Security Beyond Crypto

Prof. Chandan Mazumdar

Coordinator, Centre for Distributed Computing, &

Head

Dept. of Comp. Sc. & Engg.

Jadavpur University

Agenda

- Part 1 – Concepts & Terminologies
- Part 2 – Protocol Problems

Centre for Distributed Computing

- Distributed Computing Lab established in 1999 with a project from DRDO
- National Workshop on Distributed Computing organized in 1999
- Projects and Research on Distributed Computing continued
- Centre established in 2002

Centre for Distributed Computing - Areas

- Fault Tolerance
- Information and Network Security
- Web Technologies
- Image Processing
- Disaster Management
- Digital Forensics

Centre for Distributed Computing - Segments

- Strategic Sector – Defence, Home Affairs, Space
- Academic Sector – Fundamental Research & Training
- Industry Sector – Financial, Software, Banking & Finance, etc.
- Social Sector – Disaster Management
- **Total value of projects (2004-2010) ~ Rs. 6.0 Crore**

Present Projects

- Enterprise Level Security Metrics – DIT, GoI
- Threat and Attack Modeling of Heterogeneous Enterprise Networks - SAG, DRDO
- Comprehensive Computerization of WBIDFC
- 15 R&D projects and over a dozen consultancy jobs have been successfully completed during the last 10 years

International Conference on Information Systems Security, www.iciss.org.in

- 2011 December 15-19, Jadavpur University, Kolkata
- 2010 – DA-IICT, Ahmedabad
- 2009 – IIT Kharagpur, Kolkata
- 2008 – JNTU, Hyderabad
- 2007 – Delhi University, New Delhi
- 2006 – ISI Calcutta
- 2005 – Jadavpur University, Kolkata

Model of an Enterprise

- Computational Processes
  - Data holding and Processing
- Communication Channels
  - Copper, Fibre, Wireless
  - Different Protocols & Speed
- Messages flow from one process to another via the channels
  - Required for Cooperation

  (in MA-based systems, programs also flow!)
- Data in Store and Data in Transit

Value of Data

- Financial
- Technical
- Business
- Strategic
- Private
  - There is motivation to steal or tamper data
  - There is motivation to block legitimate access to data or service

Insecurity in Distributed Systems - Attacks

- Stealing of data
- Data Tampering
- Masquerading
- Man-in-the-middle
- Denial of service

Insecurity in Enterprise Systems - Causes

- Inadequate / Faulty Hardware
- Inadequate / Faulty Software
- Inadequate / Faulty Communication protocols
- Faulty Channels
  - Side Channels

Adversary is out there to exploit these causes.

Terminologies - Concerns

- Vulnerability
  - **An inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat**
- Threat
  - **Anything that can disrupt the operation, functioning, integrity, or availability of a network or system**
  - **Threats exploit vulnerabilities**
  - **Threats may be internal or external**
- Security Concern
  - **Each threat-vulnerability pair represents a security concern**

Terminologies – Security Parameters

- Confidentiality
  - Important data must not be accessible to unauthorized persons
- Integrity
  - Data consistency should never be compromised. All modifications must be done using authorized means by authorized agents only
- Availability
  - Legitimate users must have access to the data or service when they need them

Terminologies – Security Parameters

- Authentication
  - Process of proving the identity of the agent performing a transaction / of the source of data
- Authorization
  - Process of granting permission to some agent(s) for performing some action(s) on some object(s)
- Non-repudiation
  - Establishing accountability of the originator or recipient of a communication or action

Terminologies – Misc.

- Trusted System
  - **A system which can be verified to implement a given security policy**
- Intruder
  - **An agent who gains, or attempts to gain unauthorized access to a computer system or to gain unauthorized privileges on that system**
- Auditing
  - **Process of retaining and using the sequence of data to prove the actions performed by agents in a computer system**

Security in Enterprise Systems

- Two Approaches
  - Reactive: sense attack and respond
  - Proactive: try to prevent attack by design
- Security Trinity
  - Prevention
  - Detection
  - Response

Security in Enterprise System

- Security by Obscurity
  - **If data or network is hidden, it won't be subject to attack**
  - **Does not work in long term**
- Perimeter Defence
  - **Securing the borders of the network, so that no external attacker can enter the network**
- Defence in Depth
  - **Hardening and monitoring each system in addition to perimeter security**

Difficulty in Security Design

- Functional Correctness
  - Program satisfies specification
    - For reasonable input, get reasonable output
- System Security
  - Program properties are preserved in the face of attack
    - For unreasonable input, output not completely disastrous
- Main difference
  - Active interference from adversary
  - Refinement techniques may fail
    - More functionality can be worse

