

Table of Contents

Overview 2

The Problem 2

Typical Attack 3

 Intruder Behavior 3

 Types of Attack 4

What's Needed 5

 More than Perimeter Protection 5

 Reducing Damage-time 5

 Ready Response 6

 Protection Against Insider Jobs 6

 Flexibility, Scalability, and Transparency 6

The Security Choices 6

 Static Security Technology 6

 Active Security Technology 8

 Intrusion Detection 8

 The Key Components 9

Summary 11

Overview

There's a new concern now facing the professionals responsible for network management. It hasn't replaced the usual worries—reduced budgets and headcount, the demand for increased performance, applications and service levels, and the growth of TCP/IP connectivity through the Internet—but is an additional challenge. Security.

And unlike the traditional challenges of network management, this new issue often catches the network professional in a state of inadequate preparation, without the resources, training or expertise born of years dealing with security issues.

The good news is that there are ways to bridge the gap. Due largely to Internet growth, security issues have recently been pushed front and center, with security-related products, software, and awareness increasing rapidly.

This paper will help to provide a basic understanding of network security by focusing on the primary distinction among security technologies: static (preventative) versus active, real-time security. The distinction is an important one. While static devices such as firewalls can offer a measure of protection, their passive nature belies the burdens—in cost, maintenance and performance—that they place on the network. More importantly, their inability to function in real-time—to detect an intrusion within seconds of its occurrence—fails to adequately counter the key intruder asset, that is, the time to get in, reconnoiter and ultimately do damage to a corporate network.

With an understanding of the critical ability to detect and contain an attack as soon as possible, a network professional is better prepared to make the decisions about how to best protect corporate assets given the available resources and budget.

The Problem

Today's information technology managers are faced with a rapidly evolving technology based on open systems and extensive connectivity. With this new capability comes risks of intrusions and information compromise.

According to *Financial Times* (April 1997), a network is hacked into every 20 seconds. Using techniques such as eavesdropping, phone system tampering, and IP spoofing, an increasingly sophisticated cadre of hackers is gaining access to corporate assets. The targets of these attacks, according to the Computer Security Institute of San Francisco, CA which sponsors a research survey with the FBI every year, are most likely to be financial and medical institutions. This means that financial transactions, medical records, and credit histories—information of the most personal and confidential nature—are at risk.

And what about the actual monetary costs of these attacks? According to “Trends in Intellectual Property Laws,” a study from the American Society for Industrial Security (ASIS), the losses from intellectual property theft for US-based companies worldwide are estimated to be \$24 billion annually. Computer hacking was ranked second as a means of acquiring this information. Extortion alone has cost companies, mostly financial institutions, over \$600 million in the last three years, and possibly much more due to the reluctance to report such cases, according to the *Sunday Times* of London.

According to the Computer Security Institute, losses from 249 organizations surveyed totalled \$100 million, for an average loss of \$402,000. These are just the costs of actual theft. The research and forensics costs in systems, personnel, effort, and lost time and productivity are often not accounted for in the loss estimates.

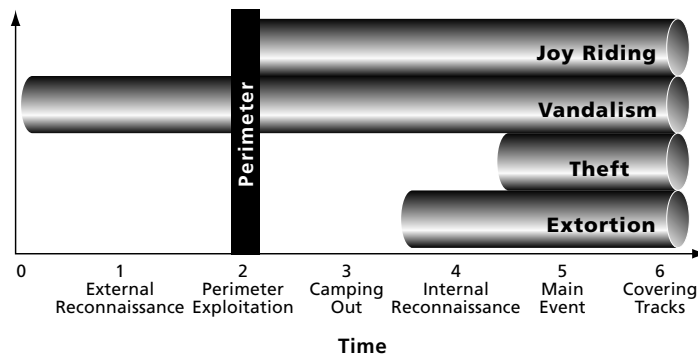
Despite the particular vulnerability of firms in the medical and financial industry, no corporate network is immune from attack, misuse or intrusion. An understanding of typical attacker behavior and intent helps to understand what a corporate network needs to identify and protect against becoming a target.

Cost of Computer Crime:

- Average attack: more than \$400,000
- Over \$600 million in extortion alone over the last three years

Typical Attack

By observing the many instances of intruder attack (and using the testimony of attackers themselves), security experts have been able to compile a *modus operandi* of intruder behavior, as well as an understanding of the different types of attack and subsequent damage.



Intruder Behavior

From the initial intrusion to the final exit, the key categories of attacker behavior can be organized into the following sequence.

