Network Management & Security

Edward Cheung
email: icec@polyu.edu.hk
18 July, 2003.

Agenda

- Network Management
  - Network management software
  - Clients, servers, managers and agents
  - Simple Network Management Protocol
- Network Security
  - Integrity mechanisms
  - Access control and password
  - Encryption and privacy
  - Public and private key with examples
  - Digital signatures
  - Packet filtering
  - Basic Internet firewall concept
- Recent development and future trends of data communication and networking

Network Management

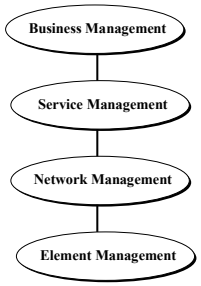
- Any complex systems requires monitoring and control this included autonomous systems or computer network.
- Network Management involved the deployment, integration and coordination of devices to monitor, test, poll, configure, analyze, evaluate, and control the network and its components.
- The objective of network management is to meet the requirements of a network which including availability, real-time, operational performance, and Quality of Service at a reasonable cost.
- But network is heterogeneous. Devices need standards to communicate and exchange data.

ISO Network Management Model

- Five areas of Network Management are defined
  - Performance Management
    - The goal is to quantify, measure, report, analyse and control the utilization or throughput of different network components
      - RFC2570 Internet-standard Network Management Framework
  - Fault Management
    - The goal is to log, detect, and respond to fault conditions in the network.
  - Configuration Management
    - The goal is to allow network manager to track which devices are on and their hardware and software configurations.
      - RFC3139 Requirements for Configuration Management of IP-based Networks
  - Accounting Management
    - Usage quotas, usage charging, allocation of resources and privileges.
  - Security Management
    - Control access to network resources according to a security policy.

Network Management Standards

- Common Management Information Protocol (CMIP)
  - OSI based management protocol
  - object oriented – complex, not popular and requires large memory
  - becomes the Telecommunication Management Network (TMN) for telecom service providers,
  - ITU-T M series recommendation defines the architecture and functions of TMN and a tutorial is available in M.3000
  - TMN includes services and business functions.
    - http://www.tmforum.org



TMN Logical Layered Architecture

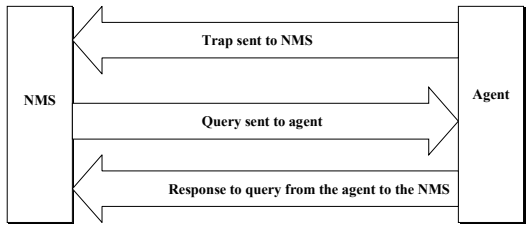
Network Management Standards

- Simple Network Management Protocol (SNMP)
- Develop on client server concept
- polling based system
- de facto network management standard
- currently SNMPv3
- platform independence
  - Web based management
  - Use ASN.1 Syntax
- By default SNMP uses UDP port 161 for sending and receiving requests and port 162 for receiving traps from managed devices.

Managers and Agents

- manager is a server running some kind of software system that can handle management tasks for a network. Managers are also known as *Network Management Stations* (NMSs). Managers use *polling* to query network information.
- A NMS is responsible for polling and receiving traps from agents in the network. the *agent*, is a piece of software that runs on the network devices that are being managed. It can be a separate program or a part of the operating system (e.g. Cisco's IOS on a router, or the OS of an UPS). A *trap* is a way for the agent to tell the NMS that something has happened. Traps are sent asynchronously
- polls and traps can happen at the same time.
- Today, many network devices come with SNMP agent built in.

SNMP Organization Model



SNMP Overview

- Management Information Base (MIB)
  - Store of network information data
- Structure of Management Information (SMI)
  - Data definition language for MIB objects
- SNMP protocol
  - Communication protocol, commands
- Security, administration capabilities
  - SNMPv3 addressed the security and provide a framework for all versions of SNMP

Different SNMP Versions

- *SNMP Version 1* (SNMPv1) - RFC 1157
- *SNMP Version 2* (SNMPv2) is often referred to as community string-based SNMPv2. This version of SNMP is also known as SNMPv2c.
  - RFC 1905, RFC 1906, and RFC 1907
  - A large installation base
- *SNMP Version 3* (SNMPv3)
  - current version
  - RFC 1905, RFC 1906, RFC 1907, RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.
  - It adds support for strong authentication and private communication between managed entities.
- The official site for RFCs is http://www.ietf.org/rfc.html.
- Alternatively - RFC index at Ohio State University http://www.cis.ohio-state.edu/services/rfc/index.html

SNMPv1

- SNMPv1's security is based on *communities.* The community names are essentially simple passwords.
- plain-text strings that allow any SNMP-based application that knows the strings to gain access to a device's management information.
- Typically, there are three communities in SNMPv1: *read-only*, *read-write*, and *trap*.
- SNMPv1 and SNMPv2 use the notion of communities to establish trust between managers and agents.
- An agent is configured with three community names: read-only, read-write, and trap.
- Most vendors ship their equipment with default community strings:-
  - *public* for the read-only community
  - *private* for the read-write community
  - It's important to change these defaults before the device is connected to the network.

