Global Information Assurance Certification Paper

Security By Itself May Not Be Enough

An Overview Of The Discipline Of System Survivability

by

John Price

A practical assignment

Submitted for the GIAC Security Essentials Certification (GSEC) program

Version 1.2c

May 10, 2001

Computer Security Defined

Computer security permeates the press these days. Few computer-oriented magazines lack some type of article addressing the topic in each issue. The terms "firewalls," "viruses" and "hackers" have permanently entered our vocabularies. What is computer security? Cheswick and Bellovin (1994) define computer security as "keeping anyone from doing things you do not want them to do to, with, on or from your computers or any peripheral devices." Garfinkle and Spafford (1996) have another view: "A computer is secure if you can depend on it and its software to behave as you expect."

Howard (1996) in his research of Internet security incidents classified computer security as "preventing attackers from achieving objectives through unauthorized use of computers and networks." His taxonomy of computer security attempts to classify a broad range of attacks, vulnerabilities and motives. This classification, although valuable, still does not adequately define the broad category of computer security.

Computer security is more than preventing attackers from accessing systems. It concerns protection of information even when the security of a system is breached. It is also the protection from acts of God such as floods, earthquakes or tornados.

Cheswick and Bellovin (1994) state, "Computer security is not a goal, it is a means toward a goal: information security." This paper does not dispute this statement, but argues that the goal of information security is also not the true end. A restatement of that sentence could be that computer security and even information security is a means to a larger goal: the continuation of computer systems' mission objectives.

Vandenoever (1995), in his Deloitte and Touche business management briefing defines computer security as "the preservation of the continuity, integrity and confidentiality of information resources." In this document, he defines continuity as the "availability of your information and processing resources when, where, and at the level, you require." Integrity is defined as "trustworthiness … Can you trust the information processes and the results it's producing?" Finally, Vandenoever defines confidentiality as "related to two principles- proprietary intellectual property and individual privacy. … The term 'need to know' embodies confidentiality, but it does not cover the entire spectrum of computer security. Privilege control- the rights to create, update, store, transmit and dispose of data- are usually far more important in most organizations."

The state of the practice for computer security identifies confidentiality, integrity and availability as its goals. Yet, stories abound regarding security breaches. Denial of Service attacks, web defacement, credit card number thefts and other attacks occupy a significant amount of news space.

No one will argue that most of the victims could have hardened their systems more against attack. But such "hardening" is becoming more difficult. Business-to-business exchanges over the Internet are increasing. No longer can security professionals defend their network behind walls of bastion hosts. Perimeters are becoming undefined. Not only is business affected, but also our national infrastructure. Linger, et al (2001) state:

> "Major economic sectors including energy, transportation, telecommunications, manufacturing, financial services, health care and education all depend on a vast array of network systems operating on local, national and global scales. This

pervasive societal dependency on networks magnifies the consequences of failure and amplifies the vital importance of ensuring their survivability."

The Internet has opened a tremendously important communications channel, but unfortunately, has changed the paradigm of security practitioners. They find themselves attempting to secure unbounded networks that have no central security administration or control.

Ellison et al (1998) state, "Despite the best efforts of security practitioners, no amount of hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack."

Computer Security- Efficacy

"A secure network does not exist; nor does a secure computer. The only secure computer is one that is unplugged, locked in a secure vault that only one person knows the combination to, and that person died last year. When you move beyond that scenario, you must expect lapses in security." (Eckel, 1996)

"In short, the nature of computing dictates that even hardened systems can and will be broken." (Ellison, et al, 1997)

"The only secure computer is one that's turned off, locked in a safe, and buried 20 feet down in a secret location—and I'm not completely confident of that one either." -- quote from Bruce Schneier to Richard Behar. (Behar, 1997)

The above comments from noted computer security experts do not inspire confidence. Is the state of computer security this dismal? Dennis Hughes, the FBI's senior expert on computer crime, expressed his frustration by saying, "The hackers are driving us nuts. Everyone is getting hacked into. It's out of control." (Behar, 1997)

For each known threat, there seems to be a counter. To protect one's network, it would seem that one only has to apply the appropriate defenses to each listed attack. Why, then, do the traditional approaches to computer security provide only a marginal level of comfort to the computer security professional?

