innovate achieve lead

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Network Security

Lecture-2, January 11, 2012

Rahul Banerjee, PhD (CSE)

Professor, Department of Computer Science & Information Systems

E-mail: rahul@bits-pilani.ac.in, Home: http://universe.bits-pilani.ac.in/pilani/rahulbanerjee/Profile

Interaction Points

innovate achieve lead

A quick recap of concepts learnt in the previous class
- Introduction to definitions and Elements of the Network Security & Cryptography

Examples of the Network types for which security may have to be provided

Types of Internetworks having varying security requirements

Classification of Network Security problems

Types of Attacks on Networks and Internetworks

Criteria for acceptable Security Solutions

Security requirements of the in-design project: BITS-Connect 2.0

Select References to the literature

Summary

Network Security: An Introduction

- Network Security <recap>
  - Network Security is often viewed as the branch of study dealing with need to protect:
    - one or more aspects of operation of Computer Networks,
    - permitted use,
    - access,
    - behaviour,
    - performance,
    - privacy and
    - confidentiality
  - Security requirements of a Network may be Local or Global in their scope, depending upon the network's or internetwork's purpose of design and deployment.

Examples of Networks to be made Secure <recap>

- Class-I: Function-based classification
  - Data Networks
  - Voice Networks
  - Multimedia Networks
  - ……
- Class-II: Location-and-Distance-based classification
  - Personal Area Networks (PANs)
  - Local Area Networks (LANs)
  - Metropolitan Area Networks (MANs)
  - Wide Area Networks (WANs) ….
- Class-III: Forwarding-based classification
  - Switched Networks
    - Circuit-Switched Networks
    - Packet-Switched Networks
  - Shared Networks
  - Hybrid Networks
- Class-IV: Ownership-based classification
  - Public Networks
  - Private Networks
  - Virtual Private Networks

Types of Internetworks to be made Secure <recap>

- Intranet:
  - Completely private network of networks
- The Internet:
  - Global public network of networks
- Extranet:
  - Intranets interconnected via the Internet
- Each of these may be of the following types:
  - Wireline
  - Wireless
    - Fixed
    - Mobile
  - Hybrid

Criteria for Security Solutions

- Ability to meet the specified needs / requirements
- Effectiveness of Approach Across Networks
- Computing Resources Needed vis-à-vis the value of the protection offered
- Quality and Scalability
- Availability of Monitoring mechanisms
- Adpatability and Flexibility
- Practicability from Sociological / Political perspective
- Economic considerations & Sustainability

Classification of Security Problems: Access Breaches in Internetworks

- Intentional / Non-Intentional Access Breaches
- Origin-based Access Breaches
- Centralized / Distributed Access Breaches
- Service Blocking / Overwhelming / Redirection / Abuse / Modification / Termination-based Access Breaches
- Periodic / Aperiodic Application-Data / Control-Data Access Breaches
- Event-based Access Breaches
- Storage-based Access Breaches

Security Attacks, Threats, Mechanisms and Services

- Security Attack => compromises the information-system security
- Security Threat => has potential for security violation
- Security Mechanism => detects / locates / identifies / prevents / recovers from “security attacks”
- Security Service => enhances security, makes use of the security mechanisms

Active versus Passive Attacks <recap>

- Active attacks involve *active attempts on security leading to modification, redirection, blockage or destruction of data, devices or links*.
  - *Examples:*
    - Modification / corruption of data or access control bits
    - Denial-of Service attacks
- Passive attacks involve simply getting access to link or device and consequently data.

Other Internetwork Attacks

- *Birthday* attacks *(based on collisions: can be mounted after choosing √n random choice for 'n' choices)*
- *Meet in the Middle* attacks *(based on collisions: build a table of √n random choice-based keys and computed MACs)*
- *Virus*-based attacks
- *Worm*-based attacks
- *Trojan Horse*-based attacks
- *Logic-Bomb*-based attacks
- *Zombie*-based attacks
- Attacks *veiled like System Administration / Network Management*

A typical Internetwork Model of Security

- Parties involved:
  - Sender
  - Receiver
  - Interceptor (Passive / Active)
- Devices involved:
  - Transmitter
  - Receiver
  - Encoder
  - Decoder
- Links involved:
  - Data and Control signal transmission links

Identification of Sources of Security Problems

- Importance of Identification of sources
  - Strategic importance for planning, preventing and / or countering
  - Importance with respect to Sensitivity-analysis and Economic-impact-analysis and pro-active protection
- Possible Approaches for Analysis
  - Monitoring-based approaches
    - Log-based
    - Agent-based
  - Non-monitoring approaches
    - Model-based
    - Experimental Replication-based