SNMP Security Models and Security Levels

SNMP version	Security Level	Authentication	Encryption	Process
v1	No A/P	Community String	No	Use a Community string matching for authentication
v2/v2c	No A/P	Community String	No	
v3	No A/P	Username	No	Use an username matching for auth.
	A and No P	MD5 or SHA	No	Use Hash-based Message Authentication Code.
	A and P	MD5 or SHA	DES	Packet authentication with 56-bit DES encryption

A=Authentication, P=Privacy

SMI & MIB

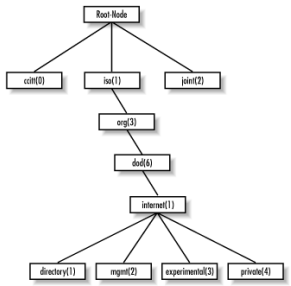
- *Structure of Management Information* (SMI) provides a way to define managed objects and their behavior. SMI is the data definition language for SNMP, it provides a way to define managed objects (MIB).
- MIB is the definition (in SMI syntax) of the objects. It is more vendor specific. (*MIB-II*, RFC 1213). The agent delivers information from the MIB or changes it under the direction of a remote manager.
- Every managed resources has a MIB which contains exposed interface; e.g. a server MIB contains information on CPU, memory system and a router MIB contains interface information such as speed of protocol on interfaces.

SMI

- The *Structure of Management Information Version 1*(SMIv1, RFC 1155) & *Version 2* (SMIv2, RFC 2578)
- SMI defines precisely how managed objects are named and specifies their associated datatypes.
- definition of managed objects can be broken down into three attributes:
  - **Name**
    - The name, or *object identifier*(OID), uniquely defines a managed object.
  - **Type and syntax**
    - A managed object's datatype is defined using a subset of *Abstract Syntax Notation One*(ASN.1). ASN.1 notation is machine-independent. Standardized by ITU-T.
  - **Encoding**
    - A single instance of a managed object is encoded into a string of octets using the *Basic Encoding Rules*(BER).

The SMI Object Tree

- Managed objects are organized into a tree-like hierarchy. This structure is the basis for SNMP's naming scheme. An object ID is made up of a series of integers based on the nodes in the tree, separated by dots (.).
- *Root node*
- *Subtree node*
- *Leaf node*



The SMI Object Tree

- The *ITU-T* subtree is administered by ITU-T and the *joint* subtree is administered jointly by ISO ITU-T, the *iso(1).org(3).dod(6).internet(1)* subtree is for SNMP and it is represented in OID form as *1.3.6.1* or *iso.org.dod.internet*.
- E.g. Cisco Systems's private enterprise number is 9, so the base OID for its private object space is defined as iso.org.dod.internet.private.enterprises.cisco, or 1.3.6.1.4.1.9. The owner of the upper node is free to do as it wishes with this private branch.
- Each managed object has a numerical OID in dotted-decimal notation and an associated textual name.
  - http://www.iana.org/assignments/smi-numbers

RMON

- Remote Monitoring Version 1 (RMONv1, or RMON) – current version RFC 2819
- Initially defined for Ethernet
  - provides the NMS with packet-level statistics about an entire LAN or WAN
- RMON Version 2 (RMONv2) - RFC 2021
  - builds on RMONv1 and allow the monitoring of network and application layers statistics.
  - Using SMIv2
- RMON is a standard MIB that allows the capturing of real-time information across the network.

Example – Free Network Traffic Grapher MRTG

- The *Multi Router Traffic Grapher* (MRTG) is a freely available, popular and fully configurable trend-analysis tool.
  - http://www.mrtg.org
- It generates graphs in the form of GIF or PNG images that can be embedded and browsed with web pages.
- MRTG is not an NMS solution
- It is a simple polling engine.
- No detection and resolution function.
- Open source NMS package,
  - http://www.opennms.org
- By default, MRTG will generate the following graphs:
  - Daily graph with 5-minute averages
  - Weekly graph with 30-minute averages
  - Monthly graph with 2-hour averages
  - Yearly graph with 1-day averages

Examples of Network Management Software

- CA UniCenter TNG
  - http://www3.ca.com/Solutions/Solution.asp?id=315
- HP Openview
  - http://www.openview.hp.com/
- IBM Tivoli
  - http://www.tivoli.com/
- OpenNMS
  - http://www.opennms.org/users/downloads/

Network Management Tools

- Hardware
  - Bit Error Rate Tester (BERT)
  - Protocol / Network Analyzer
  - NMS & RMON probes
- Software
- OS dependent, common commands available on Microsoft system are:-
  - nbtstat
  - ifconfig
  - ping
  - nslookup
  - netstat
  - tracert

Network Security

ITU-T recommendation X.800, Security Architecture for OSI divided security services into 5 catagories.

