Center for Technology in Government

Internet Security Seminar

Center for Technology in Government
University at Albany, SUNY
1535 Western Avenue
Albany, NY 12203
Phone: (518) 442-3892
Fax: (518) 442-3886
Email: info@ctg.albany.edu
http://www.ctg.albany.edu

Abstract

Internet Security Seminar

April 1996

A day-long seminar on Internet Security was presented on April 2, 1996 by the Center for Technology in Government in conjunction with our corporate and public sector partners. This summary highlights the seminar sessions and results.

Internet Security as Part of the Overall Security Plan

Laura Iwan, Director, HEALTHCOM Services Support, NYS Department of Health

An introduction to Internet security issues discussed in more detail by other presenters: the cost of security attacks, common threats and vulnerabilities, security controls, and resources.

Computer security attacks cost as much as $10 billion a year. An attack can damage data integrity, confidentiality or availability. Organizations must understand the potential costs: How would incorrect data affect decision making? What will happen if confidential information is made public? What is the cost (in lost time and credibility) of interrupted service? To understand threats, organizations should ask themselves: Does the information have a dollar value? While more security equals more cost, the cost is slight compared to a single breakdown of services.

Vulnerabilities exist in all computer systems and all Internet services (SMTP, Telnet, FTP, HTTP, etc.). Email can be intercepted or spoofed. In Email spoofing an attacker assumes a false identity to solicit information or access. Hackers also exploit root compromises on old systems, poor passwords, IP spoofing, misconfigured networks, and packet sniffers. Internal attacks represent even more danger: over 80% of all break-ins come from internal staff or staff that has recently left an organization.

Internet security starts with proper administrative and physical security. Firewalls and bastion hosts should be employed where necessary. Administrators should monitor and log all activity. For mail threats, an organization may consider authentication and/or encryption technologies.

System administrators should stay current on system vulnerabilities and controls. Resources include "double- edged swords" such as SATAN, ISS, and hacker discussion lists, as well as "lifeguards": CERT, FIRST, CIAC, NIST, COAST, and the many World-Wide-Web sites devoted to security issues.

Risk Assessment: The Foundation for Security Planning

Dave Dumas, Senior Security Consultant, Digital Equipment Corporation

Internet risk assessment must address a myriad of specific Internet threats. By running a "risk assessment workshop" an organization can determine security needs and develop a security strategy that covers both personnel and technology issues.

The risks of the Internet reflect its size: 50 million users, 30 thousand networks, 10+ million computers, 137 countries. As capacity, connectivity and mobility increase, so does risk. Prominent sites are probed daily. Banks may get 50 or more probes a day. Successful attacks are automated and posted to electronic bulletin boards; attack methodologies quickly spread.

On the other hand, 90% of all attacks come from inside sources, primarily by disgruntled or laid-off

employees. Another inside attack, social engineering, is widespread and effective. The attacker researches an organization, then uses that information to deceive users or administrators into granting him or her access.

Organizations must understand security issues. They must stay current on tools (such as SATAN), security user groups, hacker web sites and liability issues. Still, the technological approach must reflect business needs: ease of use, industry standards, employee skill-sets, etc. To determine security needs, an organization can run a risk assessment workshop.

A risk assessment workshop includes 8 to 12 subject matter experts from within an organization, outside computer security experts and a moderator. The participants analyze the following: threats (hackers, viruses, disgruntled employees); targets (files, applications, hardware); probability of attack (number per year), impact (cost) of attacks, and countermeasures. Then the participants create threat/object pairs (for example, hacker/database) and analyze the vulnerability and impact for each. From this analysis, the organization can determine its security strategies.

Securing the Server and LAN

Frank Wickham, Senior Systems Engineer, Sun Microsystems

Based on an understanding of Internet risks, an organization can implement any of a number of security architectures. These can incorporate router controls, firewalls, authentication and encryption, and a number of other technologies. An organization should secure both its LAN and its Internet server.

Computer security threats continue to increase. CERT reports a 77% increase in break-ins between 1995 and 1996. Electronic crimes are particularly costly, with a price tag of $650,000 (compared to $9,000 for the average bank robbery). Part of the problem is that break-ins often go undetected. One study used common hacker tools to break into Department of Defense systems. 88% of break-ins succeeded. Only 4% were detected.

With the Internet, security policy and technology must reflect distributed computing. More entrances equal more risk. Both host-based (network) security and perimeter (firewall) security are essential. Firewalls should deny all access except that explicitly allowed. Similarly, hosts should provide no services except those explicitly intended.

Firewalls may use a "packet inspection" or "proxy" architecture. In packet inspection, the system picks information off at the datalink layer and filters it against a rules table. Depending on compliance, the system may respond by dropping the incoming packet, passing it through, logging it, sending an acknowledgment, and so forth. In a "proxy" design the security application sits at the top of the OSI stack. Proxy architecture works best with specific services (for example, an FTP server, Telnet server, etc.).

The most common firewall implementation is a double-firewall with a DMZ. In this case, two firewalls bracket a DMZ containing a bastion host. The firewalls should be from different manufacturers, so the same holes do not exist in both.

Firewall security may be extended through one-time password authentication, encryption, stealth (non-IP addressable) machines, packet vectoring, and virtual private networks (VPNs). A VPN uses encryption technology to allow an organization to use a public network as a secure pipeline. This can save 23 to 35% in network costs.

Essential to network security is the configuration of the Internet server. This means limiting the server to required services (for example, FTP), employing a tested recovery plan, frequently checking data integrity, and fully monitoring access. When placing data on an Internet server, an organization must think of the whole world as a potential audience, not just its normal clients. Only a read-only copy of the organization’s public information should be accessible.

