An Overview Of Trends In Network Security and Controls

Kathleen Macina

July 20, 1999

Agenda

- Intrusion Detection Systems
- Trends In Cryptography
- Next Generation Firewalls
- Security and Control Implications of:
  - Intranets
  - Extranets
  - Value Added Networks
  - Virtual Private Networks
- Increasing Security Awareness

Intrusion Detection Systems

Definition:

An Intrusion Detection System (IDS) is a system used to detect unauthorized access to, or usage of, a computer system.

Intrusion Detection Systems

Host-Based and Network-Based Systems

- Host-based systems have IDS software loaded on the system to be monitored.
- Host-based systems verify the integrity of the system's files.
- Network-based systems monitor traffic on a network segment.

Intrusion Detection Systems

Knowledge-Based Systems:

- Applies information about specific attacks and system vulnerabilities.
- Any action not explicitly recognized as an attack is considered legitimate.
- Low false-alarm rate.
- May not detect other real intrusions.

Intrusion Detection Systems

Behavior-Based Systems:

- Utilizes a baseline of expected behavior.
- The baseline is compared with current system activity.
- Unusual activity is considered dangerous.
- Can help detect attempts to exploit new or unforeseen vulnerabilities.
- High false-alarm rate.

Intrusion Detection Systems

The Layered Approach:

- Host-based
- Network-based
- Knowledge-based
- Behavior-based
- Layer network security - Don’t rely on just one component!!!

Cryptography Today

- The United States permits export of encryption products of up to 56 bits without handing over a key to decrypt the data, with few exceptions.

- DES, which has a key length of 56 bits, can be easily broken.

Cracking DES

Type of Attacker	Budget	40-Bit Key Size	56-Bit Key Size
Casual Hacker	$400	5 Hours	38 Years
Small Business	$10,000	12 Minutes	556 Days
Corporate Department	$300,000	24 Seconds	19 Days
Large Company	$10,000,000	7 Seconds	13 Hours
Intelligence Agency	$300,000,000	.0002 Seconds	12 Seconds

Source: Busniess Software Alliance, 1996

Security and Freedom Through Encryption (SAFE)

The SAFE Act has three key components:

- It ensures that all Americans have the right to choose any type of encryption to protect their confidential information.
- It prohibits the government from mandating a back door into people's computer systems.
- It relaxes export controls on U.S. encryption products.

Encryption Trends

- Increasing use of Triple DES
- Development of AES
- The rise of Elliptic Curve Cryptography
- The introduction of RPK
- Development of other public-key encryption schemes

Source: PriceWaterhouse Technology Forecsast - 1998

Triple DES

- No known attacks have succeeded in breaking its two 56-bit keys
- Easily incorporated into existing systems
- Standards-based algorithm
- Requires three times the computing power as DES
- Difficult to manage and distribute keys

Advanced Encryption Standard

- The National Institute of Standards and Technology (NIST) put out an RFC on candidate algorithms for the advanced encryption standard (AES).
- Fifteen candidate algorithms were selected.
- Proposed requirements are that the algorithm be publicly defined and use a symmetric block cipher equal to or stronger than Triple DES, with significantly improved efficiency.

AES Requirements

Security - The security provided by an algorithm is the most important factor in the evaluation. It includes the actual security of the algorithm compared to other submitted algorithms, soundness of the mathematical basis for the algorithm's security, and other security factors raised by the public.

AES Requirements

Cost - NIST intends that when the AES is issued, the algorithm(s) specified in the AES shall be available on a worldwide, non-exclusive, royalty-free basis. Cost also includes computational efficiency (the speed of the algorithm) and memory requirements (the memory required to implement a candidate algorithm).

AES Requirements

Flexibility - Candidate algorithms with greater flexibility will meet the needs of more users than less flexible ones. Examples include:

- The algorithm can accommodate additional key- and block-sizes,
- The algorithm can be implemented securely and efficiently in a wide variety of platforms and applications,
- Hardware and software suitability (a candidate algorithm shall not be restrictive in the sense that it can only be implemented in hardware. If one can also implement the algorithm efficiently in firmware, then this will be an advantage in the area of flexibility.)