- **Authentication** - ensure the communicating entity is the one claimed
- **Access Control** - preventing unauthorized use of resources
- **Data Confidentiality** –protecting data from unauthorized disclosure and only the entities such as the sender and the intended receiver should understand the message contents.
- **Data Integrity** – ensure that the message has not been altered or destroyed without detection or warning
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Classification of 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

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- However, there is one particular element that underlies many of the security mechanisms in use: **cryptographic techniques.**

Authentication, Access Control and Password

- *Authentication* establishes the identity of the sender and/or the receiver of information. Any integrity check or confidential information is often meaningless if the identity of the sending or receiving party is not properly established.
  - the process of validating the claimed identity
- Authorization establishes what is allowed to do after the user has identified oneself
  - also known as *access control* or *permissions*
  - the process of granting access rights to user
  - Authorization usually follows an authentication procedure
- *access control* limiting the flow of information from the resources of a system to only the authorized users or systems in the network

Stream Ciphers

Stream cipher algorithms process plaintext to produce a stream of ***cipher text***. It is a substitution cipher.

The cipher inputs the plaintext in a stream and outputs of cipher text.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	a	b	c	d	e	f	g	h	i	j	5	6	7	8	k	l	m	n	o	p	q	r

e.g. One-time pad, RC4

Problem with Stream Ciphers

- Patterns in the plaintext are reflected in the ciphertext. This make guessing easy because certain words and letters of the alphabet appear in predictable regularity. The most commonly used letters of the alphabet in the English language are e, t, a, o, n and I; least commonly used letters are j, k, x. q and z; common combination is “th”, etc..
- One example of the stream cipher is the one-time pad. This is an unbreakable cipher.
- This can done by taking a random bit string as the key and compute the XOR of the plaintext and the key, bit by bit. The total amount of data to be transmitted is limited by the length of the key.
- Both parties must carry a copy of key and the plaintext is beyond recovery on the event of loss synchronization.

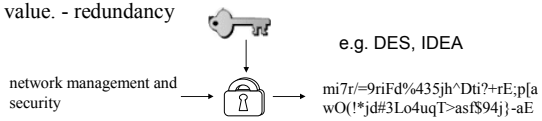
Block Ciphers

Block ciphers differ form stream ciphers in that they encrypt and decrypt information in fixed size blocks.

A block cipher passes a block of data or plaintext through its algorithm to generate a block of cipher text.

A block cipher should generate cipher text roughly equivalent in size (in term of number of blocks) to the clear text.

A cipher that generates a block of cipher text that is significantly larger that information it is trying to protect is of little practical value. - redundancy



Breaking Ciphers

- Cryptology
  - Involve devising ciphers (cryptography) and breaking them (cryptanalysis).
- Cryptanalysis
  - The art of breaking ciphers is called cryptanalysis.
  - This method requires a high level of skill and sophistication.
  - It relies very heavily on the use of ultra-fast super computer.
- Brute Force
  - This method tries every possible combination of keys or algorithms to break a cipher.
  - It require tremendous resources and computer assistance.

Breaking Ciphers

The cryptanalysis problem has 3 stages depending on what information the hacker has:-

- Ciphertext-only
- Known-plaintext
- Chosen-plaintext

Ciphertext-only Attack

- The hacker only have access to the intercepted ciphertext, without information on the contents of the plaintext message. In this case, the hacker can use statistical analysis to help in cracking the cipher. For example, knowing the letters "e" and "t" are the most frequently occurring letters in typical English text; 13% & 9% respectively and the combination of 2-letter and 3-letter occurrences of letters such as "in", "ing", etc.

Breaking Ciphers

- Known-plaintext Attack
  - This method relies on the code breaker knowing in advance the plaintext content of a cipher text message. For example, the hacker may known the name of the sender and the receiver or previous has intercepted one of the plaintext message sent by Alice to Bob. The hacker knows some of the plaintext-ciphertext pairings and he can break the code more easily.
- Chosen Plaintext Attack
  - This method relies on the ability of the hacker to choose the plaintext message and obtain its corresponding ciphertext form. For example, the hacker may ask Alice to send the message "The quick brown fox jumps over the lazy dog." For more sophisticated encryption techniques, a chosen-plaintext attack does not necessarily mean that the encryption technique can be broken.

Encryption

Encryption is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized people.

Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Encryption is the process of scrambling the contents of a file or message to make it unintelligible to anyone not in possession of the "***key***" required to unscramble the file or message.

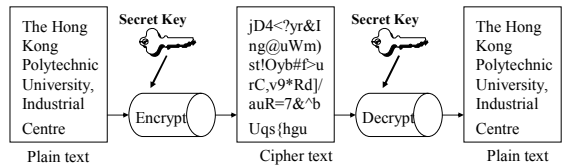
There are two types of encryption:

- Symmetric (private) key, and
- Asymmetric (public) key encryption.

Symmetric Key Encryption

Symmetric key, also referred to as private key or secret key, is based on a single key and algorithm being shared between the parties who are exchanging encrypted.

The same private key both encrypts and decrypts message.



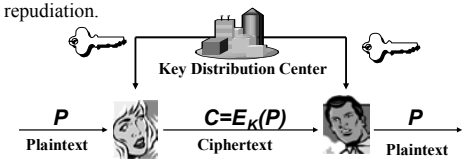
Symmetric Key Encryption

Advantages:

- If the key is larger, the more secure the scheme
- Symmetric key encryption is fast.

Disadvantages:

- The system key or algorithm has to be shared.
- Private key cryptosystems are not well suited for spontaneous communication over an unsecured network.
- Symmetric key provide no process for authentication or non-repudiation.



Symmetric Key Cryptosystems

Example of widely deployed symmetric key cryptosystems include **DES**, **IDEA**, **CAST** and **RC4**.

- **Data Encryption Standard (DES)**
  - DES is one of the oldest and most widely used algorithms.
  - DES consists of an algorithm and a key.
  - The key is a sequence of eight bytes, each containing eight bits for a 64-bits key.
  - Actually, the key is 56 bits in length, since each byte contains one parity bit.
  - DES is widely used in automated teller machine (ATM) and point-of-sale (POS) network.

Advanced Encryption Standard (AES)

- DES is published in 1977 and updated in 1993 by NIST
- For commercial and nonclassified US government use
- DES encodes plaintext in 64-bit chunks using 64-bit key; a block cipher.
- How well does DES work? How secure it is?
  - No one knows for sure.
  - RSA launched an annual DES Challenge in 1997 to crack a short phase it had encrypted using 56-bit DES. The winning teams took 4 months in 1997 and 22 hours in 1999.
- One can increase the strength of the cipher by more iterations; 3DES.
- PPP protocol (RFC2420) use 3DES at the data link layer.
- NIST in 2001 announced AES to replace DES.
- AES is a symmetric key algorithm that processes data in 128-bit blocks and can operate with keys that are 128-bit, 192-bit and 256-bit in length.
- NIST estimated that a machine that could crack 56-bit DES in 1 second would take 149 trillion years to crack a 128-bit AES key.

IDEA & CAST

- **International Data Encryption Algorithm (IDEA)**
  - IDEA is a symmetric key block cipher.
  - IDEA utilizes a 128-bit key.
  - It is efficient to implement in software than DES and triple DES.
- **CAST (Carlisle Adams and Strafford Travares)**
  - THE CAST algorithm supports variable key lengths, anywhere from 40 bits to 256 bits in length.
  - CAST used a 64-bit block size as same as the DES, making it suitable drop-in replacement.
  - CAST is 9 times faster than 3DES and use in PGP.

More on Symmetric Key Ciphers

- **Rivest Cipher #4 (RC4)**
  - RC4 is a stream cipher that uses a variable size key.
  - Used with 128 bits it can be very effective.
  - Use in Internet Explorer and Netscape.

The Advantages and Disadvantages of Symmetric Key Cryptography

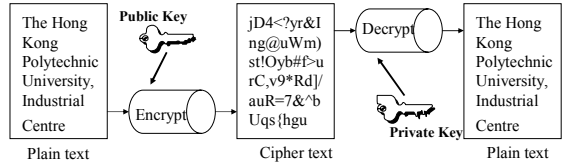
Advantages	Disadvantages
Fast	Requires secret sharing
Relatively secure	Complex administration
Widely understood	No authentication / nonrepudiation

Asymmetric Key Encryption

Asymmetric cryptosystem is also know as ***public key cryptography.***

Public key cryptography used ***two key*** as opposed to one key for a symmetric system.

There is a **public key** and a **private key**.



Asymmetric Key Encryption

Each user has a private key that decrypted only the message that were encrypted by its public key.

- The private key is kept secret
- All public keys are published in a directory.

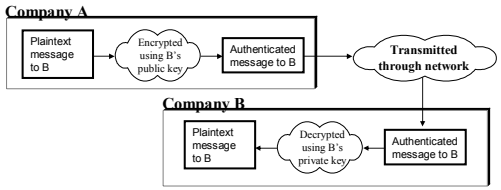


Figure: Secure transmission with public key encryption

Asymmetric Key Encryption

Asymmetric or public key cryptography is more versatile.

Public key allows for secure spontaneous communication over an open network, it is more scalable for large system.

The Advantages and Disadvantages of Public Key Cryptography

Advantages	Disadvantages
No secret sharing necessary	Slower or computationally intensive
Authentication supported	Certificate authority required
Provides non-repudiation	
Scable	

Rivest, Shamir, Adelman (RSA)

The RSA algorithm multiplies large prime numbers together to generate keys. It is extremely difficult to factor the product of large prime numbers.

Public Key:

n product of two primes, p and q
n = p*q

e relatively prime to (p-1)(q-1)
ed = 1 mod(p-1)(q-1)

Private Key:

d = e^{-1} mod [(p-1)(q-1)]

Encrypting:

c = m^{e} mod n

Decrypting:

m = c^{d} mod n

- p and q are two random prime numbers, and must remain secret
- e is encryption key
- d is decryption key
- c is the encrypted message
- m is decrypted message

RSA

- The security of RSA relies on the fact that there are no known algorithm for quickly factoring a number and since it is not known whether or not the algorithm exist, hence the security of RSA is not guaranteed.
- The exponentiation required by RSA is a rather time-consuming process. DES is at least 100 faster in software and between 1,000 and 10,000 times faster in hardware.
- In practise, RSA is often used with DES or AES.
- For example, Alice may choose a DES key to encode large amount of data, known as the session key. Alice than encode the session key using Bob's public key. Then Bob decrypts the message and obtain the session key using his private key. Bob can then use the session key to decrypt the large amount of data.

Authentication

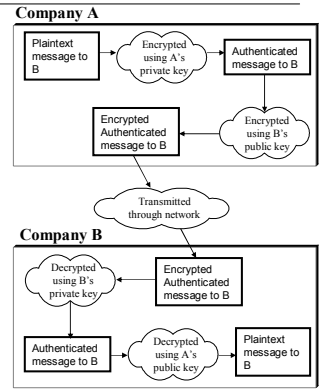
Authentication in a digital setting is process whereby the receiver of a message can be confident of the identity of the sender.

The lack of secure authentication has been a major obstacle in achieving widespread use of the Internet for commerce.

One process used to authenticate the identity of individual or entity involves digital signatures.

Authentication

The figure illustrates how authentication can be combined with public encryption to provide a secure and authenticated transmission.



Digital Signature

- A digital signature allows a receiver to authenticate the identity of the sender and to verify the integrity of the message.
- 3 requirements
  - Verifiable
  - Nonforgeable
  - Nonrepudiable
- This can be easily done by using techniques of public key cryptography.
- The problem is that the process of signing is slow; costly.
- A more efficient approach is to use message digest.

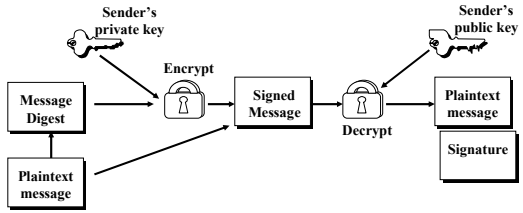
Digital Signature & Message Digest

- 2 goals
  - The sender of the data is as claimed. The sender has signed the data and this signature can be checked.
  - The transmitted data has not been changed since the sender created and signed the data
- Message digest (MD) is like a checksum; take a message of arbitrary length and computer a fixed-length fingerprint of the data known as a message digest.
- The protection is that if the message has been changed, the message digest for the original message must be different.
- Alice can just sign the MD with her private key.

Hash Function

- A hash function takes a message of any length and computes a product value of fixed length. The product is referred to as a "hash value".
- Hash functions are used to ensure the integrity of a message or file.
- The hash value is the cyptographic checksum of the message and offer refer to as the fingerprint of a message.
- Hash function must be one way only.
- Building blocks of message authentication codes
- Popular implementations are MD5 (128-bit) and SHA (160-bit)

Digital Signature



To sign a message, senders append their digital signature to the end of a message and encrypt it using the recipient public key.

Recipients decrypt the message using their owe private key and verify the sender's identity and the message integrity by decrypting the sender's digital signature using the sender's public key

Digital Certificate

A **digital certificate** issued by a **certification authority (CA)** utilizing a hierarchical **public key infrastructure (PKI)** can be used to authenticate a sender's identity for spontaneous.

Digital certificates provide a high level of confidence in the individual or entity with which you are communicating.

A person wanting to use a CA registers with the CA and must provide some proof of identify.

The CA issues a digital certificate that is the requestor's public key encrypted using the CA's private key as proof of identify.

The certificate is attached to the user's e-mail or Web transactions in addition to the authentication information.

Digital Certificate

The receiver verifies the certificate by decryption it with the CA's public key – and must also contact the CA to ensure that the user's certificate has not been revoked by the CA.

For higher-security certifications, the CA requires a unique "fingerprint" be issued by the CA for each message sent by the user.

The user submits the message to the CA, who creates the unique fingerprint by combining the CA's private key with the message's authentication key contents.

Kerberos Key Exchange

Kerberos key exchange is a network authentication protocol developed at MIT.

It is designed to provide strong authentication for client/server applications by using a combination of both **private key** and **public key cryptography**.

