Overview of Network Security and Its Related Trends

Kadambari Raghuram
IV CSE
Scsrmv University, Enathur-Kanchipuram
Kadambari.raghuram143@gmail.com

ABSTRACT
Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become “wired”, an increasing number of people need to understand the basics of security in a networked world. Cryptography is also one of the methods of network security; it plays a major role in securing the data from others which might be open. This paper briefly describes various security strategies that can be implemented, and the security measures that have to be taken in all the enterprises. To provide a better security environment to the users of the enterprise networks, security administrators have to follow the defence in depth policy and implement multiple redundant security measures suggested. It is emphasized that the security threats will increase with time along with increased dependency on the enterprise networks and Internet. However, a sound security policy and a defence in depth security implementation will provide the needed security confidence to continue the utilization of enterprise networks for all important applications.

KEYWORDS

November 2nd 1988?
Something interesting happened on this date
Any ideas?
Internet Worm Launched
Moved relentlessly across network connections from computer-to-computer
Within 12 hours, first Berkeley Univ then Purdue Univ distributed patches to stop spread.
Computers affected 2,000-3,000 maybe more
Even those computers not affected had to be tested!
Cost? Estimated between $1M and $100M. A great deal of time and resources expended.

Who did it?

Robert T Morris Jr. (Student at Cornell Univ.)

CLAIMED IT WAS AN EXPERIMENTAL PROGRAM THAT HAD A BUG :-)
2yrs later -> 3yr probation, $10K fine, 400 hours community service.

1.INTRODUCTION
In the field of networking, the specialist area of network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

Why do we need for Security
✦ 70% of all security violations happen from within an organization.
✦ Of that 70%, most “attacks” are not attacks. People make honest mistakes that cause bad things to happen.
✦ Of outside attacks, targets are normally unknown to the attacker.
✦ Most administrators are oblivious to the number of attacks that are attempted each day.

Security Services:
Authentication - assurance that the communicating entity is the one claimed
Access Control - prevention of the unauthorized use of a resource
Data Confidentiality - protection of data from unauthorized disclosure
Data Integrity - assurance that data received is as sent by an authorized entity
Non-Repudiation - protection against denial by one of the parties in a communication
Security Mechanisms (X.800)
Specific security mechanisms: Encipherment, digital signatures, access controls, data integrity,
authentication exchange, traffic padding, routing control, notarization
Pervasive security mechanisms: trusted functionality, security labels, event detection, security audit trails, security recovery
Types of Attacks

![Diagram of Active and Passive Threats]

Classify Security Attacks
Passive attacks - eavesdropping on, or monitoring of, transmissions to:
Obtain message contents, or
Monitor traffic flows
Active attacks – modification of data stream to:
Masquerade of one entity as some other
Replay previous messages
Modify messages in transit
Denial of service
What is network security?

Confidentiality:
Only sender, intended receiver should
“Understand” message contents
-- sender encrypts message
-- receiver decrypts message
Authentication:
Sender, receiver wants to confirm identity of each other
Message Integrity:
Sender, receivers want to ensure message not altered
(In transit, or afterwards) without detection
Access and Availability:
Services must be accessible and available to users

Cryptography
Cryptography means
Kryptos (hidden) + graphein (to write) = secret writing

It is used for:
-- Conceal messages from unauthorized persons (secrecy + privacy)
-- Verify correctness of message (authentication)
-- Authenticate to other party

- Conventional Encryption (or) Symmetric Encryption:
- Transformation of Plain-Text is encrypted into Cipher-text and that can be decrypt from Cipher-text to Plain-Text with the same key “K”.

Steganography
Used for concealing information inside other information
Some techniques:
-- Character marking: selected letter of printed or typewritten text are overwritten in pencil
-- Invisible ink
-- Pin punctures: small pin punctures are only shown if paper is hold against a light source
-- Typewriter correction ribbon: used between lines of normal black ribbon. Only visible under strong light

Conventional Encryption Techniques
There are three important encryption techniques now in use:
Symmetric or private key encryption
Asymmetric or public key encryption
Digital signatures, which are based on a variation of public key encryption.

Data Encryption Standard (DES)
DES is a symmetric encryption algorithm developed by IBM and maintained by the National Institute of Standards and Technology.
A 56-bit version of DES is commonly used, but can be broken by brute force.
Other symmetric encryption techniques include:
-- RC4 uses a 40 bit key, but can use up to 256 bits.
-- Triple DES (3DES) uses DES three times, effectively giving it a 168 bit key.
-- Advanced Encryption Standard (AES), designed to replace DES uses 128, 192 and 256 bit keys.