Security in Enterprise System

- System Model
- Adversary Model
- Identify Security Properties
- Ensure that the properties are preserved under attack

- Result
  - No "absolute security"
  - Security means: Under given assumptions about the system, no attack of a give form will destroy specified properties

Building Blocks of Security

- Access Security
  - **Controlling access to individual systems and networks**

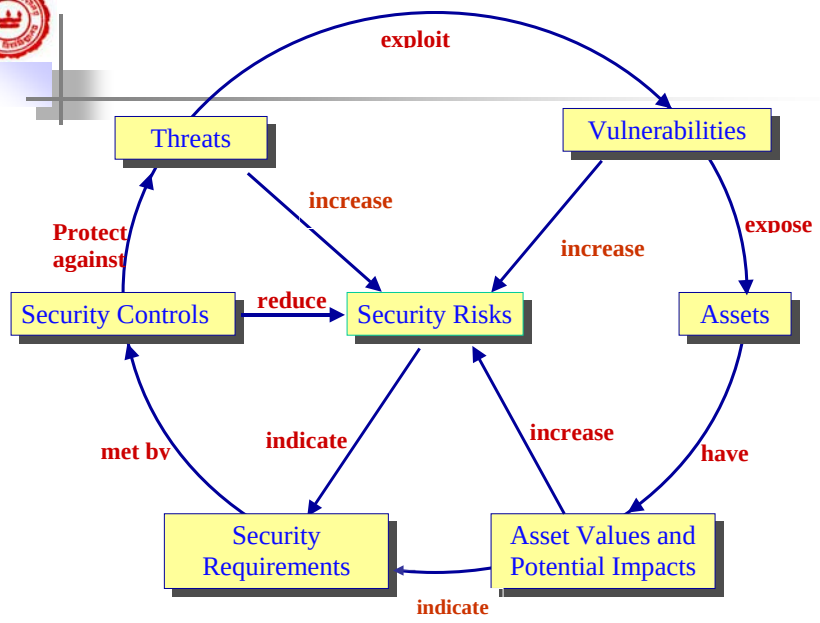
- Communications Security
  - **Providing confidentiality, integrity and authenticity to data in transit**

- Storage Security
  - **Controlling access to data or programs in store**

- Application Security
  - **Controlling access to Application Programs**

Conclusion

- There are Vulnerabilities in Enterprise Information Systems
- Threats exploit vulnerabilities for attacking systems for unlawful gain
- There are identified security properties
- There is no absolute security
- There are building blocks for improving security perception



Problems

- To determine how much is too much, so that we can implement appropriate security measures to build adequate confidence and trust
- We want a powerful logic for implementing or not implementing a security measure

Some Myths

- Myth 1 – Good passwords mean security!
- Myth 2 – Put a Firewall and you are secure!
- Myth 3 – Encrypt the records and messages, you are secure!
- Myth 4 – Isolate and quarantine the records and messages, you are secure!
- Myth 5 – Employ a security agency and you are secure!

Enterprise Security

- Determinants
  - business goals
  - operational context
  - technology used
  - organizational structures
  - connectivity
- Dynamic

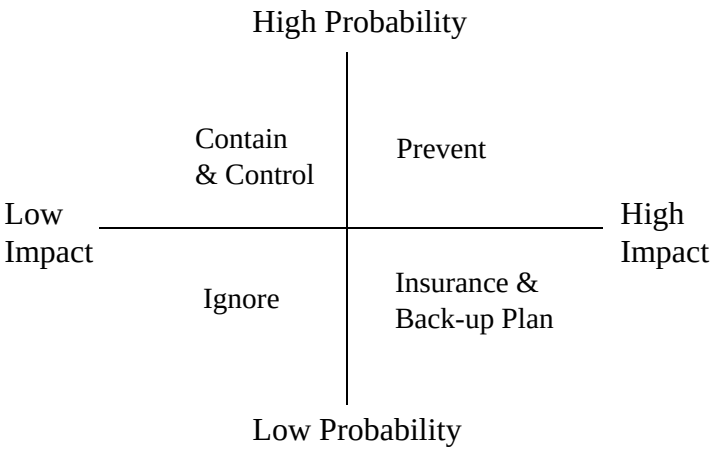
Information Security Management

- Information Security is not a static object, it's a process
- An Engineering Approach is needed
- The Security process should be survivable
- This needs a life-cycle methodology

Difference in Approach

- In Information System Design, we look for the functional properties – the need is correctness and liveness on the face of known inputs and mistakes
- In IS Security Design, we should look for the safety and protection of assets on the face of unknown malicious activity

RISK MANAGEMENT

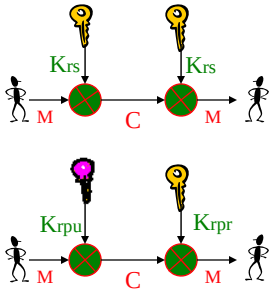


Security Infrastructure

- **Authentication systems**
- **Data & File Corruption Attacks**
- **Anti-virus software**
- **Proxy Servers**
- **Firewalls**
- **Intrusion Detection Systems**
- **Virtual Private Networks**
- **Auditing Tools**

Encryption Basics

- Encryption (Block and Stream)
  - Symmetric Encryption.
    - Same key shared between sender and receiver
    - DES, RC4, Rijndael (AES), IDEA
  - Asymmetric Encryption.
    - Different key for sender and receiver (Public key and private key are compatible with each other)
    - RSA, ElGamal, ECC
  - Digital signature and Hash
    - MD5, SHA



Protocols

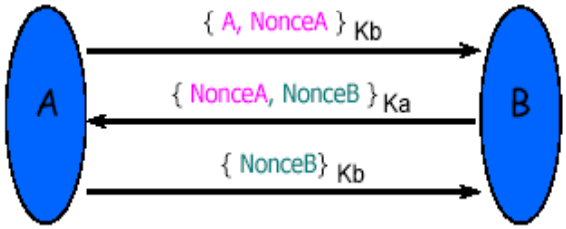
- A Protocol is a formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.
- Each message exchange is described as

  A -> B: m1, {m2}K
- Can also be represented using sequence diagrams
- A Nonce is a number used only once

Needham-Schroeder Key Exchange

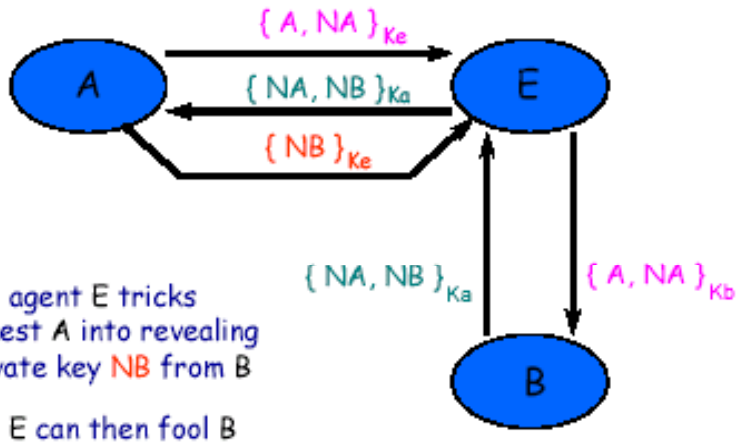
- Famous simple example
  - Protocol published and known for 10 years
  - Gavin Lowe discovered unintended property while preparing formal analysis using FDR system
- Background: Public-key cryptography
  - Every agent A has
    - **Public encryption key Ka**
    - **Private decryption key Ka^{-1}**
  - Main properties
    - **Everyone can encrypt message to A**
    - **Only A can decrypt these messages**

Needham-Schroeder Key Exchange



Result: A and B share two private numbers not known to any observer without Ka^{-1}, Kb^{-1}

Anomaly in Needham-Schroeder



Evil agent E tricks honest A into revealing private key NB from B

Evil E can then fool B

General Problem in Security

- Divide-and-conquer is fundamental
  - Decompose system requirements into parts
  - Develop independent software modules
  - Combine modules to produce required system
- Common belief:
  - Security properties do not compose
- Difficult system development problem

Example Protocol

- Protocol P1

  A -> B : {message}KB

  A -> B : KA^{-1}

- This satisfies basic requirements
  - Message is transmitted under encryption
  - Revealing secret key KA^{-1} does not reveal message

Similar Protocol

- Protocol P2

  B -> A : {message'}KA

  B -> A : KB^{-1}

- Transmits msg securely from B to A
  - Message is transmitted under encryption
  - Revealing secret key KB^{-1} does not reveal message

Composition P1;P2

- Sequential composition of two protocols

  A -> B : {message}KB

  A -> B : KA^{-1}

  B -> A : {message'}KA

  B -> A : KB^{-1}

- Definitely not secure
  - Eavesdropper learns both keys, decrypts messages

Conclusion

- Various Security operations can be achieved by using well-designed protocols
- Various applications on the Internet also require newer protocols
- It is interesting to analyze and systematically design protocols

END OF OVERVIEW