This author has divided the answer to that question into four sections:

1. Computer security tends to be reactive.
2. Systemic components are complex and not fully understood.
3. Information has increased in scope to transcend artificial boundaries.
4. People and political factors compromise computer security.

Computer security tends to be reactive

Administrators and security professionals establish their perimeter. They spend countless hours ensuring they have established protected connections to the Internet, have bolstered authentication to their dial-in systems and have strengthened host security and recoverability. Just when they feel they can simply monitor their systems for intrusion, a notice from CIAC or CERT is published regarding a weakness in their firewall, their communications protocol or even their dial-up hosts. Following recommendations, they download a patch, apply it over a non-business period and then test to ensure no production errors will result from their maintenance effort.

Unfortunately, the weakness may have been in existence for years prior to the notice. Select groups of criminals or information warriors may have been exploiting that weakness in the administrator's organization and gleaned corporate secrets for a long period of time.

The simple truth is criminals; hackers and information warriors specialize in breaking into systems. Administrators typically wear many hats including providing service to users, performing constant maintenance and administration and generally trying to keep large, complex networks from crashing around their users' heads. Perpetrators of computer crimes usually do not suffer from such distractions.

In addition, patches to vulnerabilities may require significant development effort forcing administrators to choose whether to deny users an expected service or continue providing that service with its potential weaknesses.

Similarly, virus protection is almost always reactive. Up to three viruses are created a day, yet the cure for each virus often requires a reverse-engineering effort to discover the signature of the virus before an anti-virus product's database can be updated.

Finally, it is difficult to anticipate from where attacks might come. Often, only after an attack, can the origin of the attack be guarded against. Coffee (1996) states, "It takes a great deal of insight into the mechanical and electronic mechanisms of our information devices to envision the edge conditions that might cause revealing partial failures." Prompting this statement was the discovery that two Israeli cryptographers broke the Data Encryption Standard (DES) encryption keys by applying small amounts of heat and radiation to PC's and smart cards and examined the changes in bit patterns.

Solutions to their methods of attack include the strengthening of cryptographic keys since DES is now considered weak, but the results illustrate the reactive nature of computer security. One cause of this reactive nature is the overall complexity of information technology.

Systemic components are complex and not fully understood

In the 1960s and 1970s, computer systems were encompassed largely in one box. That box, a mainframe, handled the processing for entire organizations. Connecting systems together was a complex, laborious task, but the components were bought and installed usually by a single vendor. Most processing occurred in batch mode, and users typically did not have information at their fingertips. Security could be centrally controlled both physically and logically. Physically, the systems operated in a locked, raised-floor computer facility. Logically, access and authentication existed only on that one platform.

Today, a system administrator must deal with a multi-protocol network, complete with several operating systems and a wealth of applications that span multiple platforms. Programs that used to take kilobytes of hard disk space, now occupy hundreds of megabytes with additional gigabytes of data, and backup and recovery systems must encompass multiple solutions from multiple vendors.

Few administrators have the technical expertise to decipher the myriad low-level structures of the main network protocols. Network operating system vendors either come to the rescue with utilities to assist the administrator or third-party vendors may fill the

breach. Regardless, the administrator must rely on packaged solutions to run today's complex networks.

Few organizations write their own operating system software. In the 1960s and 1970s, that practice was quite common as the operating systems at the time typically lacked critical services. Today, operating systems are extremely complex and the tools to configure them properly require a virtual library of reference material. Source code to popular operating systems such as VMS, NetWare, Windows NT, AIX, OS/400 and Solaris is not available. Even if it were, few administrators would take the time to study the code. Typically, the administrator must trust that the operating system has been written securely and that recommended practices to increase security are effective.

Even if the operating systems are configured securely, the network administrator must connect the different components and software together. Protocols such as TCP/IP have their own inherent weaknesses depending upon the OS's implementation of the stack.

Firewalls and other security hardware and software provide the network administrator with the same issues. Pre-packaged systems are purchased with the belief that they are secure. However, the administrator will never know unless a security bulletin is released or his/her system is breached.