Role of Cryptography, OS & Configuration

- Role of Cryptography <recap>
  - Symmetric / Conventional cryptography
  - Asymmetric cryptography
- Role of Operating Systems <recap>
  - Built-in OS Security at the Kernel-level
  - Support for Cryptographic APIs
  - Network Protocol Stack design based security
- Role of Configuration in Security <recap>
  - Network configuration
  - OS configuration
  - Application configuration
  - Security System configuration

The OSI Security Architecture

- OSI Security Architecture has been defined in the ITU-T Recommendation X.800.
- It is an International Standard.
- Elements of the X.800 Standard:
  - X.800 Security Services (defined as a protocol layer compliant with the IETF RFC 2828)
    - X.800 Authentication (Peer-entity Authentication / Data-origin Authentication)
    - X.800 Access Control
    - X.800 Data Confidentiality
    - X.800 Data Integrity
    - X.800 Non-repudiation
  - X.800 Availability Services

Cryptography in Networking <recap>

- Network / Internetwork Cryptography aims to handle
  - Network / Internetwork-specific issues

    and
  - problems involving authentication, integrity and secrecy / confidentiality / privacy.
- Cryptography can exist with or without networks but Internetwork / Network Cryptography specifically addresses the Internetwork / Network needs / requirements and is thus a subset of general cryptography.

Symmetric-Key Cryptography <recap>

- Symmetric-Key cryptography is called so since in this class of cryptographic algorithms, encryption as well as decryption processes are performed using the same (i.e. symmetric) key.
- The algorithms / schemes / programs that use this paradigm are often termed as Symmetric-Key Ciphers / Private-Key Ciphers / Secret-Key Ciphers / Conventional Ciphers etc.
- In such cases, Plaintext, Encryption-Decryption Algorithm, Key and Ciphertext form four basic components of the Symmetric Cipher Model.
- Such schemes *should* exhibit:
    - **Security of Key Distribution** to the legal recipients)
    - **Adequate strength of Encryption**

Characterizing the Symmetric Key Ciphers

- This is often done by:
  - Choice of key-space
  - Key-derivation / identification within the key-space
  - Number of cycles involved in encryption / decryption process
  - Choice of operations (or choice of type of operators) that are used in the process of encryption / decryption
  - Number of internal algorithms that form the final scheme of enciphering / deciphering
  - Role, if any, of the compression algorithms / schemes in adding the security value

Some More Basics

- Any cryptographic scheme is safe if and only if it is unbreakable in reasonable time using feasible resources in spite of the intruder's being aware of:
    - Encryption and decryption algorithm
    - Size of the key

- **Kerckhoff's Principle:** *Security of conventional encryption* depends only upon the *Secrecy of the Key,* and not on the *Secrecy of the Algorithm*.
- Strength of the algorithm and the size of key remain two important factors in Cryptography.
- Unconditionally secure and Computationally secure schemes of cryptography do exist; but in practice involving computers, only the latter is popular.

On the Secure Deployment of the Conventional (Secret-Key) Cryptography

Requirements for secure deployment of conventional cryptography:

- Availability of a *strong Encryption Algorithm*
- *Secure distribution* of *the Secret Key to the intended recipients*

Kerckhoff's Principle remains a guiding line for the research on conventional cryptography and its real-life use in internetworks.

Terms like Conventional / Private-Key / Secret-Key / Symmetric-Key cryptography are interchangeably used in literature.

References

- Bruce Schneier: Applied Cryptography, Wiley Student Edition, Second Edition, Singapore, 1996.
- Alfred Menezes, Paul van Oorschot, and Scott Vanstone: Handbook of Applied Cryptography. CRC Press, NY.
- William Stallings: Cryptography and Network Security. Fifth Edition, Pearson, New Delhi, 2011.
- C.Kauffman, R.Perlman and M.Spenser: Network Security, Second Edition, Prentice Hall, Englewood Cliffs, 2002.
- S.Bellovin and W.Chesvick: Internet Security and Firewalls, Second Edition, Addison-Wesley, Reading, 1998.

Recommendations for Further Reading

- Journals & Magazines
  - IEEE / ACM Transactions on Networking
  - IEEE Transactions on Wireless Communications
  - IEEE Transactions on Computers
  - IEEE Security & Privacy
  - IEE Proceedings on Information Security
  - IEEE Network
  - IEEE Computer
  - IEEE Pervasive Computing
  - IEEE Personal Communications
  - Elsevier's Pervasive Computing

Recommendations for Further Reading

- On-line Resources
  - IETF Postings at ietf.org
  - Periodic updates at nist.gov
  - Select FIPS documents at fips.org
  - Digital Libraries / Archives / Technical Reports at major research universities active in this area as shall be mentioned from time to time during lectures
  - Rahul Banerjee: **Lecture Notes on Network Security**, Electronic Read-only edition to be available just before Mid-Sem Test at the course page

Thank you for your kind attention!

Rahul Banerjee

BITS Pilani

Pilani | Dubai | Goa | Hyderabad