Reconnaissance. Before an attack begins or a system is compromised, a potential intruder scopes out potential targets. The cyberspace equivalent of a burglar casing the neighborhood, reconnaissance consists of using networking and programming techniques to determine the location of a company on the Internet, whether through dial-up links or other electronic addresses. By “pinging” networks to find the addresses of perimeter devices, an intruder can effectively map the electronic boundaries and access points of the corporate IS structure.

Perimeter Exploitation. This is the point of intrusion, equivalent to the “breaking and entering” stage of a burglary. The intruder, having located a target and defined its access points, proceeds to enter through weak points in the perimeter

or on services that are typically allowed into networks, such as e-mail and Web messages. The usual points of vulnerability are modem connections to hosts, weak administrative passwords for external devices, back doors, misconfigured firewalls, and exploitable Web hosts with links inside the network.

Camping Out. Once admission into the network is gained, the next step is creating a safe, undetected spot within the perimeter for camping out, in order to hide, study the surroundings, and plan the attack. Attackers usually compromise an easy-to-exploit host which allows them to gain root (supervisor) access.

Internal Reconnaissance. Once a camp has been set up, the outsider is now an insider, with all the time in the world to root around the network and identify the spoils. Of course, if the attacker is an insider to begin with (for example, a disgruntled employee), the attacker starts with this advantage, and proceeds to locate the assets to be stolen or damaged in the assault's main event.

Main Event. This is where the real damage is done. Typical main events include grabbing software code, pirating financial assets, accessing confidential information, destroying data or hardware, and planting hidden programs of destruction (Trojan Horses) for future activation. (See next section entitled

Types of Attacks.)

Covering Tracks. Once the main event is completed, the intruder must find a way of getting out without getting caught. A smooth exit depends on disabling, removing or replacing log information that would otherwise identify a security breach.

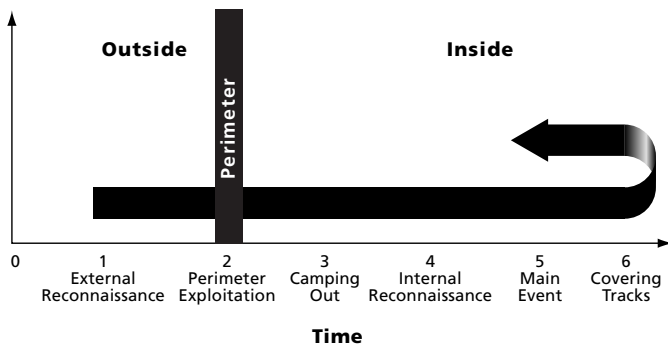
Types of Attacks

Attacks can be defined by the different ways that goods or services are taken or damaged. Following is a description of the typical categories of attack, how they occur, and what

their costs are.

Joyriding. This is the commandeering of computing resources, phone service, or Internet Service Provider connections which allow the intruder to exploit these services without paying for them. One of the most popular joyrides is gaining free access to the phone system (called "phreaking," for PHone fREAKING) for unlimited travel on the world's data communications networks. While typically non-destructive, joyriding can be a costly ride at the expense of the customer or service provider.

Vandalism. Vandal attacks include damage to systems and files as well as denial



of service to legitimate users. Common vandal acts include data destruction, and Web page creation, alteration, or misdirection.

Vandals need not be inside the network to inflict damage. Destructive viruses can be piggybacked onto files destined for the inside. Denial of Service (DoS) attacks can also be launched externally; by flooding a network device with lots of frames or doctored frames, a vandal can cause a shutdown of service to legitimate users. Internet Service Providers have been the primary victims of these DoS attacks.

Theft. With the growth of Internet commerce, the potential for and dangers of theft have also grown. Anything of value can be stolen—from data and access, to whole databases, financial assets, and sensitive personal information. The latest FBI figures estimate this loss at \$7.5 billion annually.

Extortion. Often simply the threat of an attack can effect a corporate loss of assets. The threat of destroying systems, encrypting data and otherwise corrupting the integrity of the corporate network has cost companies millions of dollars a year. In just the past three years, it's been estimated that up to \$600 million has been extorted, mostly from financial institutions. A typical scenario is the Trojan Horse threat, wherein a hacker plants a destructive program in the network, waits a period of time, and then demands payment upon threat of activating the destructive mechanism.

What's Needed

Based on the characteristics of intruder behavior and typical attacks, it's clear that an effective security solution must counter the key vulnerabilities of the corporate network. Additionally, the issues of network implementation and maintenance must be addressed.