Data Encryption Algorithms
Public-Key Cryptography
A Model for Public-Key Cryptography
Public-key Cryptosystems
Message Authentication Code (MAC)
Public-Key Authority

Digital Signatures
PKE also permits authentication (digital signatures), which essentially uses PKE in reverse. The digital signature is a small part of the message, and includes the name of the sender and other key contents. The digital signature in the outgoing message is encrypted using the sender’s private key. The digital signature is then decrypted using the sender’s public key thus providing evidence that the message originated from the sender. Digital signatures and public key encryption combine to provide secure and authenticated message transmission.

Authentication – Passwords
Most hosts use passwords to authenticate users and the technique can be extended to other uses. Traditionally (at least on UNIX) passwords have been encrypted. Once a network is involved, the problem becomes much more complex. Also widened to more general problems, e.g. one user authenticating another user.

Row Transposition Ciphers
A more complex scheme
Write letters of message out in rows over a specified number of columns then reorder the columns according to some key before reading off the rows

Key: 3 4 2 1 5 6 7
Plaintext: a t t a c k p o s t p o n e d u n t i l w o a m x y z
Cipher text: TTNAAPTMTSUOADWCOIXKNLYPETZ

Key Distribution Issues
Hierarchies of KDC’s required for large networks, but must trust each other
Session key lifetimes should be limited for greater security
Use of automatic key distribution on behalf of users, but must trust system
Use of decentralized key distribution
Controlling purposes keys are used for

Key Management
Public-key encryption helps address key distribution problems
Have two aspects of this:
– distribution of public keys
– use of public-key encryption to distribute secret keys

Public-Key Cryptography
Probably most significant advance in the 3000 year history of cryptography
Uses two keys – a public & a private key
Asymmetric since parties are not equal
Uses clever application of number theoretic concepts to function
Complements rather than replaces private key crypto
Public-key/two-key/asymmetric cryptography involves the use of two keys:
a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
a private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
Is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Private-Key Cryptography
Traditional private/secret/single key cryptography uses one key
Shared by both sender and receiver
If this key is disclosed communications are compromised
Also is symmetric, parties are equal
Hence does not protect sender from receiver forging a message & claiming is sent by sender

2. SECURITY ISSUES
External protection of a system. A classified site goes to extraordinary lengths to keep things physically tight. Among the issues to be considered:

Unauthorized access Mechanism assuring only authorized individuals see classified materials.
Malicious modification or destruction
Accidental Introduction of inconsistency.
Authentication How do we know the user is who she Says she is? Can have passwords on domains.
Protection of passwords, Trojan horse, Trap Doors, Threat monitoring, Audit Log, InternetWorm, Viruses, and Firewall:
. What is a Firewall?
. A choke point of control and monitoring
. Interconnects networks with differing trust
. Imposes restrictions on network services
. only authorized traffic is allowed
.Auditing and controlling access
. can implement alarms for abnormal behavior
Is itself immune to penetration?
Provides perimeter defence
Firewalls – Packet Filters

Firewalls – Packet Filters
. simplest of components
. foundation of any firewall system
. examine each IP packet (no context) and permit or deny according to rules
. hence restrict access to services (ports)
. possible default policies
. that not expressly permitted is prohibited
. that not expressly prohibited is permitted

Firewall Configurations

Security management
Security Management for networks is different for all kinds Of situations.
A small home or an office would only require basic security
While large businesses will require high maintenance and Advanced software and hardware to prevent malicious Attacks from hacking and spamming.

Applications:
Small homes
Medium businesses
Large Businesses
School & colleges
Large Government

Why testing security
. Get a snapshot of the current security
. Evaluate the capacity to face intrusion
. Test backup plan

SCOPE

Results:
Overview of Network Security and Its Related Trends

- Results  Date /type
- Duration
- Auditor and analyst associated
- Test type
- Scope
- Test index
- Channel test
- Test vector
- Verified test and metrics calculations of the operational protection levels, loss controls, and security limitations
- Knowledge of which tests have been completed, not completed, or only partially completed, and to what extent
- Any issues regarding the test and the validity of the results
- Test error margins
- Any processes which influence the security limitations
- Any unknowns or anomalies

