INF3510 – Information Security Review

General Security Concepts

Security = Sikkerhet
Safety = Trygghet
Certainty = Visshet

Definition of information security (ISO27001)
Security is about protecting assets from damage or harm.
Def.: **Information Security** focuses on protecting information assets from damage or harm.
IS management has as goal to avoid damage and to control risk of damage to information assets.
IS management focuses on:

– Understanding threats and vulnerabilities
– Managing threats by reducing vulnerabilities or threat exposures
– Detection of attacks and recovery from attacks
– Investigate and collect evidence about incidents (forensics)

Reasons why solving all security problems once for all are impossible:

– Rapid innovation constantly generates new technology with new vulnerabilities
– More activities go online
– Crime follows the money
– Information security is a second thought when developing IT
– New and changing threats
– More effective and efficient attack technique and tools are being developed

CIA (Confidentiality, Integrity, Availability) definition
Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities or processes. (ISO 27001)
Integrity:

Data Integrity: The property that data has not been altered or destroyed in an unauthorized manner. (X.800)
System Integrity: The property of safeguarding the accuracy and completeness of assets (ISO 27001)

Availability: The property of being accessible and usable upon demand by an authorized entity. (ISO 27001) Main threat: Denial of Service (DoS)

Confidentiality	Integrity	Availability
Definition: • The property that information is not made available or disclosed to unauthorized individuals, entities or processes (ISO 27001) Can be divided into: • **Secrecy**: Protecting business data • **Privacy**: Protecting personal data • **Anonymity**: Hide who is engaging in what actions **Main threat**: Information theft **Controls**: Encryption, Access control, Perimeter defense.	Can be divided into: • **Data integrity**: The property that data has not been altered or destroyed in a unauthorized manner. • **System integrity**: The property of safeguarding the accuracy and completeness of assets **Main threat:** Data and system corruption **Controls:** encryption, Access control, Perimeter defense, Audit etc.	**Definition:** • The property of being accessible and usable upon demand by an authorized entity. (ISO 27001) **Main threat**: Denial of service (DoS) • Def. The prevention of authorized access to resources. **Controls:** Redundancy of resources, traffic filtering, incident recovery, international collaboration and policing

Meaning of and difference between other security services
User Identification and Authentication

- Identification: Who you claim to be, Method: (user)name, biometrics
- User authentication: Prove that you are the one you claim to be
- main threat: unauthorized access

System Authentication

- goal: establish the correct identity of remote hosts
- Main threat: network intrusion, masquerading attacks, replay attacks, (D)DOS attacks

Data Origin Authentication

- goal: recipient of a message (ex: data) can verify the correctness of claimed sender identity.
- Main threats: false transactions, false messages and data.

Non-Repudiation

- Goal: Making sending and receiving messages undeniable through unforgeable evidence.
    - Non-repudiation of origin: proof that data was sent.
    - Non-repudiation of delivery: proof that data was received.
    - NB: imprecise interpretation: Has a message been received and read just because it has been delivered to your mailbox?
- Main threats:
    - Sender falsely denying having sent message
    - Recipient falsely denying having received message
- Control: digital Signature-Cryptographic evidence that can be confirmed by a third party.

Definition of Access Control

Access controls are security features that control how users and systems communicate and interact with other systems and resources.

Difference between Accesses control and non-repudiation

Data origin authentication and non repudiation are similar: –Data origin authentication only provides proof to recipient party –Non-repudiation also provides proof to third parties

Accountability

- Goal: Trace action to a specific user and hold them responsible
- Main threats: Inability to identify source of incident, Inability to make attacker responsible

Authorization

- Authorization is to specify access and usage permissions for entities, roles or processes
    - Authorization policy normally defined by humans
    - Issued by an authority within the domain/organization
    - Authority can be delegated – Management → Sys. Admin
- **Correct interpretation:** A user may have authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
- **Wrong interpretation:** If the system determines that the subject may access the resource, it authorizes the subject

Perspectives on security controls

3 categories of security controls:

Physical controls
- Facility protection
- Security guards
- Locks
- Monitoring
- Environmental controls
- Intrusion detection

Technical controls
- Logical access control
- Cryptographic controls
- Security devices
- User authentication
- Intrusion detection
- Forensics

Administrative controls
- Policies
- Standards
- Procedures & practice
- Personnel screening
- Awareness training

Preventive, detective, corrective security controls
Preventive controls: prevent attempts to exploit vulnerabilities
Detective controls: warn of attempts to exploit vulnerabilities
Corrective controls: correct errors or irregularities that have been detected.

Security controls during storage
During storage:
- Information storage containers
- Electronic, physical, human

During transmission
- Physical or electronic

During processing
- Physical or electronic

Security controls for all information states are needed.
Security controls (aka. mechanisms) – Practical mechanisms, actions, tools or procedures that are used to provide security services. Security controls supports security services.

Security Management:

Know what ISO27k series is about:
- The ISO 27000 family of standards helps organizations keep information assets secure. ISO/IEC (mostly refer to the standards as ISO) standards must be bought
- ISO: International Standards Organization
- IEC: International Electro-Technical Committee

ISO27001 – title and purpose (2013-latest version):
- **ISO 27001**: Information Security Management System (ISMS)
- ISO 27001 specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

- ISO 27001 (ISMS) defines how to manage the implementation of security controls.
- Organizations can be certified against ISO 27001 – … but not against ISO 27002
- ISO 27001 is to be used in conjunction with ISO 27002

ISO27002 – title and purpose (2013-latest version):

- **ISO 27002**: Code of practice for information security management
- ISO 27002 (code of practice) defines a set of security goals and controls.
- ISO 27002 provides a checklist of general security controls to be considered implemented/used in organizations.
    - Contains 14 categories (control objectives) of security controls
        - Information security policy
        - Security Organization
        - Human resources security
        - Asset management
        - Access control
        - Cryptography
        - Physical and environmental security
        - Operations security
        - Communications security
        - Supplier relationships
        - Incident management
        - Business continuity
        - Compliance
    - Each category contains a set of security controls
    - In total, the standard describes 113 generic security controls
- Objective of ISO 27002:

    "… gives guidelines for […] information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)."

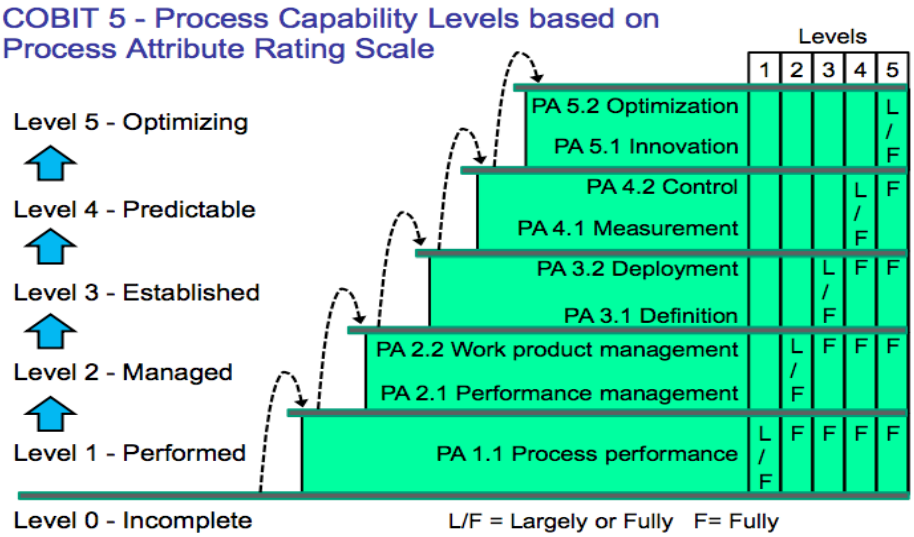
20 Critical Security Controls:

- Secure Network Engineering
- Incident Response
- Data Protection
- Account Control
- Need-to-know Access Control
- Monitoring of Audit Logs
- Boundary Defense
- Controlled Administrative Privileges
- Control of Network Ports and Protocols
- Secure Network Configuration
- Security Skills Training
- Data Recovery Capability
- Wireless Access Control
- Application Software Security
- Malware Defenses
- Vulnerability Assessment
- Security Configuration for Devices
- Inventory of Software
- Inventory of Devices
- Pentesting

Advantage over ISO27002

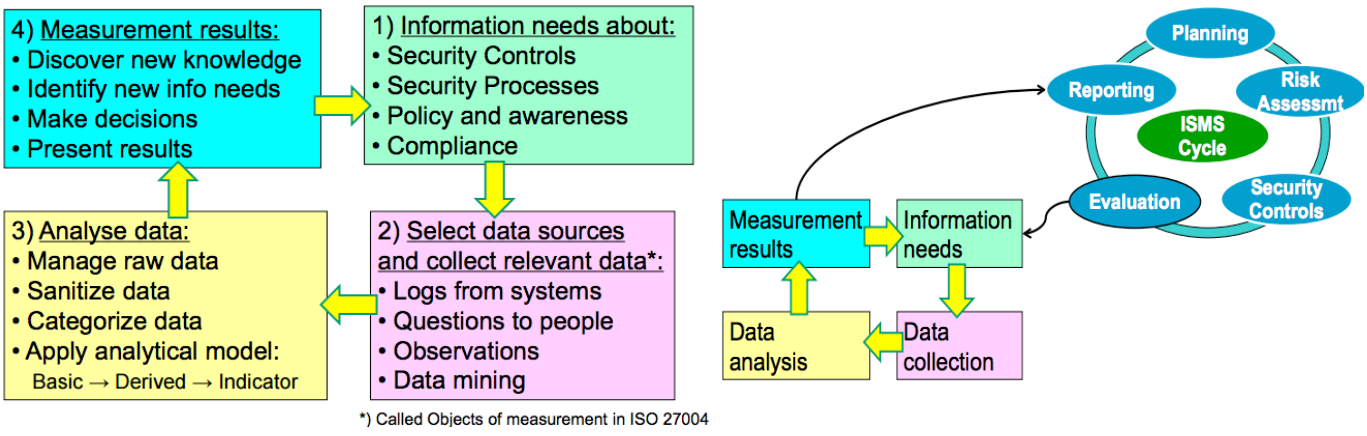
The 20 CSC has a description of each control, how to implement the controls (specific tasks), why control is critical, procedures and tools, effectiveness metrics and how to automate and test them. While the ISO27002 provides a checklist of general security controls.

