Global Information Assurance Certification Paper

Intrusion Detection Systems

The Treat

Today there exists a weapon that has the potential of creating financial chaos and creating crippling effects to the infrastructure of this country while escalating fear and plummeting moral would weaken our resolve. This weapon sits in your homes and on your desktops at work. The computer and the information infrastructure known as the Internet have become a supporting pillar to our economic system and social infrastructure. The operation of our government and our military depend on these systems operating as they were designed, when they are needed! This threat called "Information Warfare" requires a strong, successful defense effort called "Information Assurance".

We are probably only detecting 2-15% of the actual intrusions made on our information systems. This percentage is threatening to go even lower as switched networks provide addressing down to individual host computers, as virtual private networks become more widely used, as network traffic and speeds increase, and as more computers and information systems stay operational 24 hours per day.[11]

The Internet and smaller subsystems are becoming more complex, more interconnected, and more widespread as our society becomes more dependent on their successful operation.[2] This complexity and the rapid advances in technology are forcing hardware and software manufacturers to common standards, and complex systems made up of Common-Off-The-Shelf (COTS) components.[2,3] These changes are creating the next Renaissance[15], and Armageddon if we are not prepared. This information infrastructure is so important that it became the subject of a Presidential Decision Directive. PDD-63 established policies to protect that infrastructure from fatal disruptions from both internal and external causes.[6]

How serious is the threat? Recently two California teenagers with the help of one other foreign person managed to penetrate several unclassified yet protected systems within the Department of Defense.[10] As hackers and crackers gain knowledge about system vulnerabilities, their knowledge is quickly spread through underground and Internet connections. This knowledge, their tools and their techniques are readily available to everyone.[2]

While the offense (bad guy) is getting faster and smarter, the defense (good guy) continues to be plagued by problems. Ignorance of the threat seriously jeopardizes finding and utilizing solutions. Marketing requirements to "be first" with software and hardware products is a double edge sword. Not only are these products produced with security an afterthought, often neglected to obtain a "better market share", but poorly designed products lull the users into a false sense of security. Vendors are rarely challenged because most users do not understand what they are getting and usually operate in the products "default mode". Finally there is a general lack of understanding of what poor performance from a security product could cost.[2,3]

The threat is no longer just from sophisticated corporate or government spies. Easier ways to seriously disrupt or damage systems are being devised daily. One such method of causing serious damage can be achieved by forcing a system into a shutdown or overloaded condition. This type of attack, known as a "Denial-of-Service" attack does not require passwords to be known or firewalls to be violated. A single coordinator can "enlist" the cooperation of

literally thousands of individual host machines to create a diverse, overwhelming attack upon a single victim.[9] The victim system is helpless as it tries to process requests for data from thousands of different user. In attempting to service them all, service is denied to legitimate users. This method is becoming easier to invoke as more home computers are being left "on-line" and are operated by people with little knowledge of security.[8] Any programmer knows that "endless DO-loops" can easily kill a system and interactive subroutine calls can rapidly cause system termination through a technique known as "stack overflow". Another problem is a "Catch-22" situation where applications that are designed to create a more robust, secure environment actually foster a situation where damage is amplified. Many database systems are designed to withstand attack or damage through a distributed architecture, but to maintain concurrency, duplication of the database is run repeatedly. Duplication of a legal, but viral entry is thus spread to all other copies of a database under a legal and seemingly harmless transaction.[1]

Intrusion Detection Systems

Any secure system must be protected from attacks. A good defense is made up of two types of action. The first is a passive defense consisting of knowledge, effective procedures, and equipment properly initialized and maintained. These things must be done before any system is brought on-line. The second is a plan of what to do when your system is attacked.