Finally, applications have increased tremendously in complexity. In the name of features, applications are rushed to market to beat the competition. In the process, program bugs and "undocumented features" may leave holes which criminals can use to compromise an operating system. Furthermore, applications are rarely developed with security in mind. Microsoft's macro languages typify powerful application features that can wreak havoc on an unsuspecting organization.

Vendors often wait for the user community to find their bugs for them. Unfortunately, these packages are widely available to the aspiring hackers who are more than willing to test the systems for their own purposes. Bugs that may take companies months to patch, are potential gateways for criminals to exploit. Since networks contain hundreds or even thousands of these potential gateways, the security professional simply cannot keep abreast of all of their systems' vulnerabilities.

Information has increased in scope to transcend artificial boundaries

Today's users are mobile. Laptop computers, cellular phones, video conferencing and the World Wide Web have linked users to more information than ever before. Users demand that information be available whenever they want and wherever they are. The pressures this causes the network administrator leap in magnitude when their corporations demand multiple links to customers, vendors and partners. As Ellison, et al (1998) state:

> "Networks are being used to achieve new levels of organizational integration. This integration obliterates traditional organizational boundaries and integrates local operations into components of comprehensive, network-based business processes."

Such demand for increased communication drives potential holes in the administrator's fortifications.

Information abounds for the computer criminal. They have access to many tools to allow them to amass a tremendous amount of information about a target organization. Certainly, they have protocol information-gathering tools such as nmap and SAINT. They also have access to information services vendors such as the Lexis-Nexis which contains a great deal of information for those who know how to make use of it.

Not all information-gathering schemes require systems. Kevin Mitnick, the world-famous computer hacker, was asked, if he was targeting a company, where would he look first for information to assist him to compromise that target. His response: "I might look in their garbage." (Goodell, 1996) "Dumpster diving" still yields a tremendous wealth of information. Phone lists, executive memos, etc. provide short cuts that can save a criminal hours to days of time and effort.

Ira Winkler documented a situation where he was employed by a $5 billion firm to test their security. Posing as a temporary worker, he writes, "I was there for three days. I got everything they had." (Winkler, 1997) The security manager had hired Winkler because he was concerned about the openness of the company's research and development environment. Winkler simply walked in, copied critical company secrets, and left. He had never been challenged by any of the company's staff.

Winkler's success came from the research he conducted prior to arriving at the firm's offices. Internet library resources provided him information about the company's top development effort including the names of the research staff. Winkler writes, "Other open-source information identified the names of the company executives, the company's financial status and a wide range of general information about the company and its corporate philosophy." He also issued standard network commands and obtained a list of all of the firm's computer systems.

Finally, Winkler asked and received a company newsletter that defined the company's top six development efforts. This newsletter served as his "shopping list" for his later successful penetration.

None of his information gathering tools required a high-level of expertise. Yet, the information gleaned from his sources allowed him to penetrate the firm's perimeter and steal the company's innermost secrets.

Information is readily available to almost anyone about virtually anything. Obscurity can no longer be considered an adequate defense for any organization. Artificial boundaries such as firewalls and host protection of dial-up servers often fail to contain the dissemination of information. Readily available information freely given from an organization coupled with multiple communications entry and exit points from dial-up sources, Internet, etc. penetrate perimeter walls. This trend is expected to continue with additional forms of electronic commerce and increased numbers of electronic publications.

People and political factors compromise computer security

Robert Anderson of the RAND corporation succinctly states the emphasis of today's software development, "For years the market has emphasized increased

functionality, not security. If this trend continues, new vulnerabilities will arise that are unexpected and unaddressed." (Anderson, 1996)

To build upon what Anderson is saying, the emphasis of all companies is to make money. Efforts to produce goods and services provide income, while security and recovery are often viewed as an expense. Until the consumer community collectively demands security and recoverability as critical features of a product, these features will rarely be addressed outside of the defense and financial industries.

Computer security within an organization is often problematic. This paper has discussed the complexity of systems. In addition to that complexity, the industry suffers from a lack of computer security expertise. Jeffrey Schiller, a security expert at MIT said, "Vendors are selling systems that aren't perfect and the people who understand the technology are stretched so thin." (Sandberg, 1997) In addition, poor planning and documentation abounds.