Security governance and PCL (Process Capability Levels)



1. **Performed** Ad Hoc + Processes are ad-hoc and disorganized. + Risks are considered on an ad hoc basis, but no formal processes exist.
2. **Managed** but intuitive + Processes follow a regular pattern. + Emerging understanding of risk and the need for security
3. **Established** process + Processes are documented and communicated. + Company-wide risk management.' + Awareness of security and security policy
4. Managed and **Predictable** + Processes are monitored and measured. + Risks assessment standard procedures + Roles and responsibilities are assigned + Policies and standards are in place
5. **Optimized** + Security culture permeates organization + Organization-wide security processes are implemented, monitored and followed

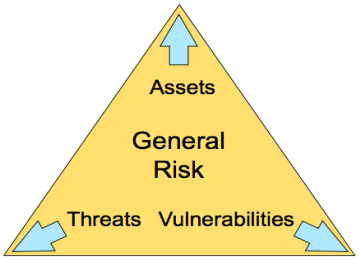
- Risk assessment as the basis for managing security
- Metrics as basis for knowing effectiveness of controls
    - What is the effectiveness of a security control?
        - You have to measure it to know it.
    - Security measurements provide
        - info about how well security controls work
        - basis for comparing effect of controls on risks
        - benchmark for assessing security investments



Risk Management

Understand the factor that contribute to risk:

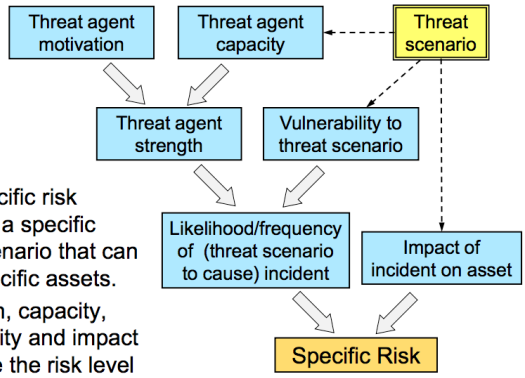
- "Risk is the effect of uncertainty on objectives
- Attacker/threat agent, vulnerability, impact(assets)
- The **more assets** you have, the **more threats** there are, and the **more vulnerable** you are, then the **greater the risk**.



Threats / incidents	Vulnerabilities	Asset impacts
•Password compromise	•Weak passwords	•Deleted files
•SQL injection	•Poor awareness	•Damaged files
•Logical bomb in SW	•No input validation	•Damaged reputation
•Trojan infects clients	•Outdated antivirus	•Stolen files
•Cryptanalysis of cipher	•Weak ciphers	- sensitivity levels 1,2,3
•Brute force attack	•Short crypto keys	•Intercepted traffic
•Social engineering	•Poor usability	•False transaction
• …..	• …	• …

Specific risk model

Threat agent strength:
motivation → to attack
Capacity → skills and resources to attack
Likelihood of threat/incident:
Each specific risk relates to a specific threat scenario that can affect specific assets.
Motivation, capacity, vulnerability and impact determine the risk level for that specific risk

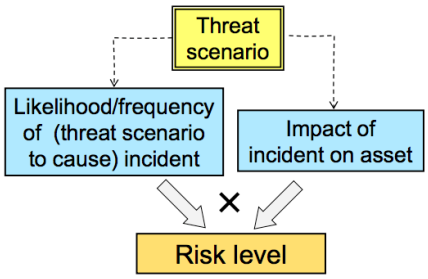


Each specific risk relates to a specific threat scenario that can affect specific assets.
Motivation, capacity, vulnerability and impact determine the risk level for that specific risk

Practical risk model

Practical risk analysis typically considers two factors to determine the level of each risk

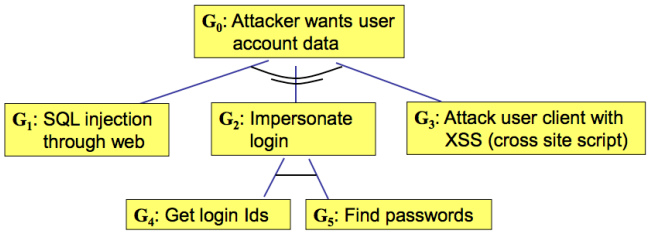
1. Likelihood / frequency of each type of incident
2. Impact on assets (loss) resulting from each type of incident



Threat scenario modelling:

- **Attacker-centric** – Starts from attackers, evaluates their goals, and how they might achieve them through attack tree. Usually starts from entry points or attacker action.

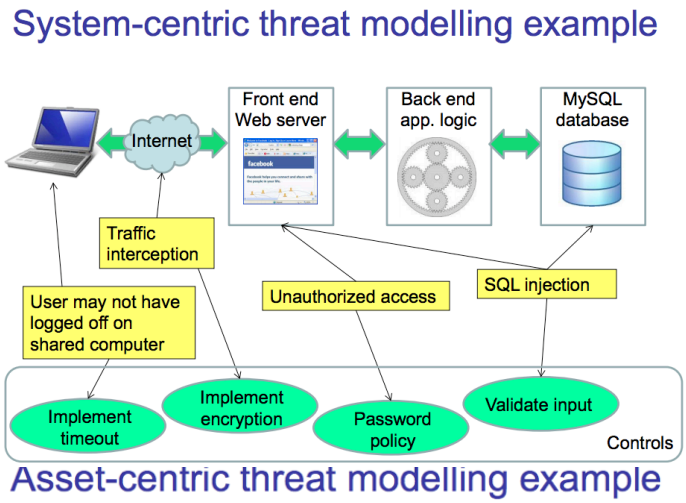
Attacker-centri



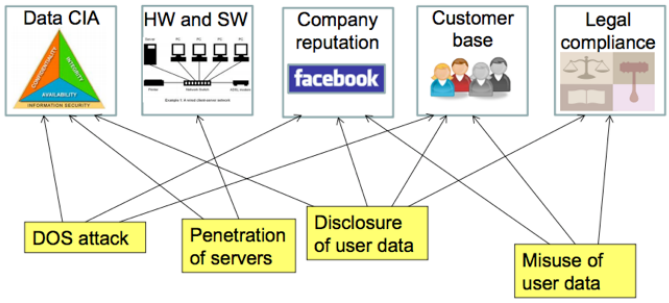
Legend:
G_0: Main goal — AND (conjunctive) all subgoals needed — OR (disjunctive) any subgoal needed

Probability of attack success: $p(G_0) = 1-(1-p(G_1))\cdot(1-(p(G_4)p(G_5)))\cdot(1-p(G_3))$

- **System-centric** (aka. SW-, design-, architecture-centric) – Starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model. This approach is e.g. used for threat modeling in Microsoft's Security Development Lifecycle.



- **Asset-centric** – Starts from assets entrusted to a system, such as a collection of sensitive personal information, and attempts to identify how security breaches of CIA properties can happen.



Models for risk level estimation:

Qualitative

- Uses descriptive scales. Example:
  - Impact level: Minor, moderate, major, catastrophic
  - Likelihood: Rare, unlikely, possible, likely, almost certain

Increasing Likelihood

Likelihood	Description
High	Is expected to occur in most conditions (1 or more times per year).
Medium	The event will probably happen in most conditions (every 2 years).
Low	The event should happen at some time (every 5 years).
Unlikely	The event could happen at some time (every 10 years).

Increasing Impact

Impact	Description
Major	**Major problems** would occur and threaten the provision of important processes **resulting in significant financial loss**.
Moderate	**Services would continue**, but would **need to be reviewed or changed.**
Minor	Effectiveness of services would be **threatened but dealt with**.
Insignificant	Dealt with as a part of **routine operations**.

Quantitative

- Use numerical values for both consequence (e.g. $$$) and likelihood (e.g. probability value)
- *Example quantitative **risk analysis method***
  - Quantitative parameters
    - Asset Value (AV)
      - Estimated total value of asset

    - Exposure Factor (EF)
        - Percentage of asset loss caused by threat occurrence
    - Single Loss Expectancy (SLE)
        - SLE = AV × EF
    - Annualized Rate of Occurrence (ARO)
        - Estimated frequency a threat will occur within a year
    - Annualised Loss Expectancy (ALE)
        - ALE = SLE × ARO
- *Example quantitative **risk analysis***
    - Risk description
        - Asset: Public image (and trust)
        - Threat: Defacing web site through intrusion
        - Impact: Loss of image
    - Parameter estimates
        - AV(public image) = $1,000,000
        - EF(public image affected by defacing) = 0.05 – SLE = AV × EF = $50,000
        - ARO(defacing) = 2
        - ALE = SLE × ARO = $100,000
    - Justifies spending up to $100,000 p.a. on controls

- *Semi-quantitative*
    - Qualitative scales assigned numerical values
    - Can be used in formulae for prioritization (with caution)

Semi-quantitative risk levels: Multiply likelihood & impact level

Risk Level / Likelihood	Impact level: (0) Nil	(1) Insign.	(2) Minor	(3) Moderate	(4) Major
(4) High	(0) Nil	(4) M	(8) H	(12) VH	(16) E
(3) Medium	(0) Nil	(3) L	(6) M+	(9) H+	(12) VH
(2) Low	(0) Nil	(2) VL	(4) M	(6) M+	(8) H
(1) Unlikely	(0) Nil	(1) Neg	(2) VL	(3) L	(4) M
(0) Never	(0) Nil	(0) Nil	(0) Nil	(0) Nil	(0) Nil

M: moderate; Specify responsibililty
L: low; Manage by routine procedures
VL: very low; Manage by routine
Neg: Negligible; To be ignored
Nil: Nil; No risk exists

E: extreme; Immediate action required
VH: very high; Priority action action
H+: high +; Management attention
H: high; Management attention
M+: moderate +; Specifu responsib

Risk treatment strategies

- Reduce, share, retain, avoid
- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
    - **Reduce/mitigate risk** (security and mitigation controls)
    - **Share/transfer risk** (outsource activity that causes risk, or insure)
    - **Retain risk** (understand tolerate potential consequences)
    - **Avoid risk** (stop activity that causes risk)
- Identify options for risk treatment by seeking opportunities that might increase positive outcomes without increasing the risk.
- **Options include**:
    - **Actively seek** an opportunity for creating value and profit
    - **Change the likelihood of opportunity** to enhance the likelihood of beneficial outcome
    - **Change the consequences** to increase the extent of the gains
    - **Sharing** the opportunity
    - **Retain** the residual opportunity
- Compare

- the level of risk found during risk analysis with
- the established risk criteria
- NOTE: Consider analysis and criteria on same basis - qualitative or quantitative

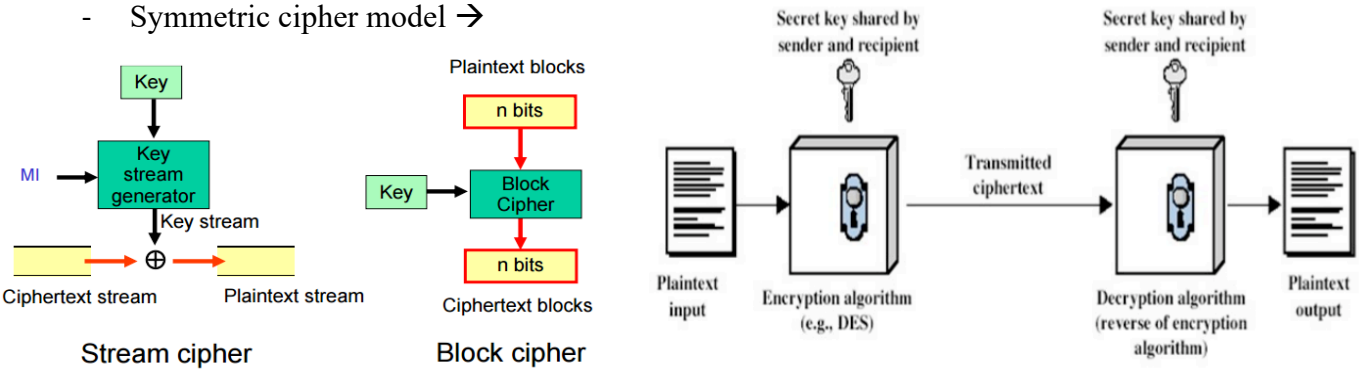
- Output: prioritized list of risks for further action
  - Risks in low or acceptable risk categories, may be accepted without further treatment

Cryptography

Cryptography is the science of secret writing with the goal of hiding the meaning of a message.
Cryptanalysis is the science and sometimes art of breaking cryptosystems.

Symmetric ciphers (one key)

- Secret key, used for both encryption and decryption and most widely used symmetric ciphers are DES (Data Encryption Standard) and AES (Advanced Encryption Standard).
- Symmetric chippers are divided into stream and block cipher
- Stream ciphers are used in wireless network to protect data confidentiality, but it cannot be used for integrity protection, because of precise relative changes to the plaintext by modifying the corresponding ciphertext bits.
- Symmetric cipher model →



Block ciphers can be used in different modes
in order to provide different security services, like:

- **E**lectronic **C**ode **B**ook (ECB)
- **C**ipher **B**lock **C**haining (CBC)
- **O**utput **F**eed**b**ack (OFB)
- **C**ipher **F**eed**b**ack (CFB)
- **C**oun**t**e**r** Mode (CTR)
- **G**alois **C**ounter **M**ode (GCM) {Authenticated encryption}

AES – Advanced Encryption Standard
Public competition to replace DES: because 56-bit keys and 64- bit data blocks no longer adequate.
The new AES, *Rijndea*[1]*l* has a block size of 128 bits, and a key size of 128-bit, 196-bit, and 256-bit key sizes.

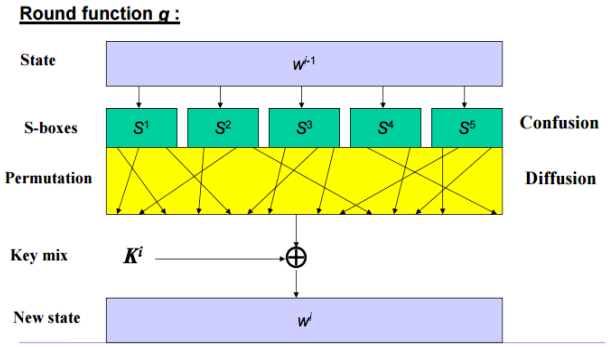
[1] Designed by Vincent Rijmen and Joan Daemen (Belgians)

Factors affecting the strength of ciphers and modes
Key length, symmetric and Asymmetric ciphers offering comparable security. →

AES Key Size	RSA Key Size	Elliptic curve Key Size
-	1024	163
128	3072	256
192	7680	384
256	15360	512

Substitution-permutation to erase statistical patterns (SPN) →

Substitusjon-Permutasjon nettverk (SPN):

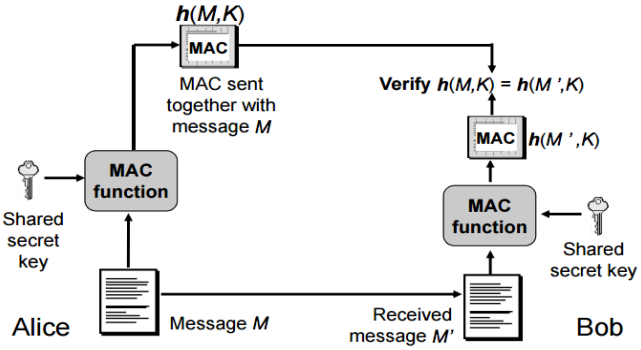


security by obscurity → Building a weak SW, just because 'nobody' knows the vulnerabilities.

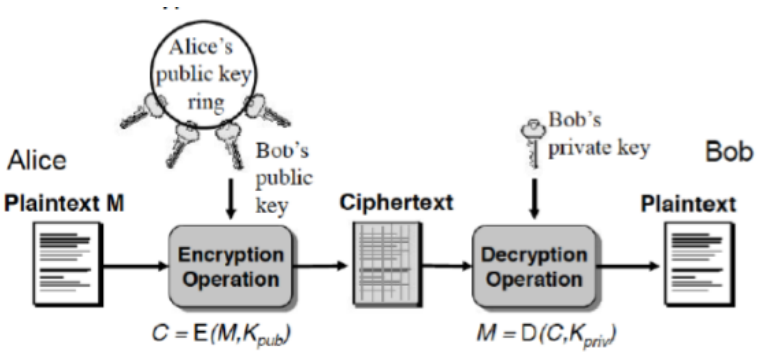
MAC – Message Authentication Code
MAC has to meanings,
1. The computed message authentication code *h (M, k)*
2. General name for algorithms used to compute a MAC
In practice MAC algorithms:

- **H**ash-based **MAC** algorithm (HMAC)
- **CBC** (cipher block chaining) based **MAC** algorithm (CBC-MAC)
- **C**hiper-based **MAC** algorithm (CMAC)

A message with simple message hash h(M) can be changed by attacker.
Purpose: MAC is for authenticating the origin of data
MAC can use hash function as h(M, k) i.e., with message M and a secret key k as input.
MAC algorithms, a.k.a. keyed hash functions[2], support data origin authentication services.



Asymmetric ciphers (two keys)
Asymmetric ciphers: pair of private and public keys where it is computationally infeasible to derive the private decryption key from the corresponding public encryption.
RSA --- best known *asymmetric* algorithm
Private keys are needed for confidentiality protection, while public keys are needed for integrity/authenticity protection.
Asymmetric encryption →

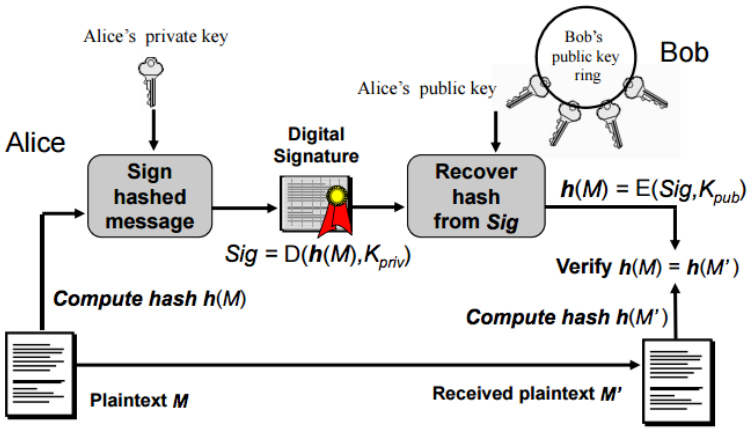


Digital Signatures:
A MAC cannot be used as evidence that should be verified by a third party. Digital signatures are **used for** *non-repudiation, data origin authentication* and *data integrity services*, and in some *authentication exchange mechanisms*.

[2] a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be one-way function, that is, a function which is infeasible to invert.

Digital signature mechanisms have three components: **key generation**, **signing procedure** (private) and **verification procedure** (public).

Practical digital signature based on hash value →



To get an authentication service that links a document to A's name (identity) and not just a verification key, we require a procedure for B to get an authentic copy of A's public key. **Only then** do we have a service that proves the authenticity of documents 'signed by A'.
This can be provided by a PKI (Public Key Infrastructure)

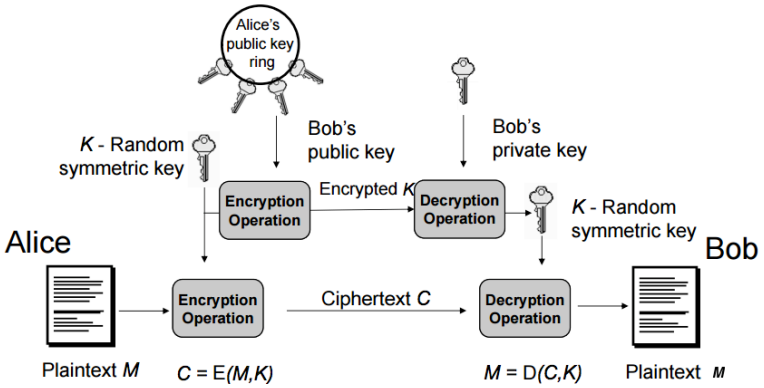
Difference between MAC and digital signature

They are both authentication mechanisms. When using MAC, the verifier needs the secret key that was used to compute the MAC. MAC cannot be used as evidence with a third party. (The third party cannot distinguish between the parties knowing the secret).
Digital signatures can be validated by third parties, and can in theory support both non-repudiation and authentication.

Hybrid Crypto Systems

Hybrid system are used where only symmetric session keys is encrypted with asymmetric algorithm. **Hybrid cryptosystems** works like this: symmetric ciphers are faster than asymmetric ciphers because they are less computationally expensive, but asymmetric ciphers simplify key distribution, therefore a combination of both symmetric and asymmetric ciphers can be used – a hybrid system.

- The asymmetric cipher is used to distribute a randomly chosen symmetric key.
- The symmetric cipher is used for encrypting bulk data.



The perfect cipher?

An attackers goal is to discover the secret key. If you require confidentiality, the One Time Pad is provably secure. But we don't use it due to its disadvantages. Its disadvantages are that each key can only be used once, each key is typically very large and it requires secure distribution of large key. Key management is therefore difficult. In the One Time Pad cipher, the encryption and decryption operations are identical.

Key Management

The strength of cryptographic security depends on:

1. The size of the keys
2. The robustness of cryptographic algorithms/protocols
3. The protection and management afforded to the keys

Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys. Key management is essential for cryptographic security.
Poor key management may easily lead to compromise of systems where the security is based on cryptography, for example using one key for two purposes.

Cryptoperiod = (protection period + processing period)
The crypto period is the time span[3] during which a specific key is authorized for use. The crypto period is **important because** it:

- Limits the amount of information, protected by a given key, that is available for cryptanalysis.
- Limits the amount of exposure and damage, should a single key be compromised.
- Limits the use of a particular algorithm to its estimated effective lifetime.

A key shall not be used outside of its specified period. The processing period (decryption stage) can continue after the protection period (encryption stage).

- **Factors affecting crypto periods**
  - In general, as the sensitivity of the information or the criticality of the processes increases, the crypto-period should decrease in order to limit the damage resulting from compromise.
  - Short crypto-periods may be counter-productive, particularly where denial of service is the paramount concern, and there is a significant overhead and potential for error in the re- keying, key update or key derivation process.
  - The crypto-period is therefore a **trade-off**

Recommended time limit for usage of AES[4], RSA and ECC[5] keys

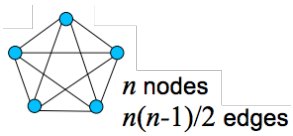
- RSA has a recommended time limit for each RSA key, the 2048-bit RSA key has an estimated limit to 2030. The 1024-bit key was recommended to stop using after 2010. 1024-bit keys are to small for todays usage.