Intrusion detection is a blossoming science, involving detection research and reaction research. Intrusion systems have largely been manual processes. The "signature" of a virus or program is discovered. The signature is then transmitted (usually by e-mail or Internet download) to a system administrator. The system administrator then adds this new signature to a long list of other "bad" signatures in the form of e-mails, programs, or Internet packets that must be stopped.[11]

The intrusion detection body of knowledge is growing rapidly. There are many new areas being explored and many older standard methods being upgraded. Currently, intrusion detection systems monitor "traffic" or "operations" from a particular site and report these conditions to a central controller (human or machine). These monitors can be located at a gateway or firewall between a corporate intranet and the outside Internet (known as Router Based monitoring). From this position, network traffic is monitored before it is allowed to enter an intranet system. E-mails, programs, and Internet packets are monitored for signatures that are on the "bad" list. This labor-intensive method prevents access to a system's intranet infrastructure. The problem is that this system relies upon known signatures and causes system performance problems as traffic density increases. In addition, this type of intrusion detection is unable to stop encrypted packets or system attacks from "inside" the intranet.

Another location for intrusion detection monitors is inside the intranet between selected subsystems or host computers (known as Network Based monitoring). These monitors also watch for unauthorized "signatures", but in addition begin a crude process of "behavior analysis". This process requires a knowledge database that contains "normal" or "acceptable" patterns. The patterns monitored ay range from counting file access requests to sophisticated comparisons of personnel patterns. System usage is then compared to these normal patterns and unusual behavior is reported to a central controller. These systems suffer from lower efficiency at higher traffic density and are subject to high false-alarm rates.

The last common location to place intrusion detection monitors is within the host (known

as Host Based monitoring). From this location behavior analysis is more effective, and not effected by network encryption schema. But these systems are expensive and very "power-hungry" because of all the CPU time needed for analysis.[7,13]

Some metrics that are used to judge intrusion detection systems are percentage of successful intrusions detected, and the number of transactions reported by the system as intrusions, but actually are legitimate operations. This later category is known as "false alarm rate". With hundreds of transactions occurring every minute, a false alarm rate of 1/10 or 1/100 of a percent means too many reports that must be analyzed by an operator. Figure 1 shows the four categories that every transaction must be cataloged as. The goal of all intrusion detection systems is to make "real attacks" = "intrusions claimed by the system"

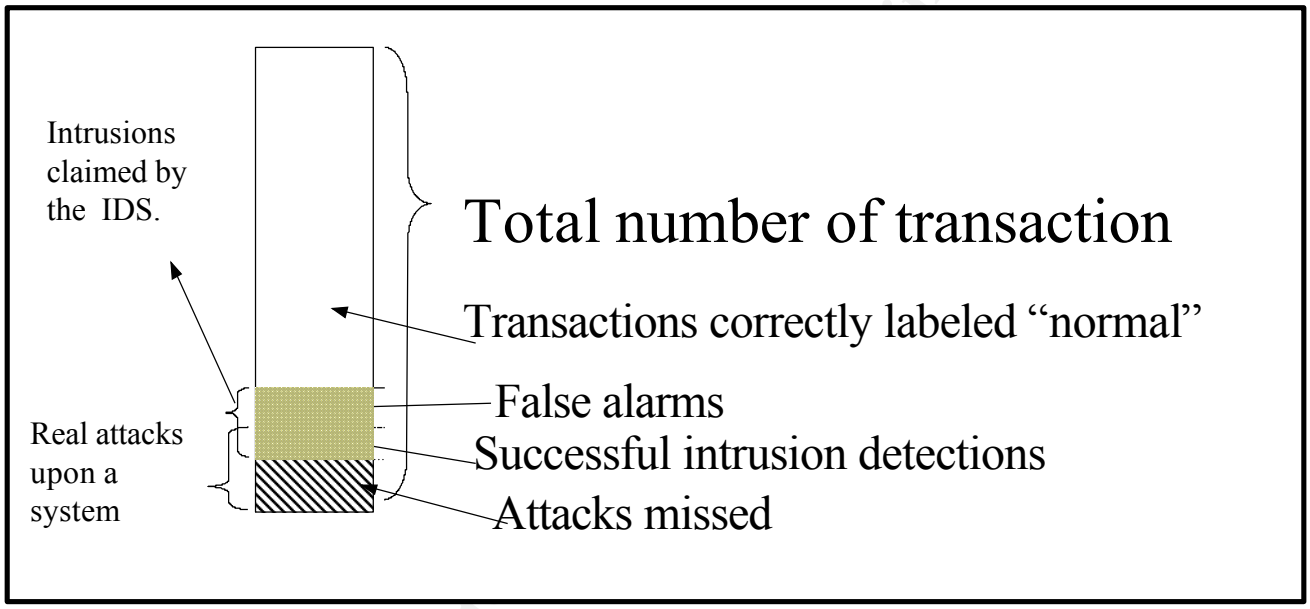

Figure 1

Not all attacks are rapid processes either. Some attacks may be designed to alter a database or program slowly and from multiple sources. A Trojan horse program may be planted over several months. This type of behavior requires intrusion detection systems to pick out unwanted transactions from everyday mistakes by watching long term behavior or setting "trip wires".