More than Perimeter Protection

The most popular types of security devices—firewalls, authentication devices, and system wrappers—are focused on protecting the entryway into a corporate network. While effective, perimeter protection alone is not adequate, due to its inability to detect attacks that originate from within the walls or succeed in vaulting over them.

Reducing Damage-time

The hacker time line proved it—time is the most valuable asset to someone launching a network attack. Given enough time, a determined hacker can penetrate any system, regardless of the security. In order to reduce the risks of damage, it's imperative that a security system operate in real time; this allows it

to detect and warn against an intrusion within seconds of occurrence, and shut the window of vulnerability as soon as possible.

Ready Response

Real-time detection can be followed up with real-time response. By automatically stopping the intruder at the time of attack, the system disables the intruder and blocks access to corporate assets.

Protection Against Insider Jobs

Recent studies estimate that 50% to 80% of intrusions originate from the inside. More disturbing is the fact that these internal attacks are the most damaging. The disgruntled worker with inside knowledge and adverse motives, the outsider who becomes an insider via an unauthorized modem on a workplace desktop: these are the real threats to corporate data because they have direct access to vital information.

Flexibility, Scalability, and Transparency

Any security system will need to be installed, maintained and updated. These costs are as real as the costs associated with a potential loss, and should be considered in the choice of technology.

The Security Choices

In response to the above threats, security vendors have introduced a host of new products and capabilities that provide information protection for the modern open systems environment. These products can be divided into two distinct categories: passive or static technology, and active or real-time systems.

A) Static Security Technology

Many of the most popular security devices on the market are categorized as passive or static security. These include perimeter protection devices—such as firewalls and system wrappers—that simply provide the mechanics for use by someone who intends to take action.

While firewall and system logs provide information that can prove valuable to response or recovery, this action takes place after the fact. Information is gathered but there is no knowledge base from which to identify an attack, nor mechanism to follow up with an alarm or response. Additionally, sometimes even the logs themselves are useless—too much time has passed and the backups have since been overwritten or the system has been rebooted and the logs not saved.

Firewalls. Firewalls are electronic packet filters and proxy servers that function as perimeter guards around a network. Usually deployed in front of Internet access links, WAN links, and dial-in servers, firewalls regulate and monitor the

protocols and services that can flow in and out of a network. Although effective, they have no true means of detecting suspicious activity. And performance/cost drawbacks make them inappropriate for deployment on the internal network.

Host-based Security. This consists of software loaded on a host to make that device less vulnerable to attack. System wrappers are software that behave like firewalls for servers, by wrapping around host operating systems and network stacks, restricting access to defined users and processes. Wrappers can also create secure logs of all network and user activity on that server.

Encryption and Authentication. Encryption is a method of scrambling information so that a sender can send a message in the open, past observers, to a trusted receiver. Encryption algorithms form the basis for most computer authentication schemes. This technology is usually used to defeat the threat of unauthorized users who may try to “look” in on your physical or vital network links, but since some encryption schemes strip the encryption security once entering the internal network, the inside network is not protected.

Limited Protection. A key drawback to perimeter devices like firewalls and encryption is that they address only external threats. An insider—or any outsider who successfully vaults the perimeter—goes undetected. The same with authentication methods: once authentication is established with the latest authentication system, a user usually has uncontested access to most of the internal network.

Additionally, firewalls tend to be vulnerable to gradual compromise. While packet filters and proxy servers can limit access to IP addresses and specified services, inevitably some users will demand access. So, the administrator ends up opening “holes” in the firewall and trying to remember to close them later—creating a “Swiss cheese” effect that leaves the network less protected.

Maintenance and Performance Costs. Another drawback to passive security technology is the effort required to implement and use it. Passive devices don’t perform active functions like tracking intruders—this must be handled by an administrator at a considerable investment of time and effort.

Firewalls are a good example of this. While firewalls are widely used to secure the corporate electronic perimeter, they are cumbersome, with high maintenance costs and loss of network performance. Money and time are spent whenever a system administrator loads security agent software on a host, analyzes firewall logs for attacks, takes a router off line to reconfigure filters, or establishes a proxy to protect a new service on the network. And, in the event of an attack, there are the costs of dedicating personnel to perform the lengthy process of investigation, recovery and future prevention.

Additionally, a number of security products, just by running on the network, significantly degrade overall network performance, having an adverse effect on normal business operations.

B) Active Security Technology

Active technology is defined by the capability to actively seek out network vulnerabilities or security breaches, often with the added capability of issuing an automatic response prior to human intervention.

Seek-out technologies include: vulnerability audit/scanning tools which test networks, systems, and applications for vulnerabilities; monitoring services, which alert network managers to router problems, network intrusions or suspicious activity; and virus detectors.

In an additional category is active intrusion detection. Combining seek-out capacity with automatic response capabilities, intrusion detectors employ algorithms to identify certain types of attack activity and issue alarms and responses when patterns are identified.

Let's take a closer look at these active security technologies.

Vulnerability Audit Tools. Also called scanning tools, vulnerability auditors are test software which run over the network and check for areas of weakness. While active in the testing sense, they still require the user to take action to patch, fix or eliminate vulnerabilities, and are valid only for that "snapshot" in time.

Monitoring Services. Similar to fault and performance monitoring tools, security monitoring tools continually check the network for router problems, network intrusions or suspect activity. While proactive in the monitoring sense, these tools also still require follow-up action on the part of a user.

Virus Detection. Virus detection software can reduce the risk of stray infections. But even secured networks can be vulnerable since viruses can travel in the code given out by software vendors, software downloaded from home, and e-mail. Some virus detection software can detect and eliminate viruses from programs with little or no user input. While an effective method of protection, loading virus detection software on every desktop and server system is time-consuming and costly.

Intrusion Detection

One of the most powerful types of active security technology, intrusion detection systems combine network monitoring with real-time capture and analysis of packet header and content data. They then utilize sophisticated algorithms to recognize types of attack signatures, and upon discovery, send alarms and even take responsive action.

Some intrusion detection systems are host-based, in which system software focuses on user-level and authentication activities, file access, system actions and shoring up known OS weaknesses. The drawbacks are **a)** the software must be loaded onto every host (expensive) and **b)** its host-focused view lacks system-wide visibility (for instance, it would fail to see a network reconnaissance sweep as a threat, since it would see only reconnaissance on itself).

The other type of intrusion detection system is network-based. A network-based system typically consists of intelligent distributed probes (or sensors) working in concert with information repositories and front-end management software. The sensors do most of the expert analysis of the data stream and send only alarm data to a central manager—reducing the added traffic burden on the network and minimizing interference with normal operations. Additionally, network-based systems that are architected for promiscuous attachment can fit into existing networks without bottlenecks or information rerouting.

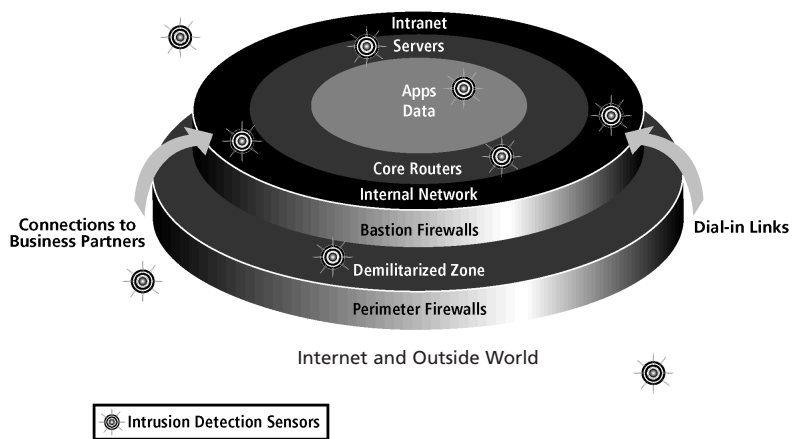
The Key Components

Given the limitations of passive technology and host-based intrusion detection, the ideal intrusion detection system is a network-based system that addresses the key needs for real-time detection, alarming and response. Other features—addressing the needs of reliability, security, transparency and recovery—are discussed here.

Real-time Component. Since the most powerful weapon in the hands of an intruder is time, a real-time component to all security systems is essential.

Real-time detection means an intrusion is identified within seconds of network misuse or compromise, before damage can occur. **Real-time automatic response** means that the attack is met with an instant reaction—the triggering of an automatic logging function, alarms to the right parties via e-mail, pager or SNMP traps, or automatic programmed response.

Event Blocking. Event blocking is an added function that can augment the logging and alarming features by performing an automatic connection disconnect (or block) in response to certain highly destructive attacks such as SYN flooding or TCP hijacking.



Strategically placed intrusion detection sensors protect essential elements at the perimeter and inside the network.

Smart Alarms. Unreliable alarms and false positives will prompt system operators to ignore not only false alarms, but all alarms. It's critical to minimize false positives and allow administrators to tune their devices according to their own network.

