Instituto Superior Técnico

Information Protection for Computer Networks

Marcelo S. Alencar
Institute of Advanced Studies in Communications
Federal University of Bahia

References: Informação, Codificação e Segurança de Redes, Marcelo S. Alencar, Editora Elsevier, Rio de Janeiro, Brasil, 2015. Data Protection Techniques and Cryptographic Protocols in Modern Computer Networks, Milan Marković, Ph.D.E.E., Docent, Mathematical Institute, SANU, Kneza Mihaila 35, Beograd.

Introduction

- The Internet has changed the way in which companies do business, because the Internet Protocol (IP) is efficient, inexpensive and flexible
- This talk addresses the main cryptographic aspects of modern TCP/IP computer networks, including:
  - Digital signature technology based on asymmetrical cryptographic algorithms
  - Data confidentiality by applying symmetrical cryptographic systems
  - The use of Public Key Infrastructure (PKI)
- This presentation is devoted to the emerging topic in the domain of modern e-business systems – a computer network security based on PKI systems
- It also considers possible vulnerabilities of the TCP/IP computer networks and possible techniques to eliminate them
- It seems clear that only a general and multi-layered security infrastructure could cope with possible attacks to the computer network systems

Introduction

- Security mechanisms are used on application, transport and network layers of the ISO/OSI reference model
- Examples of the today most popular security protocols applied in each of the mentioned layers are: S/MIME, SSL and IPSec
- A secure computer network systems consists of combined security mechanisms on three different ISO/OSI reference model layers:
  1. Application layer security (end-to-end security) based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards)
  2. Transport layer security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure
  3. Network IP layer security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks
- The layers are designed in a way that a vulnerability of the one layer do not compromise the other layers, and the whole system is not vulnerable
- User strong authentication procedures based on digital certificates and PKI systems are especially emphasized

Introduction

- There are differences between software-only, hardware-only and combined software and hardware security systems
- Ubiquitous smart cards and hardware security modules are the basic hardware security systems
- Hardware Security Modules (HSM) represent very important security aspect of the modern computer networks
- The main purposes of the HSM are twofold:
  1. Increase the overall system security
  2. Accelerate cryptographic functions (asymmetric and symmetric algorithms, key generation etc.)

Introduction

- HSMs are intended mainly for use in server applications and, optionally for client side, in case of specialized information systems (government, military, police)
- For large individual usage, smart cards are more suitable as hardware security modules
- However, for large usages, the best approach is the combination of SW and smart card solutions for best performance
- Smart card increases security and SW increases the total processing speed. In this sense, the most suitable large-scale solution consists of:
  1. Software for bulk symmetric data encryption and decryption
  2. Smart card for digital envelop retrieval and digital signature generation

Introduction

- A brief description of the main components of the PKI systems, emphasizes the Certification Authority and its role in establishing a cryptographic unique identity of the valid system users based on ITU-T X.509v3 digital certificates
- Public-key cryptography uses a combination of public and private keys, digital signature, digital certificates, and trusted third party Certification Authorities (CA), to meet the major requirements of e-business security
- Before applying the security mechanisms it is necessary to ask the answers for the following questions: Who is the CA? Where to store the private key? How to know that the private key of the person or server to talk to is secure? Where to find the certificates?
- A public-key infrastructure provides the answers to the above questions

Introduction

- In the sense of the ITU-T X.509 standard, the PKI system is defined as the set of hardware, software, roles and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography
- PKI system provides a reliable organizational, logical and technical security environment for realization of the four main security functions of the e-business systems:
  1. Authenticity
  2. Data integrity protection
  3. Non-repudiation
  4. Data confidentiality protection

Introduction

- PKI system consists of the following components:
  1. Registration Authorities (RAs) – responsible for acquiring certificate requests and checking the identity of the certificate holders
  2. Systems for certificate distribution – responsible for delivering the certificates to their holders
  3. Certification Authority (CA) – responsible for issuing and revoking certificates
  4. Certificate Holders (subjects) – people, machines or software agents that have been issued certificates, CP, CPS, user agreements and other basic CA documents, systems for publication of issued certificates and Certificate Revocation Lists (CRLs), as well as of PKI applications (secure WEB transactions, secure E-mail, secure FTP, VPN, secure Internet payment, secure document management system – secure digital archives etc.)