Computer security is expensive. Good security tools to protect a medium ($100 million) organization can cost hundreds of thousands of dollars a year. Executives rarely see a return on that investment in hard dollars. Many firms opt not to buy additional security and rely on their host computers' operating systems to protect their information. Password protection becomes the default for authentication in these circumstances. The result provides only minimal security.

Behar (1997) states, "Technology managers are forever urging users to create codes that are hard for even a computer to guess, but people prefer passwords they can relate to—favorite sports teams, astrological signs, children's names." Most users lack fundamental security awareness necessary to prevent passwords from being exploited. Their focus is on their tasks at hand, not about threats they cannot readily see.

This lack of awareness stretches to the Executive boardroom, where day-to-day battles of business take precedence over poorly defined and misunderstood outside threats. Once a breach occurs, however, security and recovery typically increase in importance. Unfortunately, many businesses elect to investigate penetrations on their own without outside assistance.

While the FBI is available to help those firms who have had their security breached, few actually take advantage of their assistance. Loyd Hession, an IBM security expert said, "Nobody wants to be on the front page of a newspaper because they were broken into. A big concern is loss of public trust and public image." (Behar, 1997) Citibank publicly admitted its security had been breached in 1994. The result: Its top 20 customers were siphoned off by competing institutions that claimed their security was superior.

Until computer security is recognized as a critical success factor for Executive management; awareness is extended to all employees, customers and industry pundits; and a strong relationship is cultivated with law enforcement; businesses will not appropriate adequate resources to maximize the strengths of their security and recoverability.

System Survivability

Unlike traditional computer security, system survivability concentrates on the measures that assume security has been or will be compromised. The focus of the study on system survivability is to either engineer or augment an existing system to:

- Resist attacks- the hallmark of existing security practices.
- Recognize an attack or failure is occurring
- Recover by being adaptive as it loses resources to a successful attack and allocate remaining resources to continue its mission while fending off the attack.
- Be diverse enough and evolutionary so that attacks upon its weaknesses will not compromise the system.

A system is deemed to be survivable if it can withstand attack and damage and yet continue to perform its function in a timely manner. Often, survivability is confused with redundancy or fault tolerance.

Ellison, et al (1997) discusses this mistake in perception, "The concept of survivability includes fault tolerance, but is not equivalent to it. Fault tolerance relates to the statistical probability of an accidental fault or combination of faults, not to a malicious attack." Therefore, fault tolerance may provide protection from a server or disk crash, but a well-orchestrated set of events would still bring down a system.

Ellison, et al (1997) also discusses redundancy. "Redundancy is another factor that can contribute to the survivability of systems, but redundancy alone is insufficient since multiple identical backup systems share identical vulnerabilities." If a set of servers has the same programs and data, any weaknesses in one would be resident on all systems. If a criminal can exploit one, all could be exploited.

Survivability of systems suggests robustness. A collective network of systems should be robust enough to continue to perform its function in the face of actual or perceived danger. A network system must respond to incidents, identify the threats and execute a solution to those threats.

Shrobe (1996) states that, "Survivability inherently implies the question of what do you do after security fails." This presents a clear difference from traditional computer security where the emphasis is protecting the information from being compromised."

Survivable systems, Shrobe and others argue, must adopt the characteristics of living organisms or societies of organisms.

> Shrobe (1996) discusses the survivability of living things,
> "If you look at organisms, they almost all have some barrier to entry, skin, membranes and the like, things to keep out attacking elements. They all, at least at some level of complexity, have some form of immune systems, which says that even after the bad guys got in, I have ways of getting them out. Many of them have things that are sacrificial organisms like tonsils -- no one really knows why tonsils exist in the human body, but one thing they do right now is they get infected and, having got infected, they let the body's immune system see the infecting elements and they tend to be somewhat of a barrier at the same time. So they are an information-gathering element that lets the rest of the system respond."

