Distributed Systems Security

Fundamentals

Prof. Dr. Stefan Fischer
Institut für Telematik, Universität zu Lübeck
https://www.itm.uni-luebeck.de/people/fischer
What do you associate with “Security in Distributed Systems”? 
Learning Goals

• Acquire a basic understanding of security issues
  – Name and explain important terms in security
  – Explain today's security risks
  – Name and explain security objectives
  – Describe two security models
  – Difference between safety and security
Overview

- Data Processing and Security Today
- Information Warfare
- Fundamentals of Network and Computer Security
  - Security Objectives
  - Communication Model
  - Attacker Models
  - Attacks
  - Security Services
  - Security Mechanisms and Techniques
Document-based security

- Replicate functions associated with documents
  - Typically based on physical (paper) documents and their integrity
  - Examples: Signatures and Dates, Protection from disclosure, tampering, or destruction, Notary or Witnesses

- Challenge: Differentiate between originals and copies/forgeries
  - Usually feasible when using physical documents
  - Modification of physical documents leave one’s mark
  - Testing procedures based on physical properties and condition of a document

- But how are electronic documents tested and verified?
Common Document-based Security Services

- Identification
- Authorization/Prohibition
- License/Certification
- Signature
- Testimony
- Compliance
- Reliability
- Confirmation
- Verification of Origin

- Annotation
- Access
- Validation
- Determination of the moment of occurrence
- Voting
- Determination of ownership
- Registration
- Privacy
Data Processing Evolution

• Until 1950/1960
  – Mechanical data processing

• 1960-1980
  – Mainframe computer, mostly standalone

• Since 1980
  – PCs and Local Area Networks

• Since 1990
  – Large interconnected networks, Internet
Security Demands

• Prior to data processing
  – Security by **physical procedures**
  – E.g.: Armored filling cabinets, security checks of future employees

• Mainframe Computers
  – Data security for time sharing systems and systems, which were externally accessible via modem connections
  – Mainly **Computer Security**

• Networking (Internet/LAN/WAN)
  – Protection of data during transmissions
  – **Network Security**
Who is at Risk?

• **Individuals**, which share computers or which are attached to shared networks

• **Organizations**, which computers are used by employees and which are attached to a shared network

• **States**, which infrastructure depends heavily on information systems  
  → Information Warfare
Examples of Security Threats

• A transmits secret data to B
  – Attacker C eavesdrops the transmission and copies data

• A network management system sends a password file to a server system E (to grant a new user access to the network)
  – Attacker $C_1$
    • intercepts the file, changes some entries, and
    • relays the changed file to the target server system E
  
  – Attacker $C_2$
    • does not intercept the file but creates one on its own and
    • passes it on behalf of the management software to the server system E
Examples of Security Threats

• An employee is fired and his account is to be disabled
  – The employee intercepts the message which will disable his/her account,
  – copies confidential data, and
  – transmits the intercepted message when he/she is done

• A customer issues a transaction and denies the order later on
Information Warfare

• The term “information warfare” has been used in the military domain for a while
  – Accomplishment of a military goal using techniques and methods from the field of information technology

• Nowadays it refers to warfare using IT
  – Attacking the IT infrastructure of a state
  – E.g., disrupt flow of information of the state or gain valuable information
  – Examples: Attacks on Natanz Nuclear Facility in Iran or attack on Estonia

• Attackers: Individuals, groups, states
**Internetangriffe: Angst um das Telefonsitz**

Die Entdeckung eines weltweiten Spionage-Netzwerks zeigt, wie verwunderbar Regierungen im Internet sind; Auch die Infrastruktur eines Landes könnte angegriffen werden. Von FOCUS-Online-Autor Torsten Klein

**Spionage: Hacker knacken Computer in 103 Ländern**

Kanadische Wissenschaftler sind einer weltweiten elektronischen Spionageaktion im Internet auf die Spur gekommen. Erste Spuren führen nach China.

**China: Cyber-Drache am Pranger**

"Rote Hacker" in Diensten des chinesischen Militärs? Stimmt alles nicht, reagiert Chinas Regierung auf die Vorwürfe.

**Hacker-Angriffe: Computerspionage unter Freunden**


**Spionage: China bestreitet Hacker-Angriff auf Pentagon**

Spezialisten der chinesischen Volksbefreiungsarmee stehen im Verdacht, die Computer des Pentagon auszupioniert zu haben. Peking distanziert energisch.