Kerberos utilizes a single central server to act as a trusted third party to authenticate users and control access to resources on the network.

The basic premise behind the Kerberos security is that it is not possible to ensure security on all network servers.

The Kerberos model proposes is possible to truly secure a single server.

Kerberos Key Exchange

Kerberos utilizes cryptographic keys referred to as "tickets" to control access to network server resources.

Tickets are encrypted passes or files issued by the "trusted" server to users and processes to determine access level.

There are six types of tickets:

1) Initial, 2) Invalid, 3) Pre-authenticated,

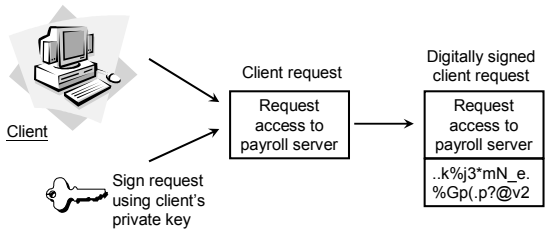
4) Renewable, 5) Forwardable, and 6) Postdated.

The following six figures illustrate the Kerberos key exchange process.

Kerberos Key Exchange

The client creates a request to send to the Kerberos server. The request is digitally signed by the client using the client own private key.

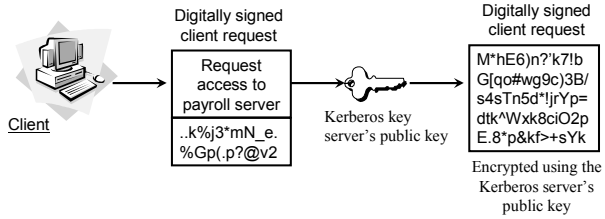
Step One:



Kerberos Key Exchange

The client takes the digitally signed request and encrypts it using the Kerberos server public key.

Step Two:

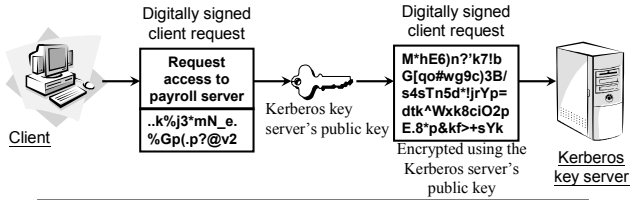


Kerberos Key Exchange

The client sends the digitally signed and encrypted request to the Kerberos server.

The Kerberos server decrypts the request using its private key and then authenticates the originator of the request by verifying the digital signature of the sender.

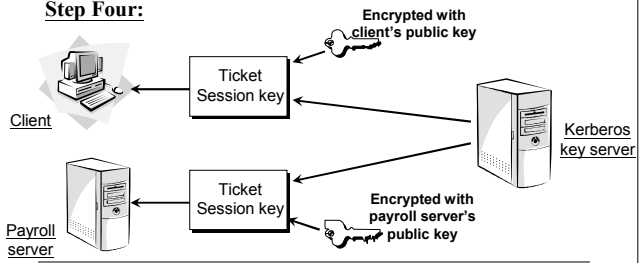
Step Three:



Kerberos Key Exchange

If the Kerberos server determines that the client does have authorization to access the payroll server, the Kerberos server sends identical session tickets to both the client and the payroll server.

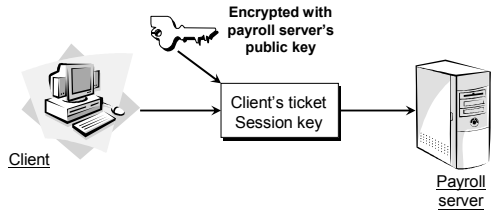
Step Four:



Kerberos Key Exchange

The client then sends a copy of its ticket to the payroll server. Before transmitting the ticket, the client encrypts the ticket using the payroll server's public key.

Step Five:

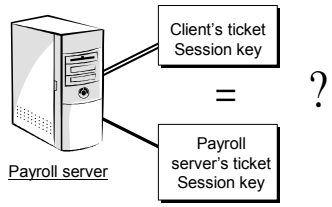


Kerberos Key Exchange

When the payroll server receives the encrypted ticket from the client the server decrypts the ticket using the server's own private key.

The payroll server then compares the ticket that it received from the client to the ticket that it received from the Kerberos server.

Step Six:



Public Key Infrastructure

The functions of a PKI :-

- Registration for a CA.
- Initialization and set up other CA
- Certification or posts that certificate in a repository
- Key Pair Recovery - The user's private key can be either backed up by a CA, or by a separate key backup system. The PKI should provide a system that permits the recovery of the private key with minimal risk.
- Key Generation
- Key Update
- Cross-Certification
- Certificate Revocation

Key Management Problem

- Key management is a difficult problem in secure communications is not due to technical reasons.
- Cryptographically secure ways of creating and distributing keys have been developed and are fairly robust.
- The weakest link - humans are responsible for keeping secret and private keys confidential.
- Keeping these keys in a secure place and not writing them down is a socially difficult task.