The Future

Intrusion detection is looking into many new areas. Combination systems are being developed that use the best of host, network, and router based monitors. These distributed systems could use mobile agents to go and monitor certain areas as needed. Much the same way that police are called to a house to investigate suspicious activity reported by a neighbor. There is research into reactive and adaptive defensive systems that make intrusion much more difficult. These systems are designed to react to suspected intrusions by adapting the environment of the system. This frustrates intruders who have spent time "mapping out" the system to prepare for an intrusion.[10]

A greater understanding of anomalous behavior is being studied through analogous behavior of the human body and its defense mechanisms. The body manages to distinguish normal cells from abnormal cells by attribute classification.[1] This same behavior can be used through "user profiling".[12]

Use of "Red Teams" is also on the rise. These teams are invited to attack a system to uncover system weaknesses. The holes in security can then be fixed before a real intrusion occurs.[5] This method allows the use of a hacker's own tools and techniques to create barriers that are so sophisticated that a lot of resources and time would have to be sacrificed to conduct a successful intrusion.

No system is foolproof, and information assurance is going to be a leapfrog game of successful intrusions and successful responses. These responses must be rapid, reactive, adaptive, and successful. The goal is to create systems that will continue to operate at a reduced status if necessary until full operation can be restored and the information assured.

Bibliography

1. Ammann, Paul; Jajodia, Sushil; McCollum,Catherine; *Surviving Information Warfare Attacks*; Computer Magazine; April 1999.
2. Benjamin, R.; Gladman, B.; Randell, B.; *Protecting IT Systems from Cyber Crime;* The Computer Journal; Vol. 41, No. 7, 1998.
3. Executive Summary of book. "Trust in Cyberspace"; http://www.nap.edu/readingroom/books/trust/trustsum.htm; Nat'l Academy Press, 1999.
4. Herringshaw, Chris; *Detecting Attacks on Networks;* Computer Magazine; December, 1997.
5. Brussin, David; Cobb, Stephen; *Hackers in White Hats;* Byte Magazine; June 1998.
6. White paper; *The Clinton Administration's Policy on Critical Information Infrastructure Protection: Presidential Decision Directive 63;* May 22, 1998.
7. Hurwicz, Michael; *Cracker Tracking: Tighter Security with Intrusion Detection;* Byte Magazine; May 1998.
8. Lemos, Robert; *New Cyber Attack Method Surfaces;* ZDNN website for Computing; October 19, 1999
9. Downey, Jeff. *Denial-of-Service Attacks;* ZDNN website; http://www.zdnet.com/devhead/stories/articles/0,4413,2172746,00.html; October 20, 1999.
10. Robinson, Brian; *Firewalls: The First Line of Defense;* Federal Computer Week website; http://www.fcw.com/ref/hottopics/security/firewalls.html; September 29, 1999.
11. Robinson, Brian; *Spotting Intruders;* Federal Computer Week website; http://www.fcw.com/ref/hottopics/security/intruders.html; September 29, 1999.
12. Marceau, Carla; Stillman, Matthew; Stillman, Maureen; *Intrusion Detection for Distributed Systems;* Communications of the ACM; Vol. 42, No. 7, July 1999.
13. Champion, Terrance; Durst, Robert; Miller, Eric; Spagnuolo, Luigi; Witten, Brian; *Testing and Evaluating Computer Intrusion Detection Systems;* Communications of the ACM; Vol. 42, No. 7, July 1999.
14. Goan, Terrance; *A Cop on the Beat: Collecting and Appraising Intrusion Evidence;* Communications of the ACM; Vol. 42, No. 7, July 1999.
15. Toffler, Alvin; *The Third Wave;* Bantam Books, New York, New York, Dcember 1991.

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS