventional forms of surveillance and analysis is very effective in determining which type of intrusion will be the most successful. Insiders, of course, are the greatest threat to any computer system – they have authorized access.

If physical access is obtained, both information gathering and actual system compromise are significantly easier. Hackers may gain physical access to your company's computers through employment as a janitor or temporary secretary – or they may simply be your next client who is left alone near a computer momentarily. Once they gain physical access to your computer, a hacker can immediately download or corrupt your information, or install sniffer software to collect information. A sniffer is a program that runs in the background of the target machine, collecting information, such as passwords or credit card numbers, during normal operations. It generally requires a return visit to retrieve the collected information, but these programs may be quite small and difficult to detect.

Physical access to your offices also allows hackers to plant conventional recording devices that will collect your information. For example, an audio recording of an impact printer may allow the printed characters to be recreated. Similarly, devices planted in nearby offices can record your entire document when it is transmitted by electronic bursts to your laser printer. Hackers may also learn relevant information by simply collecting your trash from the curbside.

Finally, hackers may use social engineering techniques to compromise your computer system. Social engineering takes advantage of the fact that most people endeavor to be honest and helpful. Unless an enterprise has taken steps to educate it's user base to the vulnerabilities represented by releasing seemingly innocuous information, social engineering gathers attack design information very effectively. Typically, a perpetrator will call on an overworked employee, either in person or by telephone, invent a plausible need-to-know excuse, and ask for relevant information. They may also offer a free magazine subscription in return for you answering a few survey questions. Or, they may actually send you free software (which contains malicious code) for you to try out on your computer. A trained practitioner in social engineering will usually obtain at least unclassified system details, but often passwords and sensitive information can also be obtained.

Seemingly innocuous information can also be very useful, leading to ease of access through system configuration details, personnel information, or guessed passwords. Public records, such as the company's web site, or public business relationships, allow a significant amount of information to be collated for use against the target. This information may point to a vulnerable electronic interface or an insecure business partner with full access. These elements of friendly information (EFI) may be insignificant in isolation, but can generate considerable weight when collected and pieced together.

Technical Exploits

All software is flawed. Software programs may have hundreds of thousands of lines of code, and a predictable number of these lines of code will be flawed. A number of these flawed lines of code, which very likely do not interfere with the intended operation of the software, will be useful for nefarious purposes, and the hacker community has proven extremely adept at finding and exploiting these flaws to gain unauthorized access to computer systems. While security patches are constantly developed to cover known flaws, market pressure to quickly add new features and interoperability prevents adequate security testing before sale.

Hackers have the innate advantage, and they work together. The collegial, intellectual nature of the hacker community and of the Internet in general guarantees that many hundreds of hours are spent by malicious individuals to develop and improve existing, published exploits. Web sites, chat rooms, private electronic bulletin board systems, and other services which cater to the malicious hacker number in the thousands. Hundreds of pre-designed exploits are categorically listed by operating system and software application on public electronic forums (*e.g.*, see www.rootshell.com). Many more exploits exist or are in development in private venues, though private exploits are published coincident with news of the first major attack using the exploit. The remainder of this section is a description of the most common technical exploits and malicious attacks.

Buffer Overflows. Buffer overflows are a common vulnerability in all software. They require specific knowledge of the targeted operating system, but are powerful in that they allow arbitrary code (*i.e.*, malicious programs) to be executed. Buffer overflows occur when data written to a pre-sized memory buffer exceeds the buffer's allocated space. The excess data then overwrites other memory areas. This can occur when a user response is longer than the software designer expected. Intentional buffer overflows attempt to write the perpetrator's code into the computer's instructions. Implementation of this exploit is routine, however, it must be precisely written, aligned, and sized so that it falls on a specific memory location.

Malformed Data. Malformed data is data in a format that isn't expected by the target. For example, sending a negative value where the programmer assumed a positive value would always be received. The result of a malformed data packet is generally undetermined, although frequently the result is to crash the target, denying service to the target.

Guest Accounts. Guest accounts are common on networking systems, designed, oddly enough, for guests. However, they usually have no real password protection and they allow perpetrators minimal access. This access can then be leveraged into more meaningful access through known exploits or by scanning for an error in the security implementation. Guest accounts are also very useful in the data gathering stage of penetration.

Obsolete User Accounts. Failure to delete user accounts for ex-employees, visitors, or consultants provides access similar to guest accounts. Obsolete user accounts retain the password protection that was in effect when the account was created, but long time lines allow a number of data gathering or password cracking techniques to be employed against them. When an obsolete account is accessed, the privileges accorded to that user are also still in effect and are typically considerably more powerful than those of a guest account.

Phreaking. Phreaking is the compromise of the telephone system. Since these systems are typically computer-based, many of the exploits identified for information systems are applicable to compromising the telephone network. Phreaking is typically employed to support hacking activities by routing attacks through long distance and foreign networks.

Spoofing. Spoofing is an electronic lie, where the header information in a communication is falsified to obtain access. The tools for this exploit are commonly available and easy to use.

Man-in-the-Middle. Man-in-the-middle attacks interrupt an established communication path with an intelligent computer in the middle. The attacking computer then communicates with each terminal as if it were the other terminal. The entire data stream of the communication is thus available and detection is quite difficult.

Standing Committee on Law and National Security

Chair: Elizabeth Rindskopf Parker

Members: E. E. Anderson, Dale E. Bosley,
Willie Curtis, Robert N. Davis, Pamela Jimenez Parizek,
Ann C. Petersen, Michael K. Powell, Suzanne Spaulding, Paul Schott Stevens, Diane P. Wood

Advisory Committee Chair: Richard E. Friedman

ABA Board of Governors Liaison: James E. McDaniel

Staff Director: Holly Stewart McMahon
740 15th St., NW
Washington, D.C. 20005-1009
(202) 662-1035
FAX: (202) 662-1032
E-mail: natsecurity@abanet.org
Web page: <http://www.abanet.org/natsecurity>

Malicious Code. Viruses, worms, trojan horses, time bombs, etc., are code written to infect the host machine and use it as a platform to infect connected machines. The methods of propagation differ widely, as do the effects of an infection.

Denial of Service. Most imperfections in software simply degrade performance. When the degradation is sufficient to halt operations, the exploit is a denial of service. This class of exploit outnumbers all others by a considerable margin.

Connection Between Internal Data and Public Networks. Open connections to the outside world render all perimeter defensive measures moot. Compliance is crucial to defend against this class of exploits, as even when system designers and administrators are careful to control connections to outside networks, individual users will often circumvent the design for operational convenience. Environmental controls are usually wide-open, for example, yet sometimes connected to a computer system.

Network Topology. Often the physical topology of the network hardware and cabling provide physical access to the data stream by tapping the cables or modifying the computers. Typically, wiring closets, wiring ducts, server storage rooms, and attics are unsecure and provide ready physical access.

Interconnectivity at Vulnerable Points. Transmission paths and interconnection nodes are frequently overlooked in security designs.

Lack of Training Leading to Exploitable Systems. User compliance with security procedures is the single largest vulnerability for any information system. User errors or ignorance in security operations produces vulnerabilities at every user access level.

E-Mail Attachments. E-mail programs are gaining the capacity to automatically execute scripts (programs) in an attempt to further consumer convenience. These programs are not limited and the targeted victim is often unaware that they are propagating nefarious scripts, viruses and possibly damage.

Public Network Analysis Tools. These tools map the network (information gathering) and automatically perpetrate known exploits against it. They were originally intended for system designers and administrators, but they work equally well for perpetrators.

Publicly Available Cracking Utilities (password crackers, etc.). These utilities use a wide variety of techniques to take advantage of relatively low-level vulnerabilities, of both the network and the user base. These utilities may simply contain a database of all the words in a dictionary and other combinations commonly used as passwords, or may be a more sophisticated program designed to run all possible number and letter combinations for a given system configuration.

Conclusion

Any computer system can be eventually compromised by a persistent and dedicated threat. This article describes a few hacker techniques – there are many more. Effective security demands constant vigilance by all users, system administrators, and corporate officers, and depends upon an integrated security program that protects against hardware, software, and social engineering attacks. The cornerstone of all computer security programs is situational awareness, training, and education.

David Tubbs is Executive VP and CTO of Talon Technology International, Inc., a California-based computer systems and information security company.

Mark Your Calendars!

Mark your calendars for October 28-29, 1999 when the Standing Committee will present its ninth annual conference on *National Security Law in a Changing World* at the Hotel Washington in the District of Columbia. October's conference will follow the pattern of recent conferences, beginning with a roundtable discussion featuring the senior legal advisers from the major national security departments and agencies. The second panel will include senior attorneys from key Senate and House committees discussing national security issues of concern to the Congress.

While the details of the four panels to follow are still being worked out, issues likely to be addressed include U.S. policy towards the new International Criminal Court, use of force issues involving Kosovo (such as the proper role of Congress and the lawfulness and scope of "humanitarian intervention"), and possibly a look at the Uniform Code of Military Justice (UCMJ) on the occasion of its fiftieth anniversary. As usual, there will also be a dinner program Thursday night and two lunches featuring distinguished speakers. Additional information appears on the Standing Committee's web page (<www.abanet.org/natsecurity/>). – *Professor Robert F. Turner*