Key distribution problem. Understand requirements for

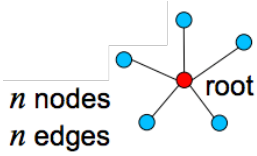
The problem with key distribution is that we want every pair of nodes to be able to communicate securely under cryptographic protection.

Number of key distributions with and without PKI:

The number needed for key distribution is **n(n-1)/2**, this is in both **public asymmetric** and **secret symmetric keys**, in this case it's very impractical in open networks, such as the internet. Works for smaller originations however.
Symmetric keys Confidentiality, is no one can see the information.
Asymmetric Authentication, is the process of proving who you are.



Asymmetric public keys with PKI: Authenticity required. Basically that every user gives the public key to the root, and the root will digitally sign it. PKI can do this, however it's hard to get through. However, this type is easily hack-able, for instance if someone switches out your public key number, they can suddenly get access to your information.



[3] from the beginning of the protection period to the end of the processing period
[4] Advanced Encryption Standard
[5] Elliptic curve cryptography

Type of protection needed /confidentiality or integrity

- In a domain of n entities, each pair of entities must be able to communicate securely. For each case A, B, & C, state:

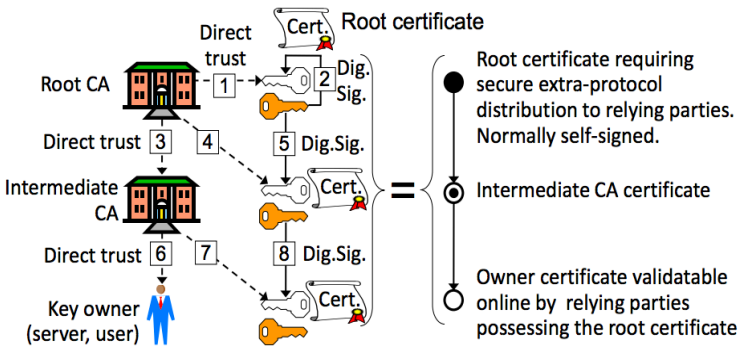
I. How many different keys are needed?
II. How many initial key distributions are needed, and ?
III. What key protection (confidentiality or integrity) is needed.

A: Symetric keys:
for: n(n-1)/2 different keys needed.
for: n(n-1)/2 distributions (or n(n-1), since 2 parties must receive each key)
for: Secret key protection: Confidentiality
B: Public/private-key cryptography without PKI
for: n different public/private key pairs needed (n keys or 2n keys acceptable)
for: n(n-1)/2 distributions, because every entity sends its public key to the others.
for: Public key protection: Integrity
C: Public/private-key cryptography with PKI (1 root CA and no intermediate CAs)
for: n + 1 different public/private key pairs needed. ("n key pairs" is acceptable)
for: n distributions of the root public key are needed.
for: Root public key protection: Integrity.

Requires confidentiality and integrity protection – Periods of protection for seeds, e.g.:
a. Used once and destroyed
b. Used for multiple keys, destroyed after last key generation
c. Kept and destroyed at the end of the protection period

PKI – public-key infrastructure
The main purpose of a PKI[6] is to ensure authenticity of public keys.
PKI consists of:

- Policies (to define the rules for managing certificates)
- Technologies (to implement the policies and generate, store and manage certificates)
- Procedures (related to key management)
- Structure of public key certificates (public keys with digital signatures)



PKI trust models:

- Each user is **completely responsible** for deciding which public keys to trust.
- Advantages:
  - Simple and free
  - Works well for a small number of users
  - Does not require expensive infrastructure to operate
  - User-driven grass-root operation
- Disadvantages:
  - More effort, and relies on human judgment
    - Works well with technology savvy users who are aware of the issues. Does not work well with the general public.

[6] Public-key infrastructure

- Not appropriate for more sensitive and high risk areas such as finance and government

PKI Summary

- Public key cryptography needs a PKI to work
  - Reduces number of key distributions from quadratic to linear.
  - Digital certificates used to provide authenticity and integrity for public keys.
  - Acceptance of certificates requires trust.
  - Trust relationships between entities in a PKI can be modelled in different ways.
  - Establishing trust has a cost, e.g. because secure out-of-band channels are expensive.

Computer Security

Approaches to strengthening platform security

- Harden the operating system
  - SE (Security Enhanced) Linux, Trusted Solaris, Windows 7/8/10
- Add security features to the CPU
  - Protection Layers, NoExecute, ASLR
- Virtualization technology
  - Separates processes by separating virtual systems
- Trusted Computing
  - Add secure hardware to the commodity platform
  - E.g. TPM (Trusted Platform Module)
- Rely on secure hardware external to commodity platform
  - Smart cards, Hardware tokens

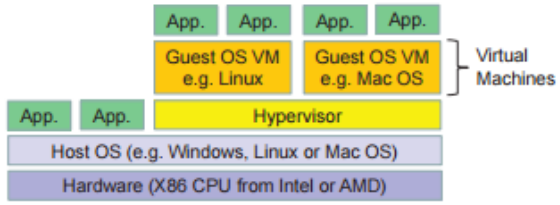
The **trusted computing base** (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.

Reference monitor is the security model for enforcing an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system.

Protection rings in microprocessor architecture

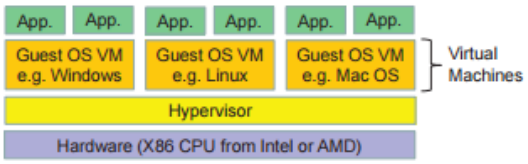
- The level hierarchy goes from level 0 and out if OS security kernel is as reference monitor, the levels depends on how privileged. **Level 0** contained the OS Kernel, **level 1 and 2** contained OS Services and **level 3** had the Applications. When the **hypervisor** was introduced in 2006, they added another level, so from 2006, the protection ring structure starts from level -1.

Type 2 VM Architecture (simple virtualization)



- Hypervisor runs on top of host OS
- Performance penalty, because hardware access goes through 2 OSs
- Traditionally good GUI
- Traditionally good HW support, because host OS drivers available

Type 1 VM Architecture (full virtualization)



No host OS
Hypervisor runs directly on hardware
High performance
Traditionally limited GUI, but is improved in modern versions
HW support can be an issue

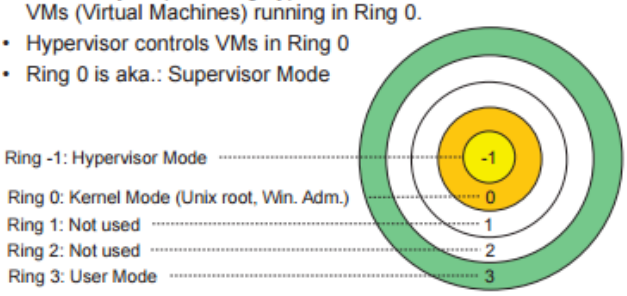
Virtual machines

Virtual machine is a software implementation of a machine (OS) that executes programs like a real machine (traditional OS). **Hypervisor** (aka. Virtual Machine Monitor) is needed to **manage** multiple guest Oss in the same hardware platform.

Challenges of running Virtual Machines

- VMs and Apps in a VM must not know that Hypervisor exists or that they share hardware (HW) resources with other VMs.
- Hypervisor must protect other VMs.
- Hypervisor must protect itself from all VMs
- Hypervisor must present virtual hardware interface to VMs.

- New Ring -1 introduced for virtualization.
- Necessary for protecting hypervisor from VMs (Virtual Machines) running in Ring 0.
- Hypervisor controls VMs in Ring 0
- Ring 0 is aka.: Supervisor Mode



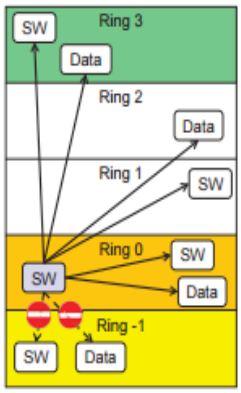
Why use platform virtualization

- Efficient use of hardware and resources
  - Improved management and resource utilization
  - Saves energy
- Improved security – Malware can only infect the VM
  - Safe testing and analysis of malware
  - Isolates VMs from each other
- Distributed applications bundled with OS
  - Allows optimal combination of OS and application
  - Ideal for cloud services
- Powerful debugging
  - Snapshot of the current state of the OS
  - Step through program and OS execution
  - Reset system state

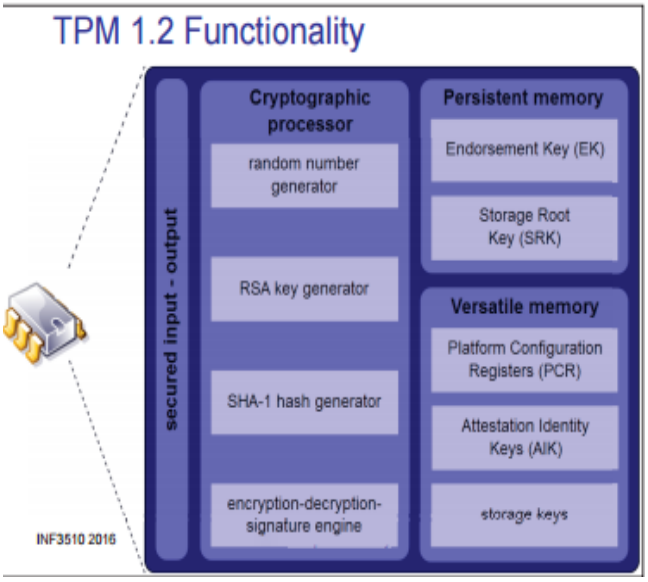
A process can access and modify any data and software at the same or less privileged level as itself.

A process that runs in kernel mode (Ring 0) can access data and SW in Rings 0, 1, 2 and 3
- but not in Ring -1

The goal of attackers is to get access to kernel or hypervisor mode.
- through exploits
- by tricking users to install software



• Security functions supported by TPM



- TPM is a chip that sits on the motherboard and the name of a standard. TPM chip at the heart of hardware / software approach to trusted computing.
- In a nutshell: a platform used for crypto processes.
- It's not an active process, thereby it's passive, and will only be called by the OS
- Supports 3 basic services:
    - Authenticated measured boot: Report the integrity status of the software when booting.
    - Sealed storage: Decryption with secret keys only ico. Correct integrity.
    - Remote attestation: Report to external party the integrity status of software
- Private keys are stored in secure non-volatile memory inside the TPM. Can not exit TPM. Can only be used inside TPM.