Methods for Securing Data Transmission

Tal Saraf, Senior Systems Engineer and Internet Technologies Expert, Microsoft Corporation

Interactive Internet sites require secure methods for transferring data and financial transactions. The solutions include encryption and digital signature technology and policy initiatives such as Certificate Authorities and SET.

The new paradigm of the Internet is the "active" interactive page. This increases the risk to users of encountering malicious code (viruses), tampered code, unknown authors and impersonations. Authentication and encryption are the key to secure data transmission, whether code, Email, or financial transactions.

One initiative to ensure data authentication is the Certificate Authority (CA) system. CAs are established organizations that verify a software publisher's identity. To apply for a certificate, a software publisher agrees to meet the CA's policies and submits the public key of its public/private key encryption. The CA publishes the public key and issues an identifying certificate that can be applied to an unlimited amount of code or other electronic items until it expires or is revoked. Verisign was the first CA. GTE, AT&T and the United State Postal Service are in the process of becoming CAs.

By allowing commercial or personal certification and various trust levels, the CA system lets code recipients know the risk level of any item. Automated systems could be designed to accept or reject transmission based on the information specified in a certificate.

As indicated, public/private key encryption plays an important role in authentication. In this form of encryption, a sender uses a private key to encrypt data. The recipient uses the sender's public key. By comparing a hash of the original code with a hash of decrypted code, a recipient can verify data integrity. Encryption is also used for digital signatures. Like a handwritten signature, digital signatures identify a software or data publisher. It guarantees that an item has not been altered from the time it was digitally "signed."

In addition to ensuring secure transmission of code, major financial and software companies (Microsoft, Visa, Mastercard) are designing means to ensure financial transmissions. The SET standard (a merging of STT and SEPP) is a universal comprehensive bankcard payment protocol. SET uses message-based encryption to allow multi-party transactions, multiple transports (Email), and secure interaction.

Methods for Testing the Security Solution

Michael Fogel, Technical Business Unit Manager, State & Local Government, UNIFIED Technologies

Michael Jones, Systems Engineering Manager, UNIFIED Technologies

Security systems should be tested with network and hacker tools. Tests should represent both inside and outside attacks. External attacks may use tools such as SATAN, COPS and CRACK. Inside attacks can take place through modems, infiltration, social engineering, or by authorized users.

Networks should be tested using tools such as SATAN, COPS and CRACK. SATAN (System Administrator's Tool for Analyzing Networks) uses PERL scripts to gather network information. Even a light scan can identify network hardware and operating systems, client and server types, and so forth. Hackers use this information to research known vulnerabilities or to find holes in the configuration. COPS (Computer Oracle and Password System) examines individual computers to discover file directory device permissions, poor passwords, and other security holes. CRACK uses a digital dictionary to break passwords.

A complete security analysis involves defining an organization's current policy, performing an internal audit, performing external testing and generating reports. External testing includes using SATAN and other tools, as well as testing against known vulnerabilities. Case studies demonstrate a wide range of vulnerability between organizations. Some have few security holes; others fail to comply to their own security policy and have numerous holes.

One currently unresolved security issue is firewall certification. A third party such as CERT or NCSC could set up standards; or firewall vendors could create their own. Standards might include testing against known

vulnerabilities, testing with SATAN and other tools, and reviewing firewall/network configuration. An organization would recertify every time its configuration changes. Planned periodic certification would ensure that the firewall meets new threats.

Beyond direct network attacks (addressed by firewalls), attacks may come through modems, through physical infiltration, through social engineering or by authorized users. Social engineering and attacks by authorized users are by far the most common threats. These threats can be addressed by interior firewalls as well as personnel policies and procedures. Note that a true security solution is just part of the network infrastructure. The solution must facilitate use or people will work around it.

Monitoring the System/Preparing for and Responding to a Break-in

Eric Elgar, Private Consultant

To prepare for a break-in, an organization must determine its security goals, the scope of security it needs and the procedures to implement. When a break-in occurs, the organization identifies the problem, notifies the right people, contains the problem, documents the event, and initiates recovery procedures.

To determine security goals, scope and procedures, an organization must first know the value of its own data. Scope must address both staff expectations regarding privacy and access and management's need for security (accountability, authentication, etc.). Procedures should cover auditing, reporting, notification, investigation, and enhancement. Recovery plans must be tested under real-life conditions.

System monitoring requires logging tools such as Netlog and Pinglogger, administrative tools such as Dig and Fping, and Host scanning tools such as COPS, CRACK and SATAN. To analyze networks, network security personnel might use Argus, Arpwatch, Klaxon, etc. Finally, the organization must keep up to date with CERT advisories and vendor information. System monitoring must be done by human operators to be successful.

When a security incident does occur, the organization implements the following steps:

1. **Identification.** Identify the problem. Make sure all activity is being logged. Determine the extent and severity of the attack, then figure out the impact on system resources.
2. **Notification.** Notify the right people, from technical and administrative personnel to users to the public. Have a defined response team to ensure that investigative and legal action starts immediately.
3. **Containment.** Contain the problem. Human safety is the first priority. After that, protect classified and sensitive data, prevent exploitation of other systems, prevent damage to system files, and minimize disruption of the system.
4. **Documentation.** Document all events and evidence on a secure, removable medium. It should be a medium that can be signed and witnessed.
5. **Recovery.** Eradicate the problem. First verify that all possible data about the problem has been collected. After eradicating the problem, audit all facilities, conduct risk analysis, determine enhancements to the system to prevent reoccurrence, and, if possible, start legal prosecution.