Diffie-Hellman Algorithm for Key Exchange

- Developed by Diffie and Hellman in 1976 leading to the development of today's public key cryptography system.
- A method to create secret session keys in a distributed manner is the *Diffie-Hellman algorithm*.
- The Diffie-Hellman algorithm provides a way for two parties to establish a shared secret key that only those two parties know even though they are communicating over an insecure channel.
- This secret key is then used to encrypt data using their favourite secret key encryption algorithm.
- Based on the difficulty on computing discrete logarithms

Diffie-Hellman Algorithm for Shared Key

- Alice and Bob have to agree on two large prime numbers n and g as public key on certain conditions..
- Alice pick a large number x (e.g. 512-bit) and keep it secret
- Bob pick a large number y
- Alice send n, g, $g^x \bmod n$
- Bob send $g^y \bmod n$
- Alice compute $(g^y \bmod n)^x$
- Bob compute $(g^x \bmod n)^y$
- From the laws of modular arithmetic, both calculation yield $(g^{xy} \bmod n)$ and this is the shared secret key.

Email Protection

- Protecting Email with Cryptography
  - http://www.pgpi.org
  - PGP uses RSA algorithm to provide digital signature and encryption capabilities for email.
  - Key exchange can be done on public network by and verify the keys using MD5 checksum which can be exchanged through different channels such as telephone call or post.
- S/MIME
  - Also use RSA algorithm and standardized by IETF
  - Integrated into browsers such as IE and Netscape

PGP

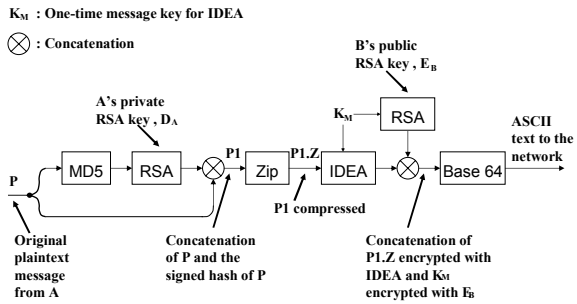


Figure : PGP in operation for sending a message

PGP

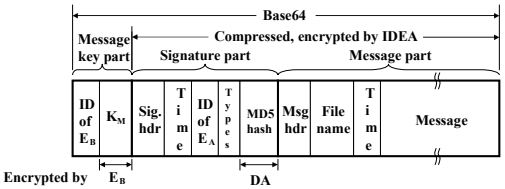


Figure : A PGP message

Firewalls

- Isolates LAN from Internet. Allowing some packets to pass and block others.
- Two types of firewall
  - Packet filter
    - Usually is a router or special
  - Application gateway / proxy
    - Allow the configuration of a more complex policy than the packet filter.
    - Filter packet on application data as well as IP/TCP/UDP headers.
    - Force web/telnet application through a gateway

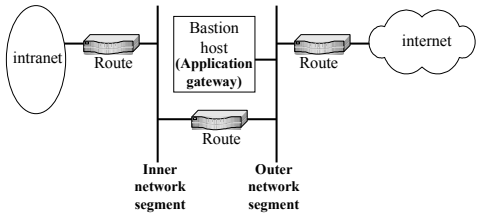
Packet Filtering

- The headers of network packets are inspected when going through the firewall. Packet filters allow or block packets, usually while routing them from the Internet to an internal network, and vice versa.
- A set of rules that specify what types of packets (e.g., those to or from a particular IP address or port) are to be allowed and what types are to be blocked is required. Packet filtering may occur in a router, in a bridge, or on an individual host. It is sometimes known as packet *screening*.
- The type of router used in a packet filtering firewall is known as a *screening router / outside router / border router*.

Firewalls

- Bastion host
  - A computer system that must be highly secured because it is vulnerable to attack, usually because it is exposed to the Internet and is a main point of contact for users of internal networks. It gets its name from the highly fortified projections on the outer walls of medieval castles.
  - "Bastions . . . overlook critical areas of defense, usually having stronger walls, room for extra troops, and the occasional useful tub of boiling hot oil for discouraging attackers".
- Dual-homed host
  - A general-purpose computer system that has at least two network interfaces (or homes).

Firewalls



A screened subnet firewall architecture

Perimeter network is a network added between a protected network (e.g. Intranet) and an external network (e.g. Internet), in order to provide an additional layer of security. A perimeter network is sometimes called a *DMZ*, which stands for *De-Militarized Zone* (named after the zone separating North and South Korea) or screened subnet.