Shrobe also looks at the survivability of societies pointing out that societies have public health systems, economies that allocate resources and duplication of skills across members of society to mitigate the risk of loss. Attacks of viruses, plagues, wars, etc. can

eliminate a portion of the society, but the society is able to heal itself and continue to perform its function.

Looking at the living organism and societal models, Shrobe identifies three characteristics which must be part of a survivable model. First, the system must have a "public health infrastructure" which can protect the system by noticing the attack, responding to the attack and extrapolating information on future attacks by isolating and studying it. Second, the system must be adaptive as it loses resources to successful attack or allocates resources to defend the system. The system must continue to function on lesser resources and appropriately prioritize its functions to successfully carry out its mission. Finally, the system must be diverse so that weaknesses that succumb to certain attacks cannot be used to compromise the entire system.

As CERT is part of Carnegie Mellon University and associated with the Software Engineering Institute, an engineering methodology called Survivable Network Analysis (SNA) has been developed. SNA helps organizations identify survivability exposures within their systems.

CERT (2001) outlines four steps in this analysis.

- System Definition- creates an understanding of mission objectives, requirements for the current or candidate system, structure and properties of the system architecture, and risks in the operational environment.
- Essential Capability Definition- both essential services essential assets are identified based on mission objectives and failure consequences. These essentials are identified by usage scenarios that trace services and assets through the architecture.
- Intrusion scenarios are selected based on the assessment of environmental risks and intruder capabilities. These scenarios are then mapped into the architecture to identify compromisable components.
- Components are then identified as to their level of essential and compromisable and compared to the "three R's" of resistance, recognition and recovery.

Lately, the emphasis on systems survivability has captured a large audience in computer security professional circles. When put into the context of the reasons that traditional computer security fails, the theory of system survivability provides some solutions.

First, the problem that computer security tends to be reactive could be eliminated. Protection mechanisms are reactive because they require vulnerabilities to be located first before appropriate fixes can be created. A significantly diverse system, as described in Howard Shrobe's third characteristic would minimize the impact of some vulnerabilities. In addition, Shrobe's "public health infrastructure" could discover an attack on a previously unknown weakness and respond. (Shrobe. 1996)

Computers are designed to perform calculations and tasks much faster and more accurately than humans. Harnessing that power to protect themselves could be much more cost-effective than trying to discover, isolate and mitigate vulnerabilities manually.

Secondly, the problem of "systemic components being complex and not fully understood" provides problems for people, but perhaps not to well-designed systems. Ellison et al (1997) state that,

> "As a broadly-based engineering paradigm, survivability is a natural framework for integrating established and emerging software engineering disciplines in the service of a common goal. These established areas of software engineering, which are related to survivability, include security, fault tolerance, safety, reliability, reuse, performance, verification and testing."

Systems built to police themselves may lessen the need for manual intervention, thereby increasing the efficiency and reliability of a system. These types of systems would be able to determine if users are exceeding the appropriate level of use designed by the system and alert administrators while taking appropriate action.

Thirdly, while information has increased in scope to transcend artificial boundaries, system survivability does not necessarily care if boundaries exist or not. The purpose of system survivability is to protect a system when an intrusion occurs regardless of firewalls or other perimeter security.

The Internet is an unbounded system where more and more "bounded networks" connect and interact. The nature of this interaction causes exploitable weaknesses, and the current level of interaction will probably increase. Ellison, et al (1997) strongly predict this increase.

> "This new paradigm represents a shift from bounded networks with central control to unbounded networks. Unbounded networks are characterized by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and lack of complete information about the network. At the same time, organizational dependencies on networks are increasing and risks and consequences of intrusions and compromises are amplified."

An example of a survivable technology is the concept of intelligent agents. These might be the communications medium in the future where each agent contains the message, authentication of the sender, an authentication mechanism for the receiver and specific defense mechanisms to protect the message against harm or interception. All information and systems operation could conceivably be designed in this manner so that protection of each "unit" would be built-in. The need for perimeters could become obsolete.