3. SCOPE

Security Test Type

Network techniques toolbox
- Network scouting
- Os fingerprinting
- Vulnerability scanner
- Network trace analysis

Why scouting is important?
- Scouting is the first step
- You can’t attack what you don’t know

Scouting Process overview

Top Network Security Tools
After the tremendously successful 2000 and 2003 security tools surveys, Insecure.Org is delighted to release this 2006 survey. I (Fyodor) asked users from the nmap-hackers mailing list to share their favorite tools, and 3,243 people responded. This allowed me to expand the list to 100 tools, and even subdivide them into categories. Anyone in the security field would be well advised to go over the list and investigate tools they are unfamiliar with. I discovered several powerful new tools this way. I also point newbies to this site whenever they write me saying “I don’t know where to start”. Respondents were allowed to list open source or commercial tools on any platform. Commercial tools are noted as such in the list below. No votes for the Nmap Security Scanner were counted because the survey was taken on a Nmap mailing list. This audience also biases the list slightly toward “attack” hacking tools rather than defensive ones.

Each tool is described by one or more attributes:

- Did not appear on the 2003 list
- Popularity ranking rose / fell the given number since the 2003 survey
- Generally costs money. A free limited/demo/trial version may be available.
- Works natively on Linux
- Works natively on OpenBSD, FreeBSD, Solaris, and/or other UNIX variants
- Works natively on Apple Mac OS X
Works natively on Microsoft Windows
Features a command-line interface
Offers a GUI (point and click) interface
Source code available for inspection.

Please send updates and suggestions (or better tool logos) to Fyodor. If your tool is featured or you think your site visitors might enjoy this list, you are welcome to use our link banners. Here is the list, starting with the most popular:

#1 Nessus: Premier UNIX vulnerability assessment tool
Nessus was a popular free and open source vulnerability scanner until they closed the source code in 2005 and removed the free "registered feed" version in 2008. A limited "Home Feed" is still available, though it is only licensed for home network use. Some people avoid paying by violating the "Home Feed" license, or by avoiding feeds entirely and using just the plugins included with each release. But for most users, the cost has increased from free to $1200/year. Despite this, Nessus is still the best UNIX vulnerability scanner available and among the best to run on Windows. Nessus is constantly updated, with more than 20,000 plugins. Key features include remote and local (authenticated) security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plugins or understanding the existing ones.

See all vulnerability scanners

- #5 Aircrack: Aircrack-ng
  The fastest wireless available tools, WEP/WPA cracking tool
  Aircrack is a suite of tools crackers for 802.11a/b/g WEP and WPA cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force. The suite includes air dump (an 802.11 packet capture program), airplay (an 802.11 packet injection program), air crack (static WEP and WPA-PSK cracking), and airdecap (decrypts WEP/WPA capture files).

The Future of Network Security: How security platforms will transform networking

DOE, Lawrence Livermore National Laboratory

“Fortinet’s ASIC-based Unified Threat management solutions provide Lawrence Livermore National Laboratory with line rate performance and protection from attacks not picked up by traditional point products – all with a dramatically reduced operational cost.”

-Arien Seghetti
Security Network Engineer
FORTINET

A new concept: Secure Networks

- No bad traffic. No viruses, no worms, no spam, no attacks, no bad guys, no inappropriate use.
Overview of Network Security and Its Related Trends

- At the carrier level: Clean Pipes, a competitive advantage
- At the enterprise level: no worm or virus spread through the network, no unauthorized access to resources.
- At the remote office: simple device set and forget.

Lessons learned from the Pentagon

FORTINET

CONCLUSION

Information security is increasingly important

Have varying degrees of sensitivity of information
  - Of military info classifications: confidential, secret etc
Subjects (people or programs) have varying rights of access to objects (information)
want to consider ways of increasing confidence in systems to enforce these rights
Known as multilevel security
  - subjects have maximum & current security level
  - objects have a fixed security level classification

The computers and communication technology will continue to advance at a rapid pace. More and more enterprises use computers, networks and Internet for all their possible activities. Hence, the security risk can never be eliminated at regular intervals about the hacking and breaking in of some of the "secured sites". Still, there is nothing to get paranoid. The use and misuse of internet, the security mechanisms have changed a lot over the years and the trend will continue. The security administrators have to keep updating the technology and products to protect their sites. It shall be a continuing process to achieve higher level of security.

REFERENCES