For this reason, intrusion detection technology has gravitated toward a misuse- or signature-based technology—built-in analytical intelligence can recognize hundreds of attack, misuse, and intrusion signatures. For instance, some attacks are simply a collection of lesser events that would go undetected, but collectively signify an intrusion. A smart system knows the difference, which makes the system more secure and reduces the likelihood of false alarms.

Logs and Trace Files. Log files are essential for tracing an intrusion. They keep a record of key attack information for pinpointing the originating address and following the intruder's course. This log helps with post-attack response too, assisting with recovery and case-building.

Evidence trace files are the detailed packet records from an attacking address that can be automatically captured once an intrusion is detected. These evidence trace files follow the intruder's "footprints" and can be used to determine attacker intent, destination, and techniques. If captured correctly, the trace files can also be off-loaded to be read by a Sniffer® Network Analyzer, or used as evidence for law enforcement.

Secure and Transparent Transmission. A detection system that uses the latest security technology to authenticate, encrypt and manage communications helps eliminate spoofing, denial of service, and snooping attacks. Additionally, transparent intrusion detection technology means that an intruder as well as authorized users cannot tell that they are being tracked.

Summary

Here's what we know. Corporate networks have been fundamentally changed by the growth in networked communications. The Internet, providing information to an exponentially growing number of users and providers, has changed the profile of corporate networks from a closed model to an open vehicle for commerce and communication. At the same time, corporate networks have become mission-critical repositories and mediums for data, assets, and services. Along with that growth have come certain risks that traditional security methods are not fully prepared to address. Firewalls and perimeter protection are no longer enough for a global communications model based on convenient access. Network security personnel can no longer hope that a perimeter fence will secure their network against savvy, patient attackers or threats from the inside.

For a corporate network to attain a more assured level of protection, a more active, intelligent technology is necessary. One that actively monitors the network and recognizes the obvious as well as subtle signs of network compromise, whether originating from the outside or inside. One that responds in a time frame that allows for immediate protective action to be taken. One that assists the network security manager at all points in the attack cycle, from initial attempt through the last stages of recovery and case-building. And one that can be implemented and maintained without an excessive burden on either personnel, network structure or network resources.

No technology can promise a "silver bullet" solution of iron-clad guarantees and promises of permanent worry-free security. But security methods that recognize the new realities of network communications are more effective than security methods that ignore these realities. Active intrusion detection technology addresses the new realities. When paired with perimeter protection, intrusion detection can provide the level of protection necessary for safeguarding one of the corporation's most valuable mission-critical assets: its own network.

To Learn More

If you would like to learn more about the new security technologies, please ask your local Network General sales representative or call 1-800-SNIFFER for more information. To learn more about Network General and our full range of fault, performance and security management solutions, please visit our Website at www.ngc.com.

Visit our Website



<http://www.ngc.com>



CALL 1-800-SNIFFER

NOTES

.....

..... **Network General**

CORPORATE HEADQUARTERS

4200 Bohannon Drive
Menlo Park, CA 94025 USA
Tel (650) 473-2000
Fax (650) 321-0855
Sales (800) SNIFFER, (800) 764-3337

EUROPEAN HEADQUARTERS

Network General UK Ltd.
Minton Place
Victoria Street
Windsor, Berkshire
SL4 1EG, United Kingdom
Tel (44) 1753-827-500
Fax (44) 1753-827-520

CANADA

Network General Canada, Ltd.
Tel (905) 709-9155
Fax (905) 709-9180
Tel (604) 299-9331
Fax (604) 299-9352
Tel (403) 254-8585
Fax (403) 254-8302
Tel (514) 733-6230
Fax (514) 733-6430

ASIA/PACIFIC/LATIN AMERICA

Network General Singapore
Tel (65) 222-7555
Fax (65) 220-7255
Network General Hong Kong
Tel (852) 2832-9525
Fax (852) 2832-9530
Network General Australia Pty Ltd.
Tel (612) 9929-8588
Fax (612) 9922-7710
Network General Latin America
Tel (305) 595-0025
Fax (305) 595-1541

**Network General products, support, and services are available
from sales offices, authorized resellers, and distributors worldwide.
For more information, visit our Website at www.ngc.com.**



TOTAL NETWORK VISIBILITY™



Network General, Sniffer, and Total Network Visibility are registered trademarks or trademarks of Network General Corporation and/or its wholly owned subsidiaries in the US and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. All specifications may be changed without notice. ©1997 Network General Corporation. All rights reserved.

Forward product suggestions to Network General at: suggestions@ngc.com



.....

**Protecting Your Network:
The Choice Between Active and
Static Security Technologies**

.....

A Network Visibility Guide



TOTAL NETWORK VISIBILITY