AES Requirements

Simplicity - A candidate algorithm shall be judged according to relative simplicity of design.

Elliptic Curve Cryptography

- Based on the same algorithm as Diffie-Hellman but uses a different method for calculations.
- Claim is that a 160-bit ECC key provides the same security as a 1,024-bit RSA key.
- Fatal security flaw discovered in a group of elliptic curves previously accepted for cryptographic implementation.
- Work is on-going.

RPK

- Developed in New Zealand in 1995
- Free public-key cryptosystem
- Faster than other public-key systems
- Easily implemented in hardware and software
- Not subject to U.S. cryptography restrictions

Cryptography Development Efforts

- Many companies are continuing research and development with public-key encryption
- IBM is working on a new encryption scheme that uses the mathematical “unique shortest vector” approach to generate keys randomly. This approach proves that all chosen keys are equally strong. The system still requires significant development.

Certificate Authorities

Digital Certificate - A software file that functions as an electronic credential. It identifies the certificate owner, authenticates the certificate owner's membership in a given organization or community, and establishes the certificate owner's access authority.

Certificate Authorities

Certificate Authorities (CA) - A trusted third-party or organization that issues digital certificates. The CA embeds the digital certificate owner's public key in the digital certificate, which is then cryptographically "signed" by the CA. The CA's signature verifies the integrity of the information within the digital certificate and validates its use with a specific organization or community.

Certificate Authority Trends

- Major government and corporate organizations will establish themselves as certificate authorities, mainly led by banks and financial institutions (in the U.S.).
- The lack of product interoperability and established processes to authenticate CAs and relieve users of liability will limit acceptance in the near term.
- Standards are still being developed.

Next Generation Firewalls

- Overlap of firewalls with other security measures such as encrypted VPNs
- Firewall functionality making its way into other network components
- Firewall services will be unbundled, allowing users to pick features they want.
- Firewall appliances becoming more popular

Next Generation Firewalls

- Real-time intrusion detection
- Decrease in use of ActiveX for applications that must operate over the Internet
- Applet monitoring due to increased use of Java
- Virus scanning
- Encryption

Intranets

- Private network that uses Internet software and TCP/IP protocols.
- Use is increasing, with many powered by internal Web servers.
- Security is often overlooked.
- Use will continue to expand due to open protocols, widely available products, and ease of use.

Extranets

- Private WANs that are accessible to business partners and customers.
- Growth facilitates electronic commerce.
- Middle-man can be eliminated.
- Use will continue to expand due to open protocols, widely available products, and ease of use.
- Due to competitive advantages, more organizations will implement extranets.

Extranets

- Business partners will have access to the internal network
- Access may be too extensive
- Need to protect the internal network
- Document all external connections
- Implement firewalls
- Limit the ability to move around the network
- Set-up audit logs and monitor the logs

Value Added Networks

- Facilitates one-stop shopping by providing the software, network, platform, and components such as payment, billing, and security.
  - Rely on VAN vendor to set-up security properly.
- Companies moving from VANs to leased lines and the Internet.
- Vendors offering new services have good growth prospects. They need to add new value to Web services and transaction processing over the Internet.

Virtual Private Networks

- Private network configured within a public network.
- Save approximately 50% over leased-line methods.
- Vendors are reporting record revenue from VPN components and are anticipating further growth.
  - Infonetics reported Q1 ‘99 revenue of $38M from VPN gateway equipment, doubling Q1 ‘98 results. Anticipated Q4 ‘99 revenue is $158M.

Virtual Private Networks

- Wireless ISPs are gaining popularity in the VPN market due to increased performance of bandwidth-intensive data packets
  - Easier to intercept transmissions
- Moving encryption from software to hardware to increase performance
- Interoperability is an issue since VPNs are new technology

Increasing Security Awareness

- Why is it needed?
  - Increasing number of companies utilizing the Internet
  - Public awareness of “hackers”
  - Security problems in the news

- What is being done?
  - Employee education and participation is critical
  - Security policies as a part of new employee orientation
  - Formal security awareness programs
  - Reminder notices

Q & A

Thanks for attending!!!