Potential Vulnerabilities in Computer Networks

- The Internet has changed the ways in which companies do business, since the Internet Protocol (IP) is efficient, inexpensive and flexible
- However, the existing methods used to route IP packets leave them vulnerable to a range of security risks such as spoofing, sniffing and session hijacking and provide no form of non-repudiation for contractual or monetary transactions
- Besides securing the internal environment, organizations need to secure communications between remote offices, business partners, customers and traveling or telecommuting employees
- Transmitting messages over the Internet or Intranet to these different entities poses an obvious risk, given the lack of protection provided by the existing Internet backbone
- Control and management of security and access between these different entities in a company's business environment are important issues

Potential Vulnerabilities in Computer Networks

- Without security, both public and private networks are susceptible to unauthorized monitoring and access. Internal attacks might be a result of minimal or nonexistent intranet security
- Risks from outside the private network originate from connections to the Internet and extranets. Password-based user access controls alone do not protect data transmitted across a network
- Without security measures and controls in place, the data might be subjected to an attack
- Some attacks are passive, in that information is only monitored
- Other attacks are active and information is altered with intent to corrupt or destroy the data or the network itself

Eavesdroping

- In general, the majority of network communications occur in a plaintext (unencrypted) format, which allows an attacker who has gained access to data paths in a network to monitor and interpret (read) the traffic
- When an attacker is eavesdropping on communications, it is referred to as sniffing or snooping
- The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise
- Without strong encryption data can be read by others as it traverses the network

Data Modification

- After an attacker has read the data, the next logical step is often to modify it
- An attacker can modify the data in the packet without the knowledge of the sender or of the receiver

Identity Spoofing

- Most networks and operating systems use the IP address to identify a computer as being valid on a network
- In some cases, it is possible for an IP address to be falsely used. This is known as identity spoofing
- An attacker might use special programs to construct IP packets that appear to originate from valid addresses inside an organisation intranet
- After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete data

Password-based Attacks

- The password-based access control is common among most operating systems and network security plans
- Access to both a computer and network resources are determined by a user name and password
- Earlier versions of operating system components did not always protect identity information as it was passed through the network for validation
- This might allow an eavesdropper to determine a valid user name and password and use it to gain access to the network by posing as a valid user
- When an attacker finds and accesses a valid user account, the attacker has the same rights as the actual user
- For example, if the user has administrator rights, the attacker can create additional accounts for access at a later time

Password-based Attacks

- After gaining access to a network with a valid account, an attacker can do any of the following:
  - Obtain lists of valid users and computer names and network information
  - Modify server and network configurations, including access controls and routing tables
  - Modify, reroute, or delete data

Denial of Service Attack

- Unlike a password-based attack, the denial-of-service attack prevents normal use of a computer or network by valid users
- After gaining access to a network, an attacker can do any of the following:
  - Distract information systems staff so that they do not immediately detect the intrusion. This gives an attacker the opportunity to make additional attacks
  - Send invalid data to applications or network services, causing applications or services to close or operate abnormally
  - Send a flood of traffic until a computer or an entire network is shut down
  - Block traffic, which results in a loss of access to network resources by authorised users

Man-in-the-middle Attack

- As the name indicates, a man-in-the-middle attack occurs when someone between two users, who are communicating, is actively monitoring, capturing, and controlling the communication without the knowledge of the users
- For example, an attacker can negotiate encryption keys with both users
- Each user then sends encrypted data to the attacker, who can decrypt the data
- When computers are communicating at low levels of the network layer, the computers might not be able to determine with which computers they are exchanging data

Compromised-key Attack

- A key is a secret code or number required to encrypt, decrypt, or validate secured information
- Although determining a key is a difficult and resource-intensive process for an attacker, it is possible
- After an attacker determines a key, that key is referred to as a compromised key
- An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack
- With the compromised key, the attacker can decrypt or modify data
- The attacker can also attempt to use the compromised key to compute additional keys, which might allow access to other secured communications