**Botschaften: Hacker veröffentlicht Mail-Zugangsdaten**

Aug. 2007

**Internet: Eine Großmacht perfektioniert die Internet-Kontrôle**

Apr. 2005

**INTERNET: Sicherheit? Stecker ziehen!**

Jul. 2004

**Sorgen wegen chinesischer Lieferanten**

Botnet attackiert Weblogs vietnamesischer Dissidenten


Firefox 3.6.3 schließt kritische Sicherheitslücke


Versionen vor Firefox 3.6 sollen von dem Problem nicht betroffen sein. Heiligtum zum regulären Download bereit und wird über die automatische Update-Funktion verteilt.

Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations

by Michael Arrington on Jan 12, 2010

Google is releasing information about a "highly sophisticated and targeted attack" on their corporate infrastructure that occurred last month. The attack originated in China and resulted in the "theft of intellectual property from Google." In light of the attack Google is making sweeping changes to its Chinese operations.
Russia claims Stuxnet could have triggered second Chernobyl

Dmitry Rogozin, the Russian ambassador to NATO, has warned that Stuxnet could have triggered a catastrophe comparable to the core meltdown at Chernobyl in 1986. Reuters reports that Rogozin has asked NATO to investigate Stuxnet. In the ambassador’s opinion, Stuxnet’s impact is comparable to that of an explosive mine.

Stuxnet is currently believed to have had two digital payloads — one designed to destroy the uranium enrichment centrifuges in Natanz and one designed to destroy the turbine control systems at the Bushehr nuclear plant. Rogozin is well placed to understand the potential effects of damaging the turbines in the Iranian nuclear plant, as it was built by Russian nuclear contractor Atomstroyexport.

The worst case scenario in the event of a failure cause systems for a high pressure turbine is an emergency past incidents show, where a failure occurs, followed resolve the failure, things can go wrong. For example nuclear plant is reported to have narrowly escaped...
Zero-Day-Lücke im Adobe Reader


Bei einer der DLLs handelt es sich anscheinend um einen Trojaner, der eigenständig versucht, über einen HTTP-Request eine Verbindung zur Außenwelt herzustellen. Laut FireEye zündet der Exploit bei den jeweils aktuellem Versionen aller drei Versionszweige: 9.5.3, 10.1.5, und 11.0.1. Ältere Versionen dürften ebenfalls betroffen sein.

Frostiger Angriff auf die Android-Verschlüsselung


Botnetz kostet Werbebranche viel Geld

IT Security Tasks

• Prohibit frauds (German: Betrug)
  – If not possible: Detect frauds

• Frauds
  – Unauthorized access to information
  – Faking one’s identity
  – Repudiate responsibility (German: leugnen)
  – Shoving responsibility on to someone else
  – Denial of reception of information
  – Unauthorized modification of software
  – …
Fundamental Terms

- Security Objectives
- Communication Model
- Attacker Model
- Attacks
- Security Services
- Security Mechanisms

- Sicherheitsziele
- Kommunikationsmodell
- Angreifermodell
- Angriffe
- Sicherheitsdienste
- Sicherheitsmechanismen
## Security Objectives (Sicherheitsziele)

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation
- Access Control
- Availability

- Vertraulichkeit
- Authentizität
- Integrität
- Nicht-Anfechtbarkeit
- Zugangskontrolle
- Verfügbarkeit
Confidentiality

• Protection of saved and/or transmitted data against passive attacks
  – Unauthorized access to the content
  – Analysis of the availability of data
  – Analysis of data flow

• Applicable on two different layers
  – Single data unit or message
  – Complete data storage or data flow between two parties
Authenticity

• Verification of a message’s genuineness
  – Was it really sent by the reputed sender?

• Applicable on two different layers
  – Individual messages: Authentication of single messages
  – Long-lasting relations: In addition to authenticating messages, guarantee that an authorized communication is not hijacked
Integrity

- Protection against undetected modification

- Protection against *modification* of messages

- Protection of an *entire connection* against
  - modification,
  - permutation,
  - replay,
  - fabrication, and
  - omission of individual messages.
Non-Repudiation

- Precludes sender and recipient of a message to repudiate its transmission / reception

- Recipients can prove that the message was sent by the stated sender

- Senders can prove that the intended recipient actually received the message
Access Control

- Controls and restricts access to hosts and applications

- First step
  - **Authentication** of the entity trying to gain access

- Second Step
  - Check **authorization** for the desired action
  - Definition of fine-grained tailored access rights can be set up for individual and groups of entities
Availability

• A system is utilizable when required
  – Multitude of attacks known that try to compromise this security objective

• Some countermeasures available
  – Software-driven (can be activated automatically)
  – Quite often only physical measures are effective
Communication Model

- Communication between (two) principals

Alice (Principal 1) → Information channel → Bob (Principal 2)

Messages and secret information

e.g. Internet, Wi-Fi, UMTS, optical fiber

Trusted third party

Eve (Attacker)
Network Security Model

• Fundamental Assumptions
  – Endpoints are secure
  – Network is insecure

• Advanced Assumption: Network and endpoints insecure
  – Consequence for, e.g., secure authentication
  – Combination of a software and secure (hardware) reader required
Attacker Model: Dolev-Yao

- Dolev-Yao (Internet security model)
  - Formal model proposed by Danny Dolev and Andrew Yao
  - Used to characterize interactive protocols

- Assumption: Attackers are valid members of a network and can
  - send messages to other network participants,
  - receive messages from other network participants,
  - intercept, modify, delete, duplicate and fabricate messages, and
  - fake their identity.

- But: Attackers are not able to…
  - break cryptographic methods
  - compromise end systems
Attack

- **Operation** which endangers the **security** of information and systems

- Attacker aim to change the original data flow to their own advantage

- To ease the detection, classification, and defense of attacks, one needs to
  - examine the deviation from the intended data flow and
  - classify attacks
Data Flow Deviations

- **Interruption**
  - A resource (message) is destroyed or corrupted
  - Attacks availability

- **Interception**
  - A resource is accessed by an unauthorized party
  - Attacks confidentiality

- **Modification**
  - A resource is (a) accessed and (b) modified by an unauthorized party
  - Attacks integrity and confidentiality

- **Fabrication**
  - A forged resource is injected into the system
  - Attacks authenticity
Classification

Passive Attacks
- Publication of message content
- Analysis of data traffic

Active Attacks
- Spoofing
- Replay
- Denial of Service
- Message Modification
Passive Attacks

- **Goal**
  - Eavesdropping (information retrieval)
  - Attacks confidentiality of data

- **Type 1: Publication of data**
  - Particularly harmful if the data is confidential
  - Example: WikiLeaks

- **Type 2: Traffic analysis**
  - Who communicates with whom
  - Example: Heavy e-mail traffic is detected between the management of two companies
Active Attacks

- Denial-of-Service (DoS)
  - Inhibits or suppresses intended usage of resources
  - Attacks a resource’s *availability*
  - Example: Prohibit access to the online store of competitors

- Spoofing
  - Faking one’s identity
  - Often combined with other types of active attacks
  - Attacks *authenticity*
  - Example: Use fake sender IP addresses to circumvent firewalls
Active Attacks

• Replay
  – Interception of a message and subsequent re-transmission to achieve an mischievous affect
  – Attacks a message’s **authenticity**
  – Example: Re-send intercepted (and even encrypted) message with log-in credentials to gain invalid access to a resource

• Message modification
  – Modification of a message’s content
  – Re-order, delay
  – Attacks a message’s **integrity**
  – Example: Change the bank account number of an intercepted bank transfer
Fundamental Terms

- So far, based on the presented communication and attacker models we have seen some attacks on the presented security objectives

- We will now focus on countermeasures
  - Security Service (realizes security objectives)
    - Enhances the security of IT systems and data exchange of organizations
    - Counters attacks using one or more security mechanisms
  - Security Mechanism (implementation of security service)
    - Mechanisms for detection, prevention or elimination of attacks
    - No single mechanism realizes all possible security objectives
Security Mechanisms

- There is no single security mechanism providing all security objectives

- Different security mechanisms exist
  - Simple example: access control using username and password
  - The most important one is cryptography (discussed later)
Design of Security Services

- Fundamental tasks for the design of a security service
  - Based on communication and attacker models

- Development of an **algorithm** for the realization of a **security-related conversion**

- Creation of **secret information** to which the algorithm is applied

- Development of methods **to distribute** and use the **secret information**

- **Establishment of a protocol** to be used by the participating principals, which provides a certain security service by utilizing the algorithm and the secret information
Safety vs. Security

• Safety
  – Something bad will never happen
  – Safe from harm, e.g., due to malfunctions
  – Mechanisms against potential and random faults

• Security
  – Assumption of attackers with certain capabilities (attacker model)
  – Attackers have strategic goals
  – “Faults don’t log in”
Summary of this Chapter

• In a connected world where business has changed from (HW-) products to services security gains more and more attention
  – Success stories like the company Amazon demonstrate the importance of the Internet for effective business
  – The financial systems of the world cannot survive without a working IT Infrastructure
  – Governments of countries concern about security attacks and develop measures against the information warfare

• There are 6 security objectives
  – Confidentiality, Authenticity, Integrity, Non-Repudiation, Access Control, Availability

• Models help to understand and design security

• To counter numerous security attacks, several security objectives are combined to provide security services
Outlook

1. Detailed look on successful attacks
2. “High-Level“ overview of security concepts like, e.g.:
   - Classification of attacks and appropriate counteractive measures
   - Security policy
3. Security mechanism: cryptography
4. Important security services
Literature