Detecting Unauthorized Access

Intrusion Detection System (IDS)

There are three general type of IDS and two fundamental techniques:

The first type is a **Network-based IDS**:

- IDS sensors are place on key network circuit.
- An IDS sensor is simply a device running a special operating system that monitors all network packets on that circuit and reports intrusions to an IDS management console

The second type is a **Host-based IDS**:

- It is a software package installed on a host or server.
- This type of IDS monitors activity on the server and the incoming circuit are reports intrusions to an IDS management console

Detecting Unauthorized Access

The third type is a **Application-based IDS**:

- It is specialized from of host-based IDS that just monitors one application on the server.

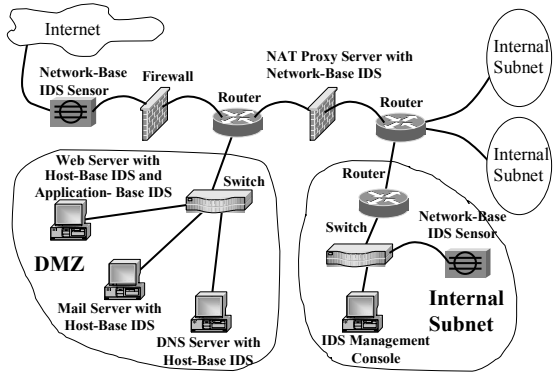
The first technique is a **Misuse Detection**:

- Which compares monitored activities with signatures of know attacks.

The second technique is a **Anomaly Detection**:

- Which works well in stable networks by comparing monitored activities with the "normal" set of activities.

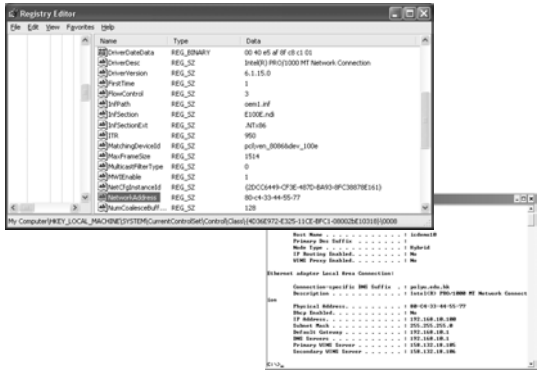
Detecting Unauthorized Access



Example - MAC Spoofing on Windows

- Some Network Card allow the spoofing of MAC address directly from the property of the NIC
- MAC address can also be changed by changing a key in the Registry
  - HKLM\System\CurrentControlSet\Control\Class\{4d36e97-e325-11ce-bfc1-08002be10318}\00xx
- This is due to the application of Network Devices and Protocols API of the Windows DDK

MAC Spoofing



Privacy Issues in Network Security

- From computer to network
- On-line Privacy
  - Cookies
  - Cache
  - Autocomplete
  - Ad ware and Spy ware
- Email
- Any form of security control would affect privacy
  - http://epic.org/

Preventing Disruption, Destruction and Disaster

Preventing Viruses

- The best way to prevent the spread of viruses is to not copy or download files of unknown origin.
- Using anti-virus software packages to check disks and files to ensure that they are virus free.

Preventing Denial-of-Service (DoS) Attacks

- With a DoS attack, a hacker attempts to disrupt the network by flooding the network with messages so that the network cannot process messages from normal users.
- This would prevent the use of faked IP addresses and enable users to easily filter out DoS message from a given address.

Preventing Disruption, Destruction and Disaster

Using Redundant Hardware

- An ***uninterruptable power supply*** **(UPS)** is a separate battery-operated power supply unit that can supply power for minutes (or even hours) in the event of a power loss.
- ***Disk mirroring***, uses a second redundant disk for every disk on the server. Every data item written to the primary disk is automatically duplicated on the mirrored disk.
- Redundancy can be applied to other ***Network components***, such as client computers, circuits, or devices (e.g., routers, bridges, multiplexers) can be install to ensure that the network remains operational should any of these components fail..

Development

- Recent development and future trends of data communication and networking
- IP World
- VoIP
- How to make IP routing more effective?
- Last mile solution
- Deregulation of telecommunication industry
- Wireless multimedia solution
- Multimedia communication
- Security

Reference

- Kurose, James and Ross, Keith, Computer Networking – A Top-Down Approach Featuring the Internet, 2nd Ed., Addison-Wesley, 2003.
- Stallings, William, Cryptography and Network Security – Principles and Practices, 3rd Ed., Prentice Hall, 2003.
- Garfinkel, Simon and Spafford, Gene, Web Security Privacy & Commerce, 2nd Ed., O'Reilly, 2002.
- Stallings, William, SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, 3rd Ed., Addison-Wesley, 1999.
- Subramanian, Mani, Network Management – Principles and Practice, Addison-Wesley, 2000.
- Mauro, Douglas, and Schmidt, Kevin, Essential SNMP, O'Reilly, 2001.
- Hegering, H.G. et all, Integrated Management of Networked Systems, concepts, architectures, and their operational application, Morgan Kaufmann, 1999.