User Authentication

A credential is the 'thing' used for authentication, may also be referred to as a "token" or "authenticator". Credential categories:

1. Knowledge-Based (**Something you know**): Passwords
    - **Problems**:
        - Easy to share (intentionally or not)
        - Easy to forget
        - Often easy to guess (weak passwords)
        - Can be written down (both god and bad)
            - If written down, then "what you know" is "where to find it"
        - Often remains in memory and cache
2. Ownership-Based (**Something you have**): Tokens
   Types of authentication tokens:
    a. **Clock-Based Tokens**
        - The token displays time-dependent code on display, the user has to copy the code to log in. Possession of the token is necessary to know the correct value for the current time. Each code computed for specific time window. Clocks must be synchronized, an *example* is BankID.
    b. **Counter-Based Tokens**
        - Counter-based tokens generate a 'password' result value as a function of an internal counter and other internal data, without external inputs. A counter-based token exists between the client's token and the authentication server. *Example*: bombrikke, registrerer per gang du kjører, ikke tids synkronisert.
    c. **Challenge-Response Tokens**
        - A challenge is sent in response to access request
            - A legitimate user can respond to the challenge by performing a task which requires use of information only available to the user (and possibly the host)

        - User sends the response to the host (Access is approved if response is as expected by host.)
        - **Advantage**: Since the challenge will be different each time, the response will be too – the dialogue can not be captured and used at a later time
3. Inherence-Based (**Something you are/do**): Biometrics
    - Biometrics are automated methods of verifying or recognizing a person based upon a physiological characteristic.
    - Requirements:
        - **Universality:** each person should have the characteristic;
        - **Distinctiveness:** any two persons should be sufficiently different in terms of the characteristic;
        - **Permanence:** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
        - **Collectability:** the characteristic should be measurable quantitatively.
    - Practical considerations:
        - **Accuracy:** the correctness of a biometric system, expressed as ERR (Equal Error Rate), where a low ERR is desirable.
        - **Performance:** the achievable speed of analysis, the resources required to achieve the desired speed,
        - **Acceptability:** the extent to which people are willing to accept the use of a particular biometric identifier (characteristic)
        - **Circumvention resistance:** the difficulty of fooling the biometric system
        - **Safety:** whether the biometric system is safe to use
    - Modes of operation:
        - **Enrolment:** analog capture of the user's biometric attribute. Processing of this captured data to develop a template of the user's attribute which is stored for later use.
        - **Identification** (1:N, one-to-many)**:** capture of a new biometric sample. Search the database of stored templates for a match based solely on the biometric.
        - **Verification** of claimed identity (1:1, one-to-one)**:** capture of a new biometric sample. Comparison of the new sample with that of the user's stored template.

a. physiological biometric characteristics
    - *Examples*: fingerprint, facial recognition, eye retina/iris scanning, hand geometry, etc.

b. behavioral biometric characteristics
    - *Examples:* keystroke dynamics, written signatures, speech patterns/ voice print etc.

Password security

- The main problem with creating good passwords is not the users, it's the way hackers think. They are using huge databases, with possible combination, which makes the time from exponential to linear. You can reuse passwords, however in low sensitivity
- Strategies are:
    - User education → Not necessarily with strict enforcement. However, it's like smoking, people (IT security) usually have weak passwords.
    - Proactive password → Users test a potential password. (grønn, rød)

- Reactive passwords → Admins run cracking tools, to detect weak passwords.
- Computer-generated passwords → Random passwords from a system. Usually very strong, however difficult to remember.

Hashing

- Using hash values or encrypted on a password file is a logical strategy. Hash functions are practically impossible to crack.
- Hackers use a hashtable, on a couple TB, and a compressed called a rainbow tables.

Salting

- Used to prevent Rainbow tables or hash tables.
- Salting means to add a random number to the password, before it's hashed.
- ***This makes it nearly impossible for the crackers to find the data.***
- Takes away the advantages of pre-computing hash tables, because the salt is different for each user.
- ***Password salting ensures that equal passwords have different hashes***

E-Government user authentication frameworks

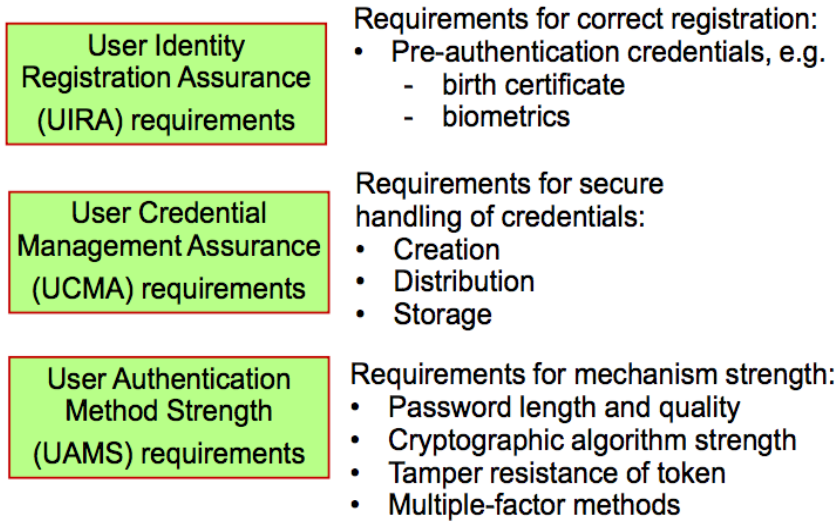
- Trust in identity is a requirement for e-Government
- Authentication assurance produces identity trust.
- Authentication depends on technology, policy, standards, practice, awareness and regulation.
- Consistent frameworks allow cross-national and cross-organizational schemes that enable convenience, efficiency and cost savings.

Assurance levels

No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
Level 0	Level 1	Level 2	Level 3	Level 4
No registration of identity required	Minimal confidence in the identity assertion	Low confidence in the identity assertion	Moderate confidence in the identity assertion	High confidence in the identity assertion

Assurance requirement classes

- Authentication Method strength
- Credential Management Assurance
- Registration Assurance

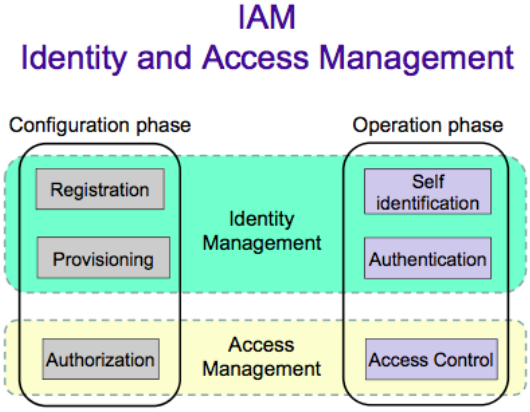


Identity and Access Management

• Meaning of entity/identity/identifier/digital identity

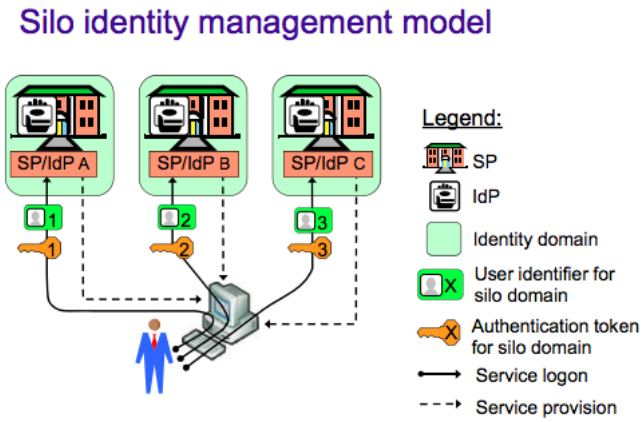
- **Entity:** can be a person, organization, agent, system, etc.
- **Identity:** "same one as last time".
  - A set of names / attributes of entity in a specific domain
  - An entity may have identities in multiple domains
  - An entity may have multiple identities in one domain
- **Identifier:** a name that identifies (that is, labels the identity of) either a unique object or a unique class of objects.
- **Digital identity:** Digital representation of names / attributes in a way that is suitable for processing by computers.

• IAM phases and steps: diagram.



Silo Id domains

- SP (Service Provider) = IdP (Identity Provider): SP controls name space and provides access credentials
- Unique identifier assigned to each entity
- **Advantages:** Simple to deploy, low cost for SPs
- **Disadvantages:** Identity overload for users, poor usability, lost business



Identity Federation Roles

- User – Need identities and credentials to access multiple SPs.
- Service Provider (SP) – Needs to know identity of users, and needs assurance of authenticity.
- Identity Provider (IdP) – Controls name space of identities. Issues/registers identities for users.
- Credentials Provider (CrP) – Issues/registers credentials for users. Performs authentication of users.

Identity Federation

- Identity Federation
  - A set of agreements, standards and technologies that enable a group of SPs to recognize user identities and credentials from different IdPs, CrPs and SPs.

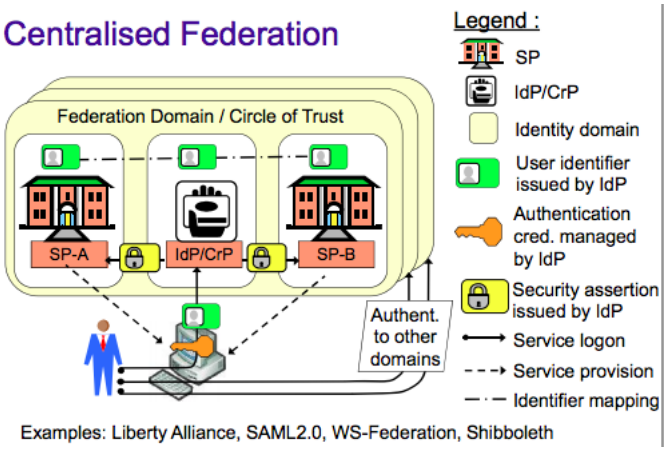
- Three main architectures:

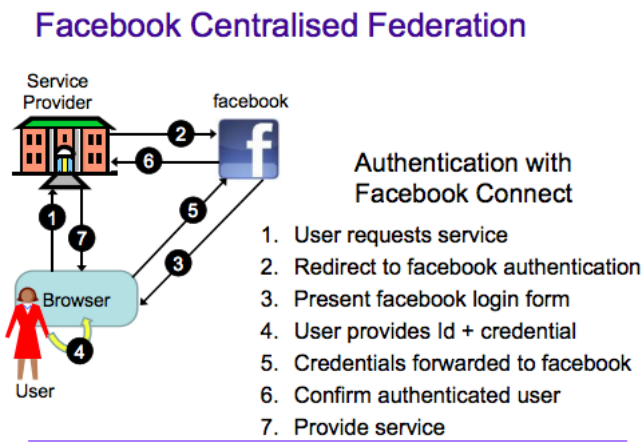
1. **Centralized Federation**: Centralized management of name space and credentials by single IdP/CrP.
2. **Distributed Federation**: Distributed management of name space and credentials by multiple IdPs and CrPs. Normally combined IdP/CrP.
3. **Centralized Identity with Distributed Authentication**: Centralized management of name space by single IdP. Distributed mgmt. of credentials and authentication by multiple CrPs.

Identity federation **usually based on** SAML protocol (Security Assertions Markup Language)
- Involves multiple entities: user, IdP, CrP, SP, and sometimes broker entity.