Unfortunately, dealing with the people and political factors can not be totally solved with technology, or even engineering. The responsibility for computer security must become that of all the parties (organizations, vendors, law enforcement, etc.) who have a vested interest in their shared communications resources. Computer systems could be used cooperatively to assist these parties to develop protection mechanisms. Although this would never be a perfect solution, since involving inherently imperfect organisms such as people makes this impossible, there could be fewer compromises of information. Fewer resources would be required for computer security since expensive perimeter defenses may no longer be necessary.

Issues such as password control could give way to more sophisticated authentication mechanisms at the "unit" level versus the host level. Intelligent agents, using biometric technology, could make the authentication process invisible to the user, thereby eliminating the memorization of passwords.

Political battles would still wage in the boardroom and the bottom-line will still rule decision making, however, if CERT is correct, centralized information repositories with survivable encapsulated information vehicles such as intelligent agents would free the individual organizations from having to see to their own protection.

Computer security specialists would be centralized thereby increasing expertise and communication among themselves. Linking these specialists with law enforcement would provide a formidable, unified defense against the criminal element.

Conclusion

System Survivability is not a substitute for computer security. The concept of resistance in system survivability encapsulates the efforts to protect the confidentiality, integrity and availability of information. However, the concepts of recognizing attacks and automatically recovering from them adds robustness to the security paradigm.

Applying survivability to our secure systems allows us to ensure the missions of our systems continue to be performed even if our systems are damaged or compromised.

To get us to the level of true survivability, however, focused efforts toward achieving survivability goals must be set and met. This will not be an easy task. First, organizations will need to determine these goals. Then operating systems and application vendors will need to engineer their systems to meet diverse goals from a wide variety of system users.

Finally, survivability must evolve and adapt to effectively handle new successful attacks and damage. Only then, will true system survivability be assured.

References

Anderson, Robert H. (1996) *Survivability Architectures* [WWW document] URL http://www.cs.virginia.edu/~survive/Papers/Anderson.html

Behar, Richard (1997) Who's reading your e-mail? Fortune Magazine Feburary 3, 1997 pp. 56-70.

CERT Coordination Center (2001). *Survivable Network Analysis Method*. [WWW document] URL http://www.cert.org/archive/html/analysis-method.html

Cheswick, William R. and Bellovin, Steven M. (1994) Firewalls and Internet Security: Repelling the Wiley Hacker. Reading, MA: Addison-Wesley Publishing Company

Coffee, Peter (1996) Reality: It's Worse Than You Imagine. PC Week November 25, 1996 pp. 22.

Eckel, George (1996) Intranet Working. Indianapolis, IN: New Riders Publishing

Ellison, R. J.; Fisher, D. A.; Linger, R. C.; Lipson, H.F.; Longstaff, T.; and Mead, N.R. (1997) *Survivable Network Systems: An Emerging Discipline* [WWW document] URL http://www.cert.org/research/97tr013.pdf

Ellison, R. J.; Fisher, D. A.; Linger, R. C.; Lipson, H.F.; Longstaff, T.; and Mead, N.R. (1998) *Survivaility: Protecting Your Critical Systems* [WWW document] URL http://www.cert.org/archive/html/protect-critical-systems.html

Garfinkel, Simson and Spafford, Gene (1996) Practical UNIX and Internet Security (2nd ed) Sebastopol, CA: O'Reilly and Associates, Inc.

Goodell, Jeff (1996) The Cyberthief and the Samurai, New York, NY: Dell

Howard, Dr. John D. (1996). *An Analysis of Security Incidents on the Internet 1989-1995*. [WWW document] URL http://www.cert.org/research/JHThesis

Linger, R.C.; Mead, N.R.; and Lipson, H.F. (2001- *no publishing date) Requirements Definition for Survivable Network Systems* [WWW document] URL http://www.cert.org/archive/pdf/icre.pdf

Sandberg, Jared (1997) Accidental Hacker Exposes Internet's Fragility; in The Wall Street Journal, July 10, 1997 pp. B1

Shrobe, Howard, Dr. (1996) *Survivability* [WWW document] URL http://www.arpa.mil/ito/arpatech96_briefs/survivability/survive_brief.html

Vandenoever, Chris (1995) Computer security, Your Business and the Internet New York: Deloitte & Touche LLP

Winkler, Ira (1997) Assignment Espionage. Information Security News February, 1997.