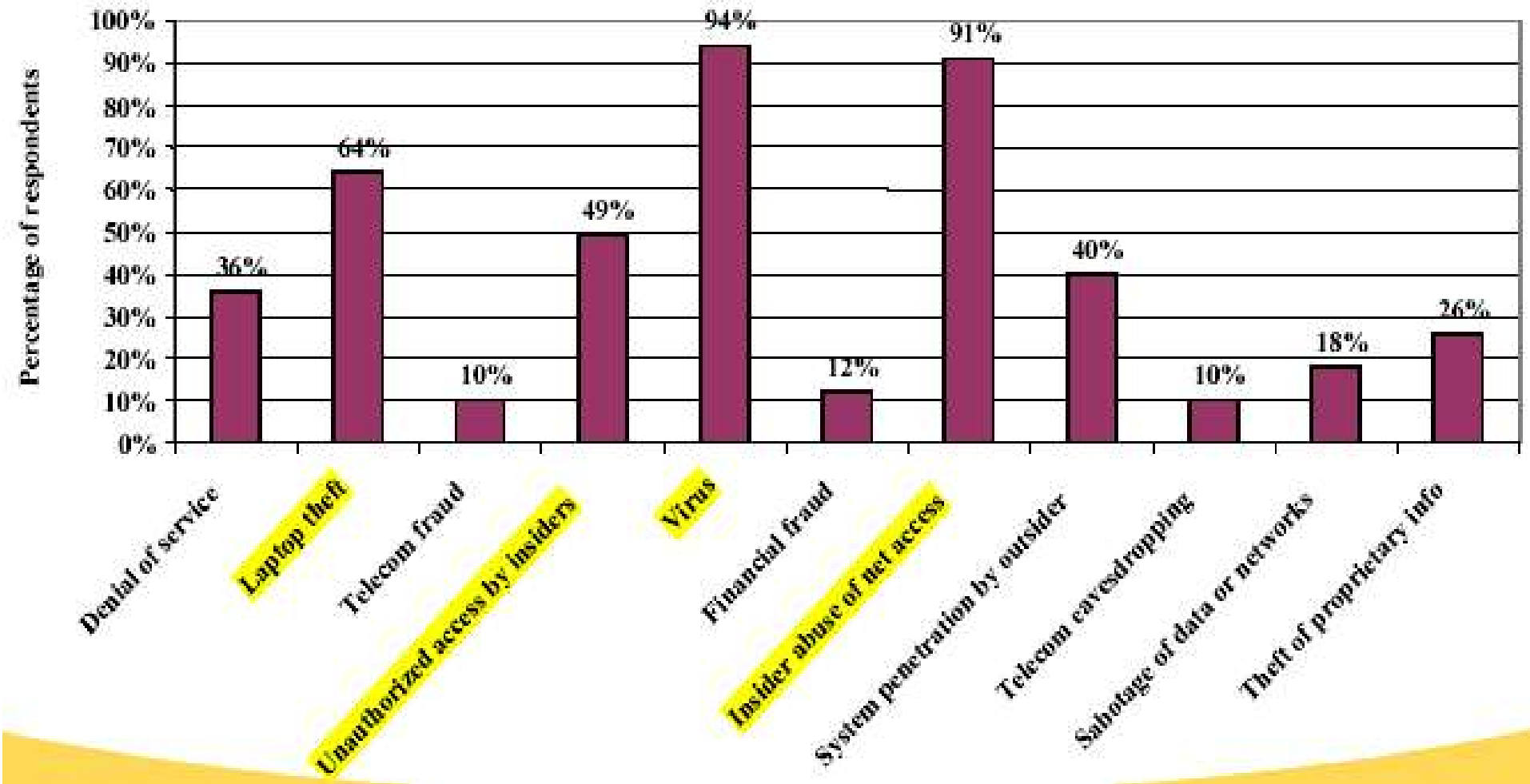
Sniffer Attack

- A sniffer is an application or device that can read, monitor, and capture network data exchanges and packets
- If the packets are not encrypted, a sniffer provides a full view of the data that is inside the packet
- Even encapsulated (tunneled) packets can be opened and read if they are not encrypted
- Using a sniffer, an attacker can do the following:
  - Analyse a network and access information, eventually causing the network to stop responding or become corrupted
  - Read private communications

Application Layer Attack

- An application-layer attack targets application servers by causing a fault in a server's operating system or applications
- This results in the attacker gaining the ability to bypass normal access controls
- The attacker takes advantage of this situation, gaining control of an application, system, or network, and can do any of the following:
  - Read, add, delete, or modify data or an operating system
  - Introduce a virus that uses computers and software applications to copy viruses throughout the network
  - Introduce a sniffer program to analyse the network and gain information that can eventually be used to cause the network to stop responding or become corrupted
  - Abnormally close data applications or operating systems
  - Disable other security controls to enable future attacks

Attack Statistics



Attack Statistics