Advantages
- Improved usability
- Allows SPs to bundle services and collect user info
- Strengthen privacy through pseudonym identities

Disadvantages
- High technical and legal complexity
- High trust requirements
  - E.g. IdP is technically able to access SP on user's behalf.
- Privacy issues,
  - IdP collects info about user habits wrt. which SPs are used
- Limited scalability,
  - Limited by political and economical constraints
  - An Identity federation becomes a new form of silo

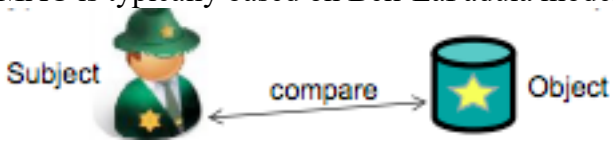




• Meaning and principle of MAC, DAC, RBAC and ABAC

MAC – Mandatory Access Control
- Access authorization is specified and enforced with security labels
  - Security clearance for subjects
  - Classification levels for objects
- MAC compares subject and object labels
- MAC is mandatory in the sense that users do not control access to the resources they create.
- A system-wide set of AC policy rules for subjects and objects determine modes of access.

- **MAC principles: Labels**
  - Security Labels can be assigned to subjects and objects
    - Can be strictly ordered security levels, e.g. “Confidential” or “Secret”
    - Can also be partially ordered categories, e.g. {Sales-dep, HR-dep}
  - Dominance relationship between labels
    - (L_A >= L_B) means that label L_A dominates label L_B
  - Object labels are assigned according to sensitivity
  - Subject labels are determined by security clearance
  - Access control decisions are made by comparing the subject label with the object label according to specific model
  - MAC is typically based on Bell-LaPadula model (see later)



DAC – Discretionary Access Control

- Access authorization is specified and enforced based on the identity of the user.
- DAC is typically implemented with ACL (Access Control Lists)
- DAC is discretionary in the sense that the owner of the resource can decide at his/her discretion who is authorized
- Operating systems using DAC: Windows and Linux

DAC principles

- AC Matrix
  - General list of authorizations
  - Impractical, too many empty cells
- Access Control Lists (ACL)
  - Associated with an object
  - Represent columns from AC Matrix
  - Tells who can access the object

Columns→ ↓Rows		Objects			
		O1	O2	O3	O4
Subject names	S1	r,w	-	x	r
	S2	r	-	r	r,w
	S3	-	x	-	-
	S4	r,w	x	x	x

AC Matrix

AC lists →

	O1
S1	r,w
S2	r
S3	-
S4	r,w

	O2
S1	-
S2	-
S3	x
S4	x

	O3
S1	x
S2	r
S3	-
S4	x

	O4
S1	r
S2	r,w
S3	-
S4	x

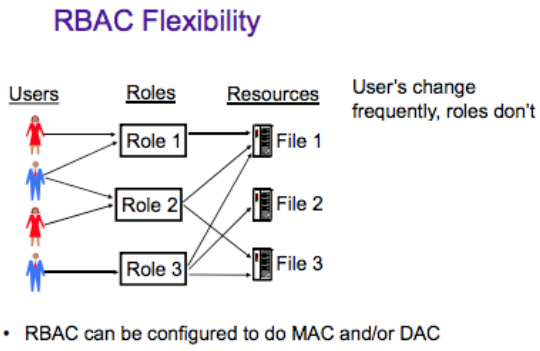
Combined MAC & DAC

- Combining access control approaches:
  - A combination of mandatory and discretionary access control approaches is often used
    - MAC is applied first,
    - DAC applied second after positive MAC
    - Access granted only if both MAC and DAC positive
  - Combined MAC/DAC ensures that
    - no owner can make sensitive information available to unauthorized users, and
    - ‘need to know’ can be applied to limit access that would otherwise be granted under mandatory rules

RBAC: Role Based Access Control

- A user has access to an object based on the assigned role.
- Roles are defined based on job functions.
- Permissions are defined based on job authority and responsibilities within a job function.
- Operations on an object are invocated based on the permissions.

- The object is concerned with the user's role and not the user.

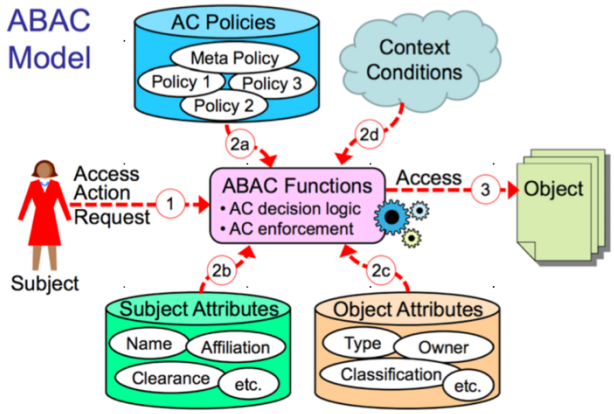


RBAC Privilege Principles

- Roles are engineered based on the principle of least privilege.
- A role contains the minimum amount of permissions to instantiate an object.
- A user is assigned to a role that allows her to perform only what's required for that role.
- All users with the same role have the same permissions.

ABAC: Attribute Based Access Control

- ABAC makes AC decisions based on Boolean conditions on attribute values.
- **Subject**, **Object**, **Context**, and **Action** consist of attributes
    - Subject attributes could be: Name, Sex, DOB, Role, etc.
    - Each attributes have a value, e.g.:
    - (Name (subject) = Alice), (Sex(subject) = F), (Role(subject) = HR-staff), (AccessType(action) = {read, write}), (Owner(object) = HR), (Type(object) = salary)



- The AC logic analyses all (attribute = value) tuples that are required by the relevant policy.
    - E.g. permit if: [Role(subject) = HR-staff) and (AccessType(action) = read) and (Owner(object) = HR)] and (Time(query) = office-hours)]
- ABAC specifies access authorizations and approves access through policies combined with attributes. The policy rules can apply to any type of attributes (user attributes, resource attribute, context attributed etc.).

ABAC: + and On the positive side:

- ABAC is much more flexible than DAC, MAC or RBAC
    - DAC, MAC and RBAC can be implemented with ABAC
- Can use any type of access policies combined with an unlimited number of attributes.
- Suitable for access control in distributed environments
    - e.g. national e-health networks

On the negative side:

- Requires defining business concepts in terms of XML and ontologies which is much more complex than what is required in traditional DAC, MAC or RBAC systems.
- Political alignment and legal agreements required for ABAC in distributed environments.

Communication Security

Network Security: two main areas

Communication Security: measures to protect the data transmitted across networks between organisations and end users.

Perimeter Security: measures to protect an organization's network from unauthorized access.

TLS (Transport Layer Security) / SSL (Secure Socket Layer):

Handshake Protocol

- The handshake protocol
    - Negotiates the encryption to be used
    - Establishes a shared session key
    - Authenticates the server
    - Authenticates the client (optional)
    - Completes the session establishment
- After the handshake, application data is transmitted securely •
- Several variations of the handshake exist: RSA variants **or** Diffie-Hellman variants

Handshake Four phases

- Phase 1: Initiates the logical connection and establishes its security capabilities
- Phases 2 and 3: Performs key exchange. The messages and message content used in this phase depends on the handshake variant negotiated in phase 1.
- Phase 4: Completes the setting up of a secure connection.

Elements of Handshake

- Client hello
    - Advertises available cipher suites (e.g. RSA, AES, SHA256)
- Server hello
    - Returns the selected cipher suite
    - Server adapts to client capabilities
- RSA and Server Certificate
    - X.509 digital certificate sent to client, assumes RSA algorithm
    - Client verifies the certificate including that the certificate signer is in its acceptable Certificate Authority (CA) list. Now the client has the server's certified public key.
- RSA and Client Certificate
    - Optionally, the client can send its X.509 certificate to server, in order to provide mutual authentication, assumes RSA algorithm
- Anonymous Diffie-Hellman
    - Optionally, the client and server can establish session key using the Diffie-Hellman algorithm

Record Protocol Overview

- Provides two services for SSL connections.
    - Message Confidentiality:
        - Ensure that the message contents cannot be read in transit.
        - The Handshake Protocol **establishes a symmetric key used to encrypt SSL payloads.**
    - Message Integrity:
        - Ensure that the receiver can detect if a message is modified in transmission.
        - The Handshake Protocol **establishes a shared secret key used to construct a MAC.**

Record Protocol Operation

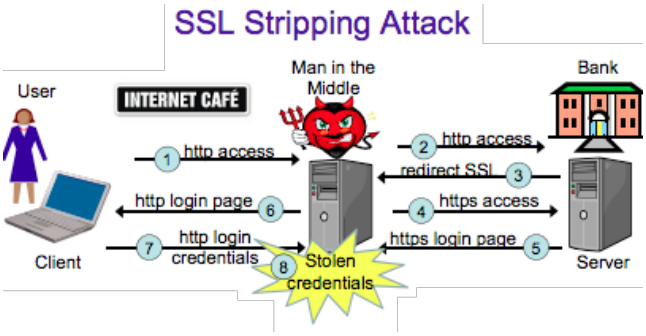
- Fragmentation:
    - Each application layer message is fragmented into blocks of 214 bytes or less.
    - Compression:
        - Optionally applied.
        - SSL v3 & TLS – default compression algorithm is null
    - Add MAC:

        - Calculates a MAC over the compressed data using a MAC secret from the connection state.
    - Encrypt:
        - Compressed data plus MAC are encrypted with symmetric cipher.
        - Permitted ciphers include AES, IDEA, DES, 3DES, RC4
        - For block ciphers, padding is applied after the MAC to make a multiple of the cipher's block size.

SSL Stripping Attack

Variations include:

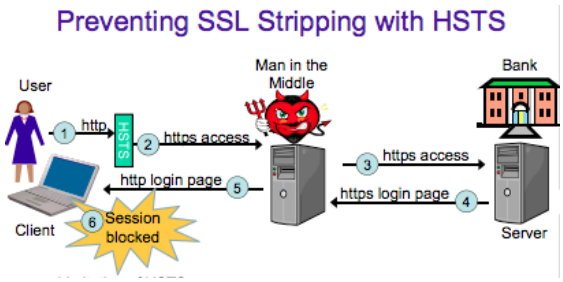
- MitM server can connect to client over https in msg (6) with server certificate that has similar domain name as real server.
- Attacker can leave the connection after stealing credentials, then the client connects directly to real server with https.



