Introduction to Information Security

Security Areas and Definitions,
Security in Context to Business Life,
Network Security Aspects

Agenda

- **Security Areas and Definitions**
- **Security in Business Context**
- **Network Security Aspects**

Security Areas 1

- **Information Security**
  - the global level
  - in the past provided by physical and administrative means
    - filing cabinets with a combination lock for storing sensitive documents, screening people during hiring process
  - with the introduction of the computer
    - automated tools for protecting files and other information stored on it were developed (integrity protection and access control)

    Computer Security
  - with the introduction of networks and distributed systems
    - tools for protecting data transmission and protecting network infrastructure against security attacks

    Network Security

Security Areas 2

- **Security Management**
  - security standards
    - ISO/IEC 17799 : 2005 (Information technology – Security techniques – Code of practices for information security management)
    - ISO/IEC 15408 : 1999 (Common Criteria)
  - process-oriented
  - risk analysis based
- **Best Common Practices**
  - hardening
  - downsizing
  - patch management
  - well known mitigations
  - compliance based

Information Security (Definition ISO 27001:2005)

- **Preservation of confidentiality, integrity and availability of information**
  - in addition other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
- **Confidentiality**
  - the property that information is not made available or disclosed to unauthorized individuals, entities or processes
- **Integrity**
  - the property of safeguarding the accuracy and completeness of assets
- **Availability**
  - the property of being accessible and usable on demand by an authorized entity

Information Security (intuitive)

- **Confidentiality**
  - the information can be read only by intended persons
- **Integrity**
  - we can trust in the information, it is not changed unintentionally
- **Availability**
  - the information is accessible when it is really needed
- **Access control**
  - the information can be accessed only by properly authorized persons
  - is strongly based on proper authentication and authorization

Information Security Areas

- **Information Security**
- **Information Technology (IT-) Security**
  - Computer Security
  - Network Security
- **Information Differentiation**
  - IAR (Information At Rest)
  - IIT (Information In Transit)
- **Different basic security methods for IAR and IIR to achieve**
  - Confidentiality
  - Integrity
  - Availability

Computer Security

- **Information At Rest (IAR)**
  - Availability
    - Downsizing to required functionality
    - Hardening and access control
    - Redundancy
    - Backup
  - Confidentiality and Integrity
    - Access control (in most cases generic functionality of the OS)
    - Authentication (e.g. username / password)
    - Authorization (e.g. ACLs)
    - (Encryption)

Network Security

- **Information In Transit (IIT)**
  - Availability
    - Redundancy
    - Backup
    - Simultaneous Transmission over separated paths
  - Confidentiality
    - Encryption (e.g. 3DES, AES)
  - Integrity and identity
    - Cryptographic checksums (e.g. keyed MD5, keyed-SHA1)

Agenda

- **Security Areas and Definitions**
- **Security in Business Context**
- **Network Security Aspects**

Security in Real Business Life

- **In companies security must be seen from the global level**
  - know the business threats if security is not assured
  - risk analysis to balance cost of security versus value of protected target
  - security policy
    - regulations to which people have to follow
  - security audit (internal, external)
    - monitoring what is going on
    - periodical proofing by an independent certified information systems auditor -> where we are and what must be improved
  - security management
    - is necessary to stay in business (e.g. Basel II)

Security Policy

- **According to "Site Security Handbook" RFC 2196**
  - a security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide
- **Provides a general security framework for implementing security by defining what is and what is not allowed**
- **Helps determination of tools and procedures necessary for a organization**
- **Defines the roles and responsibilities of users and administrators**
- **States consequences of misuse**
- **Defines processes for handling network security incidents**
- **Defines processes for audit, review and improvement of the covered security issues**

Security Costs, Asset Values, Risk Analysis

- **Security is not for free**
  - costs must be taken into account
- **No perfect defense**
  - methods should be evaluated and compared
- **Compromise is needed**
  - risk analysis should give background for decisions
  - the cost of defense must be matched against the value of the target (asset) of the defense
  - methods to avoid higher risks should have higher priority in resource allocation

Resource Allocation

- **Resources usable for security are normally limited**
  - Allocation of security resources must be based on risk analysis
  - The cost of defense must be matched against the value of the target of the defense
- **Exceptional needs might arise**
  - some functions might be so critical, that their loss should be avoided at all available costs
- **Resource usage must be tracked**
  - provide data for future planning

Business Threats 1

- **Financial loss**
  - loss of electronic funds and other valuables
  - costs of correcting exposure
- **Legal repercussions**
  - lack of adherence to laws and regulations results in punishments
- **Loss of credibility and competitive edge**
  - service firms (banks, investment, insurance etc.) based on public trust
  - security violation can severely damage credibility
  - loss of business and prestige

Business Threats 2

- **Industrial espionage**
  - active information searching by intruders
  - early access to new developments damage competitive edge
- **Disclosure of confidential, sensitive or embarrassing information**
  - accidental or unintentional information leakage
  - damage means of conducting business
  - legal or regulatory actions against the company
- **Sabotage**
  - cause damage due to dislike
  - conducting business might fail

Breaching Security

- **Unreliable operations**
  - same result as malicious intruder intended to do sabotage
  - the nature of humans can be treated in some cases with the same general methods
- **Access control violations**
  - serious impact on business
    - so it is very important to avoid it
  - in most cases cannot be recognized immediately
    - so managers tend to overlook it, or ignore it
- **The human factor**
  - most security violations are coming from inside
    - outside hackers represent only a small risk compared to employees

Security Attacks

- **Typical algorithmic break-ins**
  - information eavesdropping
    - leakage of information helps the most for the intruder
    - security algorithms assume some information is secret
      - account name, password, PIN code, encryption key etc.
  - password cracking
    - passwords are difficult to be remembered
    - after false authentication, the intruder uses authorized rights of others
      - very difficult to recognize

Security Environments 1

- **Physical protection**
  - the most basic level of protection
  - all the other methods rely on the physical security environment of the critical core of other security services
    - i.e. if the physical console of a computer is easily accessible, then all software methods can be cheated
  - typically the emphasis is on the integrity protection of devices and services

Security Environments 2

- **Regulatory and operational protection**
  - all the security methods can be violated easily if the human control is not properly operating
  - no humans can be fully trusted
  - a complex scheme of controls can provide an environment where individuals would not risk violating the regulations
  - human procedures can be used as compensating controls for deficiencies in technology

Security Environments 3

- **Algorithmic protection**
  - Hardware
    - more difficult to make malicious changes
  - Software
    - integrity protection of security services is a critical problem
  - Networking concerns
    - most of the operational domain cannot be protected by physical and hardware security environments
    - must rely on more fragile software and procedural methods
    - highest complexity of security solutions

Top Ten Threats to Security

- **In real systems** (from Matt Blaze)

1. Software quality problems
2. Ineffective protection against denial-of-service attacks
3. No place to store secrets
4. Poor random number generation
5. Weak passwords
6. Mismatched trust
7. Poorly understood protocol and service interactions
8. Unrealistic threat and risk assessment
9. Interfaces that make security expensive and special
10. Little broad-based demand for security

Security in Context - Summary

- **Security solutions should be driven by real business needs**
- **Security is a compromise**
  - between potential damages and resources needed to avoid problems
- **Security should be designed and then carefully implemented**
  - Security evaluations might help to optimize solutions
  - Security auditing is necessary for assurance
- **Security is a never-ending topic**

Agenda

- **Security Areas and Definitions**
- **Security in Business Context**
- **Network Security Aspects**

Risks in Network Security

- **Three categories**
  - Break-ins
    - access to data in computer storage on networked systems
  - Privacy violations
    - compromise of data in transit over the line
    - active (insertion, replay)
    - passive (sniffing, analyzing)
  - Denial of service attacks
    - overwhelming a service with seemingly legitimate data or sending malformed data to a service
- **Cryptography can help in all cases**
  - encryption, data integrity, access/source authentication

Adversaries in in Network Security

- **Who are the attackers?**
  - Casual crackers (script kiddies)
    - any target, low funding
    - doing things because they are there
  - Motivated/paid crackers
    - specific targets, high funding,
    - can produce severe damage
  - Military/government intelligence
    - specific targets
    - can be unlimited funding
  - Hacker
    - good guys (crackers are the bad ones)
    - experiments with the limitation of systems for intellectual curiosity or sheer pleasure having a particular set of skills

Some Network Security Attacks 1

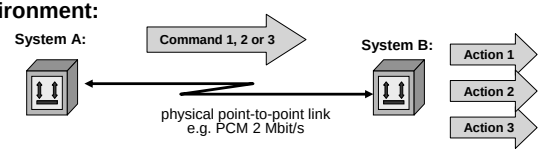
- **Wire tapping** (passive attack)
  - to get access to cleartext data and passwords
- **Impersonation** (active attack)
  - to get unauthorized access to data or to create unauthorized e-mails, orders, etc.
- **Denial-of-service** (active attack)
  - to disturb network resources in order to make them non-functional
- **Replay of messages** (active attack)
  - to get access to information and change it in transit
- **Modification of message contents** (active attack)
  - to get some advantage or to disturb

Some Network Security Attacks 2

- **Guessing of passwords** (passive attack)
  - to get access to information and services that would normally be denied (dictionary attack)
- **Guessing of keys** (passive attack)
  - to get access to encrypted data and passwords (brute-force attack)
- **Viruses** (active attack)
  - to destroy data and/or disturb systems functionality
- **Masquerade** (active attack)
  - one entity pretends to be a different one
- **Traffic analysis** (passive attack)
  - e.g. cryptanalysis to decrypt encrypted information

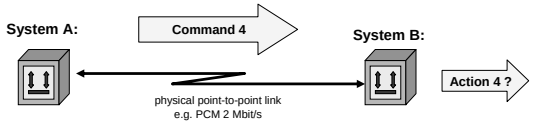
What makes the difference between functionality and security?

- **Lets consider the following simple system in a closed environment:**



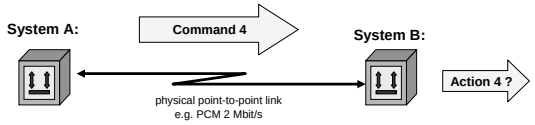
- **Focus in design, development, implementation and testing**
  - is on ensuring the corresponding functionality
    - Command 1 -> Action 1
    - Command 2 -> Action 2
    - Command 3 -> Action 3
- **Mindset of people involved in above topic areas is concentration on the correct function of the system**

What happens if system B receives command 4?



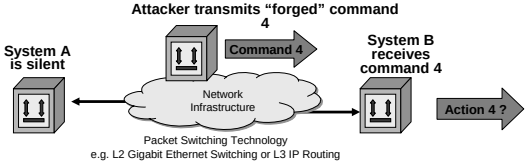
- **System B has four principle possibilities:**
  - 1. ignore command 4 and skip it
  - 2. increment an event counter and skip it
  - 3. inform a management function about the event and skip it
  - 4. inform a management function about the event, skip it and additionally tell system A about the event for error recovery
    - e.g. messages like: system A: hey you are wrong! What do you really mean? Please repeat it again!
- **Necessary CPU cycles (= time dedicated) increases with complexity of countermeasures**
  - possibility 1 means minimum, possibility 4 means maximum amount of CPU cycles

Functionality is not stressed by the timing behavior of an erroneous event !



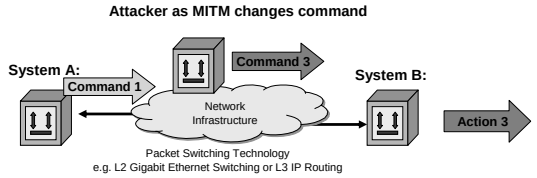
- **A well-engineered system will have a solution for this problem and things like that will rarely happen**
  - a well-behaving system A will not send command 4
  - however if it does and the event is recognized the code will be patched by SW-engineers (hopefully in the test-phase)
- **Performance impact on the system is not a critical issue**

What can happen in an open environment? 1



- **An attacker can stress our system with "forged" commands**
  - forged means that these commands look like coming from System B
  - stressing means that frequency of occurrences is much higher than in the closed environment
- **Intention of the attacker may be "Denial of Service" (DoS)**
  - depending on the basic strategy of the system to overcome such erroneous events sooner or later the system components will be cut off from the communication channel or even collapse because of the performing issue
- **Availability of system B gets in danger**

What can happen in an open environment? 2



- **Attacker performs active „Man-in-the-Middle“ (MITM) attack**
- **Functionality can not be ensured**
- **System B should check**
  - The **identity – authentication** of messages (who sent it?)
  - The data **integrity** (was something changed?) of received commands

What makes the difference between system functionality and system security?

- **1) Change of environment**
  - Closed (protected) versus open (unprotected)
- **2) Frequency of “erroneous” events**
  - e.g. command 4 arrives 1000000 times per second instead of just sometimes
  - DDoS (Distributed Denial of Service)
    - caused by a huge number of coordinated attackers (botnets)
  - **Availability** problem
- **3) System although fulfilling the functionality in an adequate manner**
  - May become insecure when the environment upon system communication happens changes
  - e.g. command 3 arrives instead of command 1
  - MITM (Man-in-the-Middle)
  - **Functionality** problem

Some Network Security Solutions 1

- **Encryption**
  - to protect data and passwords
- **Authentication by digital signatures and certificates**
  - to verify who is sending data over the network
- **Authorization**
  - to prevent improper access
- **Integrity checking and message authentication codes**
  - to protect against improper alteration of messages

Some Network Security Solutions 2

- **Non-repudiation**
  - by public key techniques to make sure that an action cannot be denied by the person who performed it
- **One-time passwords and two-way random number handshakes**
  - to mutually authenticate parties of a conversation
- **Frequent key refresh, strong keys and prevention of deriving future keys**
  - to protect against breaking of keys (cryptanalysis)
- **Address concealment (hiding)**
  - to protect against denial-of-service attacks

Some Network Security Implementations

- **IP Filtering**
- **Network Address Translation (NAT)**
- **IP Security Architecture (IPsec, IKE)**
- **Secure Shell (SSH)**
- **Secure Sockets Layer (SSL) or TLS**
- **Packet Level Firewall (Filtering Router)**
- **Stateful Inspection Firewall**
- **Circuit Level Firewall (SOCKS)**
- **Application Level Firewall (Proxy)**
- **Authentication systems (Kerberos, AAA servers)**
- **Virtual Private Networks (VPN)**
- **Secure Electronic Transactions (SET)**

Conclusions

- **1) In order to cover security a different mindset in all related topics is additionally be necessary**
  - not only to concentrate on the wanted function of a system but also to find the ways how to disturb/destroy a system in order to identify vulnerabilities of a system
  - starts from system design, SW implementation, testing/auditing, change management, internal training, accounting phase, customer training .....

  Security Awareness
- **2) In order to ensure functionality the overall system have to implement certain security elements / security functions**
  - **Availability**
  - **Authentication - Identity**
  - **Integrity**
  - **Confidentiality**
    - **Remark: confidentiality is not only a topic of secrecy but also important to avoid reconnaissance which may be later be used to perform attacks**

