



Introduction to the Network Security

Lecture-1

Dr. Rahul Banerjee
Associate Professor: CS & IS Group
Birla Institute of Technology & Science, Pilani
(India)
Email: rahul@bits-pilani.ac.in
Home: <http://discovery.bits-pilani.ac.in/rahul/>





Interaction Points

- A brief introduction to:
 - the Course Objectives and Scope
 - the Plan of Interaction for this semester
- Network, Internetwork and their Security Perspectives
- Network Security and Trustworthy Computing
- Identification of Sources of Security Problems
- Role of Cryptography, OS and Configuration
- Discussions
- Recommendations for further reading





Objectives & Scope

- Introduction to the fundamental aspects of security in a modern networked environment
- Focus on system design aspects and cryptography in the specific context of network / internetwork security
- Study of elements of cryptographic techniques, algorithms and protocols
- Study of system/application design issues in building secure networked systems
- Designing effective Internetwork Security Systems
- Analyzing these designs from viewpoints of real-life security needs vis-à-vis current best practices and evolving trends





Plan of Interaction

- We plan to have our interaction for this course in three ways:
 - Through regular interactive online lecture-cum-discussion sessions <32 lectures planned, at an average 8 lectures per month, each lecture may be of 90 minutes to 120 minutes depending upon the level of interactions we have during the lecture>
 - Course's mailing list <once a week at an average>
 - Course's Web page <updated once a week with added reading material, lecture slides in PDF form and summary of concepts learnt>
- This is in addition to the resources that may be planned to be delivered through the BITS Virtual University's asynchronous delivery system
- You will have self-assessment questions and self-learning assignments in addition, delivered through one of the above referred means





Networks, Internetworks & Security

- Network
 - A **Computer Network** is an interconnected group of autonomous computing nodes which:
 - Use a well-defined, mutually-agreed **set of rules and conventions** known as **Protocols**,
 - **Interact** with one-another meaningfully;
 - Allow **resource-sharing** preferably in a **predictable** and **controllable** manner.
- Internetwork
 - A network of two or more networks is called an **Internetwork**
 - **Participating networks** in an Internetwork may be **interconnected for restricted** or **unrestricted resource sharing**
- Security
 - **Security** is often viewed as **the need to protect one or more aspects of network's operation and permitted use** (access, behaviour, performance, privacy and confidentiality included),
 - **Security requirements** may be **Local** or **Global** in their scope, depending upon the network's or internetwork's purpose of design and deployment.





Criteria for Evaluating Security Solutions

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





Classification of Security Problems: Access Breaches in Internetworks (S/W & H/W)

- 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





Of Security Attacks, Security Threats, Security Mechanisms and Security 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

- **Active attacks** involve *active attempts on security leading to modification, redirection, blockage or destruction of data, devices or links.*
 - *Examples:*
 - Replay attacks
 - Masquerade attacks
 - 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.**





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**
 - Secret-key cryptography
 - Public-key cryptography
- **Role of Operating Systems**
 - Built-in OS Security at the Kernel-level
 - Support for Cryptographic APIs
 - Network Protocol Stack implementation decision-based security
- **Role of Configuration in Security**
 - Network configuration
 - OS configuration
 - Application configuration
 - Security System configuration





Security Architectures: The OSI Route

- 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





X.800 Security Mechanisms: 1 of 2

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization





X.800 Security Mechanisms: 2 of 2

- Trusted functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

These five mechanisms are sometimes called "Pervasive Security Mechanisms".





On the Internetwork Cryptography

- Internetwork Cryptography **aims to handle**
 - internetwork-specific or network-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

- 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.





Types of Cryptographic Attacks

- Classification One: **Approach of mounting attacks**
 - *Brute-force* Attacks
 - *Cryptanalytic* Attacks
 - *Differential cryptanalytic attacks*
 - *Linear cryptanalytic attacks*
- Classification Two: **Attacks that try to recover Keys**
 - *Ciphertext-only* attacks (*here, the attacker has only the Ciphertext*)
 - *Known Plaintext* attacks (*the attacker has the Ciphertext of some known plaintext*)
 - *Chosen Plaintext* attacks (*the attacker has the Ciphertext of some chosen plaintext*)
 - *Chosen Ciphertext* attacks (*here, Ciphertext and corresponding plaintext are chosen*)
- Classification Three: **Attacks that focus upon discovering the difference between the actual and expected (ideal) cipher**
 - *Distinguishing* attacks (*exploit imperfections of encrypting functions*)





Unconditionally Secure Versus Computationally Secure Encryption Schemes

- Unconditionally Secure Encryption schemes:
 - Here, the generated *Ciphertext* simply *does not have adequate information to allow discovery of the unique plaintext irrespective of the amount of Ciphertext available (as well as irrespective of the computational resource available)* to the attacker.
- Computationally Secure Encryption schemes
 - Here, the *cost of deciphering exceeds the value of enciphered information*
 - *Time needed to decipher exceeds the lifetime of the enciphered information*





Recommendations for Further Reading

- Books
 - 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**. **Fourth Edition**. Prentice-Hall, Englewood Cliffs, 2006. <Recommended companion>
 - C.Kauffman, R.Pearlman 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.
 - Rahul Banerjee: **Internetworking Technologies**, Prentice-Hall of India, New Delhi, 2003.





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 URL:
<http://discovery.bits-pilani.ac.in/rahul/NetSec/>





That's all for today!

Any questions?

Thank you!