HSTS – HTTP Strict Transport Security

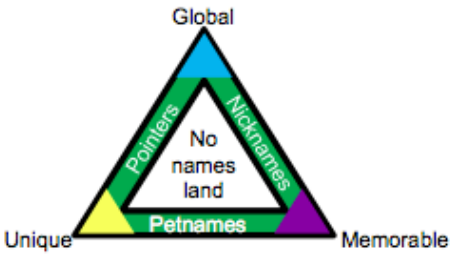
Preventing SSL Stripping

- A secure server can instruct browsers to only use https
- When requesting website that uses HSTS, the browser automatically forces connect with https.
- Users are not able to override policy
- Two ways of specifying HSTS websites
    - List of HSTS websites can be preloaded into browsers
    - HSTS policy initially specified over a https connection HSTS policy can be changed over a https connection
- *Disadvantages*
    - HSTS websites can not use both http and https
    - Difficult for a website to stop using https
    - Can cause denial of service, e.g. no fallback to http in case of expired server certificate
- Limitation of HSTS:
    - No HSTS policy defined in browser at first visit to secure website
- Can be solved by browser having preloaded list of HSTS websites
- Browsers would be vulnerable if attacker could delete HSTS cache



Zooko's Triangle of name properties

- No name class exists of names that are global, unique and memorable
- Name classes can only have 2 of the 3 required properties
- The edges of Zooko's triangle represent possible name classes:
    - Pointers, e.g. domain names, www.pepespizza.com
    - Petnames, personal names, e.g. "My favourite pizza restaurant"
    - Nicknames, local names, e.g. Pepe's Pizza



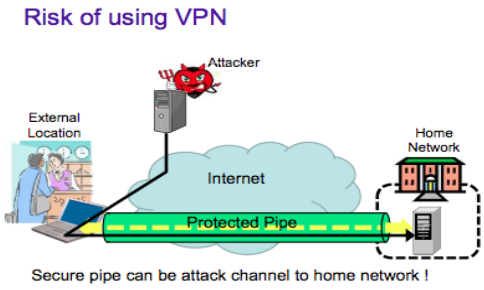
IPSec (Internet Protocol security)
The standard for secure communication over Internet Protocol (IP) networks, through the use of cryptographic security services. It uses encryption, authentication and key management algorithms. It is based on an end-to-end security model at the IP level and provides a security architecture for both IPv4 (Optional) and IPv6 (Mandatory). **Requires** operating system support, not application support.

IPSec: Security Services

- *Message Confidentiality.*
  - Protects against unauthorized data disclosure.
  - Accomplished by the use of encryption mechanisms.
- *Message Integrity.*
  - IPsec can determine if data has been changed (intentionally or unintentionally) during transit.
  - Integrity of data can be assured by using a MAC.
- *Traffic Analysis Protection.*
  - A person monitoring network traffic cannot know which parties are communicating, how often, or how much data is being sent.
  - Provided by concealing IP datagram details such as source and destination address.
- *Message Replay Protection.*
  - The same data is not delivered multiple times, and data is not delivered grossly out of order.
  - However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
- *Peer Authentication.*
  - Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate.
  - Ensures that network traffic is being sent from the expected host.
- *Network Access Control.*
  - Filtering can ensure users only have access to certain network resources and can only use certain types of network traffic.

IPSec: Protocols Types

- Encapsulating Security Payload (ESP)
  - Confidentiality, authentication, integrity and replay protection
- Authentication Header (AH)
  - Authentication, integrity and replay protection. However, there is no confidentiality
- Internet Key Exchange (IKE)
  - negotiate, create, and manage security associations

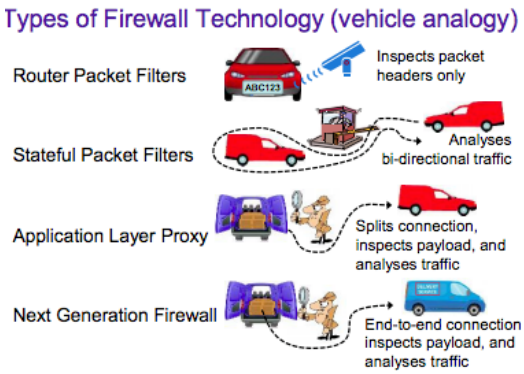


Risks of using IPSec for VPN

- IPSec typically used for VPN (Virtual Private Networks)
- A VPN client at external location may be connected to the Internet (e.g. from hotel room or café) while at the same time being connected to home network via VPN.
  - VPN gives direct access to resources in home network.
- Internet access from external location may give high exposure to cyber threats
  - No network firewall, no network IDS
- Attacks against the VPN client at external location can directly access the home net456work through VPN tunnel

Firewall

A firewall is a check point that protects the internal networks against attack from outside networks. The check point decide which traffic can pass in & out based on rules.



Router-based Packet Filter

A packet filter is a network router that can accept/reject packets based on headers. High speed, but primitive filter.

- Packet filters examine each packet's headers and make decisions based on attributes such as:
    - Source or Destination IP Addresses
    - Source or Destination Port Numbers
    - Protocol (UDP, TCP or ICMP)
    - ICMP message type
    - And which interface the packet arrived on

Host-based Packet Filters

A host can also perform packet filtering, in addition to performing other host tasks such as web serving.

- in this case the packet filter is designed to protect the host itself, not other hosts on the network

Common packet filter software includes:

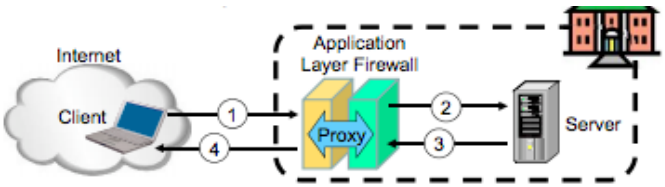
- IPChains for Linux (superseded)
- TCP Wrappers for various Unix
- IP Filter for Sun Solaris

Personal Firewalls

A personal firewall is a program that is designed to protect the computer on which it is installed. Personal firewalls are frequently used by home users to protect themselves from the internet. Personal firewalls are usually a stateful packet filter.

Application Layer Proxy

1. External client sends a request to the server, which is intercepted by the outwards-facing firewall proxy
2. Inwards-facing proxy sends request to server on behalf of client.
3. Server sends reply back to inwards-facing firewall proxy.
4. Outwards facing proxy sends reply to the client.
    a. Client and server both think they communicate directly with each other, not knowing that they actually talk with a proxy.
    b. The proxy can inspect the application data at any level of detail, and can even modify the data



Application Proxy Firewalls

Strengths:

- Easy logging and audit of all incoming traffic.
- Provides potential for best security through control of application layer data/commands.

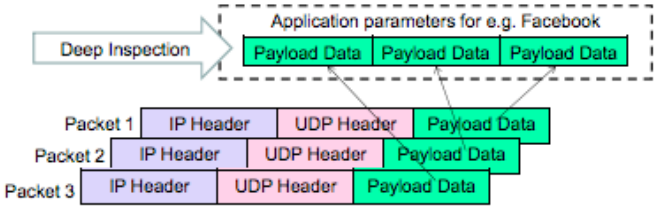
Weaknesses: – May require some time for adapting to new applications. – Much slower than packet filters. – Much more expensive than packet filters.

Next Generation Firewalls (NGFW)

- Inspects payload in end-to-end application connection
- Can support specific application protocols
  - e.g. http, telnet, ftp, smtp etc.
  - each protocol supported by a specific proxy HW/SW module
- Can be configured to filter specific user applications
  - E.g. Facebook, Youtube, LinkedIn
  - Can filter detailed elements in each specific user application
- Very high processing load in firewall
  - High volume needs high performance hardware, or else will be slow.

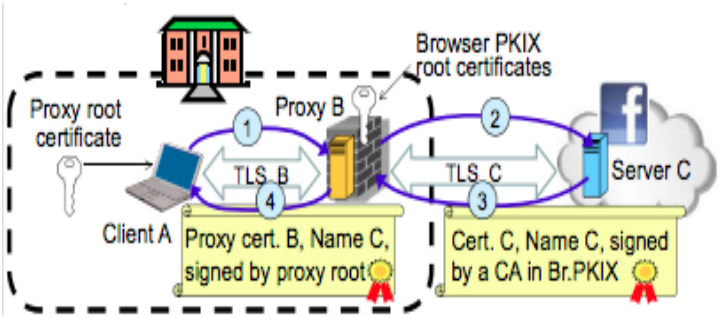
Deep Packet Inspection

- Deep Packet Inspection looks at application content instead of individual or multiple packets.
- Deep inspection keeps track of application content across multiple packets.
- Potentially unlimited level of detail in traffic filtering.



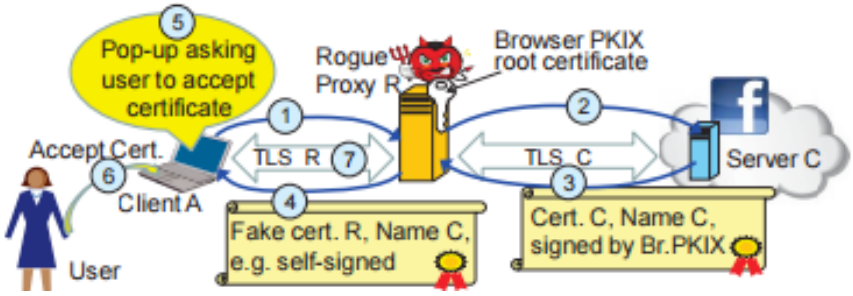
TLS/SSL content inspection in firewalls

- TLS designed for end-to-end encryption, normally impossible to inspect.
- In order to inspect TLS, proxy must pretend to be external TLS server.
- Proxy creates proxy server certificate with the name of external server (ex: facebook.com), signed by proxy root private key.
- Assumes that proxy root certificate is installed on all internal hosts.
- The proxy server certificate is automatically validated by internal client, so user may believe that he/she has TLS connection to the external server.



TLS inspection attack with rogue proxy server

- Depending on network, attackers may be able to install rogue proxy
- SSL inspect does not assume pre-installed client proxy root certificate
- Proxy creates fake server certificate with the name of external server (e.g. facebook.com), that e.g. can be self-signed
- Fake server certificate is not validated, so browser asks user to accept it
- Fake certificate has (name = domain dame), so browser sets up TLS, and user believes that he/she has TLS connection to the external server



WIFI security architecture

Terminology:

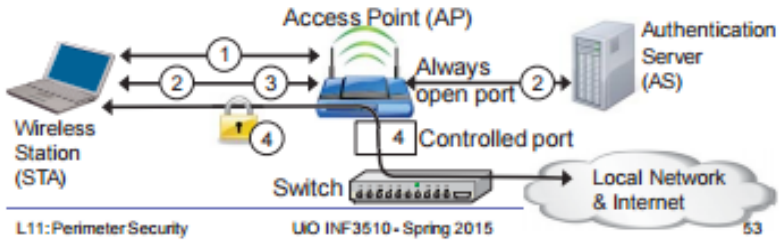
- WEP: Wired Equivalent Privacy (broken)
- WPA: WiFi Protected Access
- EAP: Extensible Authentication Protocol
- Station (STA) – Wireless terminal that communicates with 802.11 functionality
- Access Point (AP) – Receives radio signals and controls access to network
- Basic Service Set (BSS) – Set of stations and one AP
- Extended Service Set (ESS) – Set of multiple BSSs
- Distribution System (DS)
    - Contains an Authentication Server (AS)
    - Integrates multiple BSSs into one ESS

Only authorized terminals (or users) may get access through Wireless LAN. It should be impossible to set up rogue AP. Interception of traffic by radios within range should be impossible.

802.11i WiFi Access Control

1. Mutual identity request between STA and AP
2. Mutual authentication between STA and AS.
3. Derive pairwise master key (PMK) between STA and AP.
4. Encrypt radio link and open port (connect) to network access

- *Controlled port from AP to network*
    - is closed (disconnected) before authentication
    - is open (connected) after successful authentication



When you don't control the WLAN

- Often you want to connect to a wireless LAN over which you have no control, e.g. in café
- Options:
    - If you can, connect securely (WPA2, 802.11i, etc.)
        - Beware of SSL-stripping
    - If unsecured, connect to online resources securely:
        - Use a VPN (Virtual Private Network)
            - IPSEC connection to home gateway
            - TLS/SSL connections to secure web server (with HSTS)
    - Be careful not to expose passwords
    - Watch for direct attacks on untrusted networks

Application Security

The Open Web Application Security Project (OWASP) is a non-profit organization that promotes security awareness and security solutions for Web application development. OWASP Top-10 security risks identify the most critical security risks of providing online services. OWASP ASVS (Application Security Verification Standard) specifies requirements for application-level security. Provides and maintains many free tools for scanning and security vulnerability fixing.

Top-10 Web Application Risks (vulnerabilities)
1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

Main vulnerabilities

SQL Injection

SQL injection is misinterpretation of data input to database system, attacker disguises SQL commands as data-input or disguised SQL commands = 'injected' SQL commands. With SQL injection, an attacker can get complete control of database. No matter how well the system is patched or firewall is configured. Vulnerability exits when web application fails to sanitize data input before sending it to database. Flaw is in web application, not in SQL database.

Prevention of SQL Injection

Check and filter user input.

- Length limit on input (most attacks depend on long query strings).
- Different types of inputs have a specific language and syntax associated with them, i.e. name, email, etc
- Do not allow suspicious keywords (DROP, INSERT, SELECT, SHUTDOWN) as name for example.
- Try to bind variables to specific types.

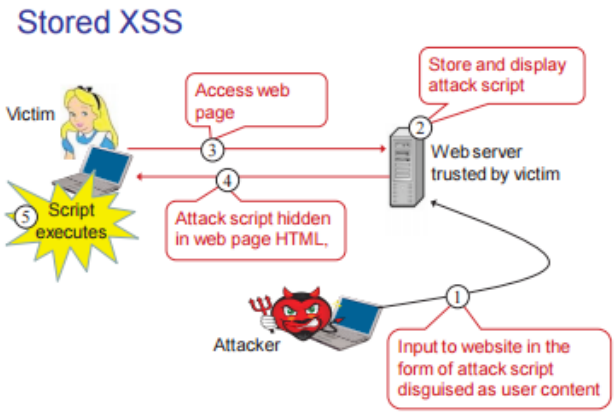
XSS - Cross-Site Scripting

XSS attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Stored XSS

- Data provided by users to a web application is stored persistently on server (in database, file system, …) and later displayed to users in a web page.

- Typical example: online message boards.
- Attacker uploads data containing malicious script to server.
- Every time the vulnerable web page is visited, the malicious script gets executed in client browser.
- Attacker needs to inject script just once.

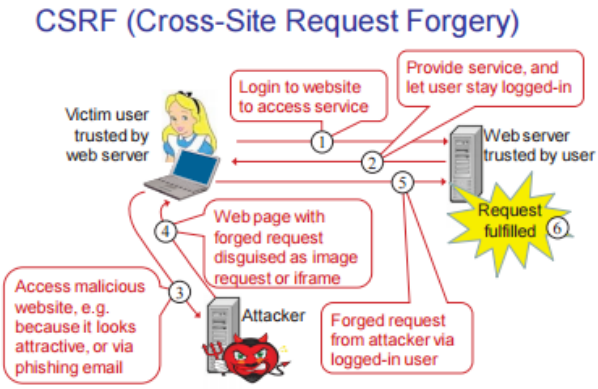


Reflected XSS

- Data provided by client is used by server-side scripts to generate results page for user.
- User tricked to click on attacker's link for attack to be launched; page contains a frame that requests page from server with script as query parameter.
- If unvalidated user data is echoed in results page (without HTML encoding), code can be injected into this page.
- Typically delivered via email, containing an innocently looking URL that contains a script.
    - E.g., search engine redisplays search string on the result page; in a search for a string that includes some HTML special characters' code may be injected.

XSS – The Problem

- Ultimate cause of the attack: The client only authenticates 'the last hop' of the entire page, but not the true origin of all parts of the page.
- For example, the browser authenticates the bulletin board service but not the user who had placed a particular entry.
- If the browser cannot authenticate the origin of all its inputs, it cannot enforce a code origin policy.



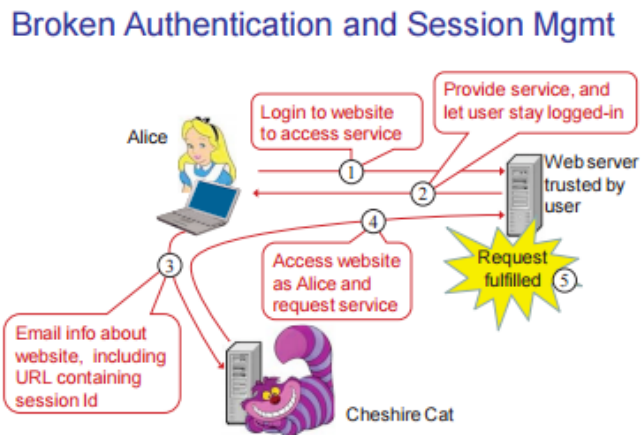
CSRF – Cross-Site Request Forgery

CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

Problem and Fix

- Users stay logged-in at websites even when not using them
    - Can be exploited by attackers sending fake requests via users
- Forged HTTP requests for a specific website that requires user login are hidden on attacker's webpage in the form of fake image requests, iframes or other elements.
- Browser accesses webpage and forwards forged requests.
- Preventing CSRF usually requires the inclusion of an unpredictable reference token (e.g. a random number) with each HTTP request to websites requiring login. Request tokens should at a minimum be unique per user session.
- Because the request token is unpredictable, the attacker is unable to create a forged request that will be accepted and fulfilled by the web server.

Broken authentication and session management



Authentication and session management includes all aspects of handling user authentication and managing active sessions. Authentication is a critical aspect of this process, but even solid authentication mechanisms can be undermined by flawed credential management functions, including password change, forgot my password, remember my password, account update, and other related functions.

Problem and Fix

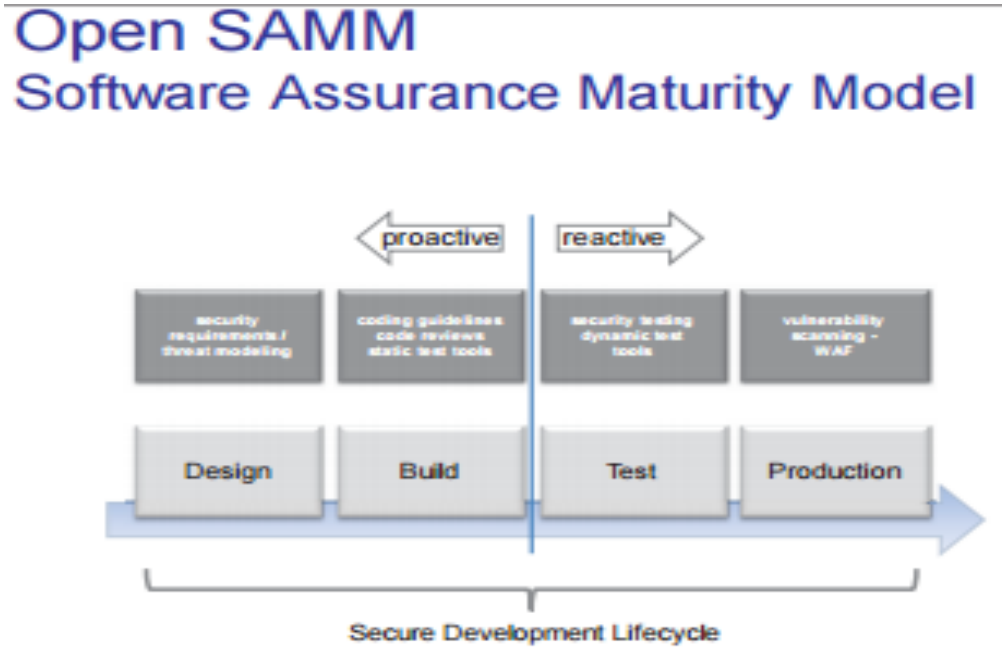
- Users stay logged-in at websites even when not using them
    - Can be exploited by attackers sending fake requests via users
- Forged HTTP requests for a specific website that requires user login are hidden on attacker's webpage in the form of fake image requests, iframes or other elements.
- Browser accesses webpage and forwards forged requests.
- Preventing CSRF usually requires the inclusion of an unpredictable reference token (e.g. a random number) with each HTTP request to websites requiring login. Request tokens should at a minimum be unique per user session.
- Because the request token is unpredictable, the attacker is unable to create a forged request that will be accepted and fulfilled by the web server.

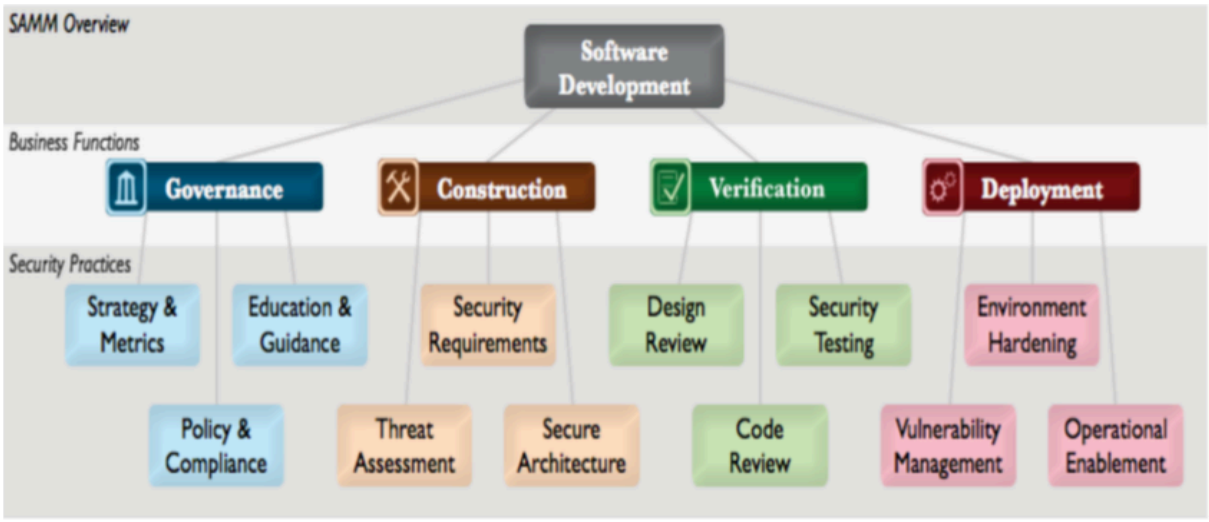
Secure Software development

SDLC: Software Development Life Cycle model contains 5 basic stages:

1. Requirements Specification
2. Design
3. Implementation
4. Verification and Testing
5. Deployment and Maintenance

Each SDLC model organises/integrates these basic stages in a specific way: Waterfall, Agile (XP: Extreme Programming), Iteration model, etc.





- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘silo’ for improvement The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘silo’ for improvement