Chapter 1

Security Engineering

1.1 Introduction

Confidentiality: preventing unauthorized disclosure of information

Availability: preventing of unauthorized withholding of information or resources

Integrity: preventing unauthorized modification of information

- Data Integrity: data are not modified by unauthorized individuals
- System Integrity: system performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Accountability: (track back the action of somebody)
the property of tracing security related actions/events to the responsible entity

Non-repudiation:
the property of having unforgeable evidence that an event/action has occured
non-repudiation of origin, non repudiation of delivery

Privacy (Often grouped with Confidentiality)
the right of an individual to control what data are collected and stored by who and to whom are disclosed

Unauthorized disclosure: Exposure, Interception, Inference, Intrusion
Deception: Masquerade, Falsification, Repudiation
Disruption: Incapacitation, Corruption, Obstruction
Usurpation: Misappropriation, Misuse
Threat: a potential cause of an unwanted incident

1.2 Terminology

Asset: something to which a party assigns value and hence for which the party requires protection

- Hardware: computer systems, data storage, data communication devices
- Software: operating systems, system utilities, applications, services
- Data: files and databases
- Communication Lines: local and wide area network communication links, router, gateways..

- Active: aim to modify system's assets or to affect their operation
  Preventing them is harder than detecting them
  e.g reply attack, SQL injection
- Passive: aim to learn or make use of information that not affect the systemsassets
  Detecting them is harder than preventing them
  e.g traffic analysis

1.3 Security Management

1. Identify Threats and Risk to your assets
2. itigate those with Security Controls
3. Deploy the Controls
4. Monitor their effectiveness
5. Check security indicators
6. Revise periodically

1.4 GRC

Governance
policies, laws, culture and institutions that define how an organization is managed/run and drives the strategy

Risk Management
the coordinated activities that direct and control an organization's risks

Compliance
the act of adhering to regulations as well as corporate policies and procedures

Example: San Raffaele
Private Hospitals Manage Drug Dispensation to Patients on behalf of Health Care Authority and Claim Reimboursement Afterward

- Some drugs are very expensive: huge financial issues
- Process is highly regulated
- Many steps are run by external actors

Privacy and security issues
Protect patient identity
Authenticate patients, doctors and nurses

Target is to "govern" the process, manage the risks and show compliance with law and show "we are in control"

Why is it important?
Investors in North America and Western Europe will pay a premium of 14 % for companies with good governance.

Companies adopt GRC to

1. Comply with regulations
2. Avoid failing an audit
3. Learn from a bad experience
4. Managing risks
5. Insure, improve and optimize an existing business

1.5 Security Management

It is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity inside an organization.

Some standards specify how to do it
ISO/IEC 27001 is the ”how”
ISO/IEC 27002 is the ”what”

Many different variations on how...
COSO, COBIT, SABSA, etc. etc.

COSO: Committee of Sponsoring Organizations of the Treadway Commission
Coso developed the Enterprise Risk Management

COBIT: Control Objectives for Information and related Technology

The ISO/IEC 2700x Family of Standards

- ISO/IEC 27001
  Describes the process to establish, implement, operate, monitor and maintain a security management process
- ISO/IEC 27002
  Provides a list of security control objectives and best practice security controls
- ISO/IEC 27005
  Security risk management

Chapter 2

IAM

2.1 IAM - Identity and Access Management

Definition 1 The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Definition 2 includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, then granting the correct level of access based on the protected resource, this assured identity, and other context information.

2.1.1 Policy

Definition A specification of what is a "correct level of access" and who are the "identities" for which this level is appropriate and the "contextual conditions".
Policy elements:

- Subject: user or process
- Object: files,directories,records (also a subject can be an object)
- Access right: read,write,execute,delete,create,search

Policy components:

- Target: subject,action,object
- Rule: if Condition is satisfied then applies the Effect (eg permit/deny) upon the Target
- Evaluation results: permit; Deny; Indeterminate;
- Evaluation Procedures (for rule selection): deny-ovveride,permit-ovverride
- Obligations: Security Actions that must be performed after the decision (bad practice)

Types of policy rules
Authorization: if conditions satisfied THEN then grant/deny access
Authorization with obligations: if conditions satisfied THEN then grant/deny access AND
check user FULFILL Obligation

Example:

- Time: ”file A must be deleted whithin a week”
- Cardinality: ”Play game at most twice before paying it”
- Event defined: ”If the document is revoked it must not be used”
- Purpose: for personal use only
- Environment: allow usage if firewall is installed

2.1.2 Key components of IAM

- Authentication: The verification an identity claimed by (or on behalf of) a system entity
  Eg. Social Security Number in Italy
- Authorization: The granting of a right (or permission) to the claimant system entity to access a system resource
  Eg. identity card in Italy, boarding pass in an airport
- Audit: The monitoring and processing of user accesses to system resources
  Eg. Assuming A. and I. are already done, decides whether identified principal can get access to resource

2.2 Authorization

- PAP - Policy Administration Point
  The (logical) system entity that creates a policy or policy set
- PEP - Policy Enforcement Point
  The (logical) system entity that performs access control, by asking decision requests and enforcing authorization decisions
  Eg. file system
- PDP - Policy Decision Point
  The (logical) system entity that evaluates applicable policy and renders an authorization decision
- PIP - Policy Information Point
  The (logical) entity that acts as a source of attribute values

Authorization
Use a reactive PEP + stateless PDP.
Easy to implement: If the users don’t ask anything you don’t need to remember and do anything.

(History Based) Authorization
Use a reactive PEP + stateful PDP.
Reasonable to implement: If the users don't do anything you might need to remember something but don't need to do anything

True obligation
Use a proactive PEP (obligation monitor) + stateful PDP
Costly to implement: even if the user don't do anything you must remember something, monitor users and eventually do something

Example 1 this is the reason why bancomat is free while credit card is not. With credit card user is monitored to check if he pays the amount due to the bank while with bankomat there is no need for it.

Example 2 Airport Security control before going into the gate

- Generic authorization "Anybody without forbidden items"
- List of "Forbidden Items" is provided by PAP
- X-ray scanner provide attributes
- Security officer at entrance is PDP and PEP

2.2.1 Access controls

- **Discretionary Access Control**
  Policy decided by individual subjects
  Access based on identity of subjects
  Structures: access matrix,capability list,access control list

- **Role based Access Control**
  Policy decided by system
  Roles are assigned access rights to resources:
  Users are assigned to roles
  Inherit access rights of the role they play
  Possibly add constraints or inheritance

  Example: Assistant professor,Post Doc,Phd student

- **Mandatory Access Control**
  Policy decided by system
  Subject assigned to security levels (clearance), Object assigned to security labels
  Access based on matching objects' labels to subjects' clearances

- **Credential based Access Control**
  Access based on attributes qualifying a subject

2.2.2 Bell-LaPadula Confidentiality model

It prevents low security level subjects to read high level security objects.
BLP elements

- S: set of subjects
- O: set of objects
- A: set of access operations (read,write,append,exceute)
- L: set of partially ordered security levels
  Top secret, secret,confidential,unclassified

BLP state

- $fs : S \to L$ assign to a subject maximum security level
- $fc : S \to L$ assign to a subject the current security level
- $fo : O \to L$ assign to an object its seurity level

BLP properties No read-up security policy:
A subject can only read an object of less or equal security level: $fo(o) \leq fs(s)$

No write-down policy
A subject can only write objects of greater of equal security level: $fs(s) \leq fo(s)$
Remark a high level subject is not able to send messages to a low level subject (there are several ways to escape from this restriction)

Limitations

- Restricted to confidentiality
- No policies for changing access rights
- BLP contains covert channels (information flow that is not controlled by the model)
  Telling a subject that a certain operation is not permitted constitutes information flow

2.3 Authentication

What is authentication?
It is the process of verifying a claimed identity.
It consists of two main steps:

- Identification (you announce who you are)
- Verification (you prove who you are)

Means of authentication

- Something the individual knows: password-based
- Something the individual owns: token-based
- Something the individual is: static biometric
- Something the individual does: dynamic biometrics
- Something the individual is: location based

2.3.1 Password authentication

Typical issues:

- how to get the password to the user
- forgotten passwords
- password guessing
- protection of the password file

Dangers:

- User accounts without password
- Unchanged default password
- Badly chosen passwords
- Passwords stored in the clear
- Passwords transmitted in the clear
- User forgets passwords

Proactive password checking

- Rule enforcement plus user advice
  8+ chars, upper/lower/numeric/punctuation
- Password cracker
  time and space issues
- Markov model
  generates guessable passwords and reject the ones who can be generated

- Bloom filter
  Used to build a table based on dictionary
  Check password against this table

Password file access control
Block offline guessing attacks by denying access to encrypted passwords
Make it available only to privileged users and often using a separate shadow password file.
There are vulnerabilities:

- exploit OS bug
- accident with permissions making it readable
- users with same passwords on other systems
- access from unprotected backup media
- sniff password in unprotected network traffic

Limit validity of passwords

- Limit password validity forcing users to change it regularly and preventing them from reverting to old passwords
- Limit attempts of testing password validity
- Inform users by displaying time of last login

Authentication
Weak authentication of a remote user
For remote users passwords could be sent by mail,email,phone or entered by user on a web page.
How secure is it? A letter containing a password could be stolen

Stronger authentication of a remote user
Send passwords that are valid only for a single log-in request
Request confirmation on a different channel (send confirmation by SMS)

countermeasures to spoofing attacks

- Mutual authentication (the system has to authenticate itself to the user)
- Trusted path (guarantees the user communicates with the system)
- Log monitoring

2.3.2 Something you hold

Memory card

- store but do not process data
- magnetic stripe card (eg. bank card)
- electronic memory card
- used alone for physical access
- with password/PIN for computer use
- drawbacks of memory cards: need special reader,loss of token issues

Smartcard

- It has its own processor
- Secrets are used but not disclosed and are tamperproof

Chapter 3

WebApp and Database

3.1 Database

Design requirements

- **Precision**
  protect sensitive information while revealing as much nonsensitive information as possible
- **Internal consistency**
  the entries in the database obey some prescribed rules
- **External consistency**
  The entries in the database are correct

Database security threats:

- Excessive and unused privileges
  Example: a bank employee whose job requires the ability to change only account holder contact information may take advantage of excessive database privileges and increase the account balance of a colleague's savings account
- Abuse of privileges
  Example: Consider an internal healthcare application used to view individual patient records via a custom Web interface
  The Web application normally limits users to viewing an individual patient's healthcare history However, a rogue user might be able to circumvent these restrictions and copy electronic healthcare records on his laptop
- Unmanaged sensitive data
  Example: Forgotten databases may contain sensitive information
- SQL injection
- Storage media exposure
  Backup storage media is often completely unprotected from attack

Database encryption

- Entire database: very inflexible and inefficient
- Individual fields: simple but inflexible
- Records (rows) or columns (attributes): best choice

Different kind of encryption:

- Order-preserving
  $x \leq y \implies E_{op}(x) \leq E_{op}(y)$
- Deterministic
  $x = y \implies E_{det}(x) = E_{det}(y)$
- Additively homomorphic
  $D_{hom}(E_{hom}(x) * E_{hom}(y)) = x + y$

Remark: perfomance is heavily affected.

Statistical database security
Sensitivity level of an aggregate computed over a group of values may differ from the sensitivity levels of the individual elements.
The user is allowed to make queries over groups of values but he can infer information by combining results from different queries.
Countermeasures

- Suppress obviously sensitive information
- Disguise the data
  Randomly modify entries in the database so that an individual query will give a wrong result although the statistical queries still would be correct
- Track what the user know

Chapter 4

Networking/Infrastructure

4.1 Network

Network attacks:

- Attive attacks
  The goal is to modify the content
  - Impersonate legitimate parties (masquerade)
  - Replay or retransmit
  - Modify the content
  - Launch denial of service
- Passive attacks
  Traffic analysis: the goal is to obtain information, content is not modified
- TCP attacks

Countermeasures

- IPSec
- SSL/TLS
- Kerberos
- Firewalls
- Intrusion detection systems
- Honeypot

Remark the first three are security protocols, the last three are security services.

Network protocols were designed to rely messages between trusted partners. This lead to unintеded consequences: addresses and content are forgeable, content and rely operators can be malicious.

SSL/TLS

Transport Layer Security (TLS) protocol is based on SSL (Secure Socket Layer) protocol.
Handshake protocol
Use public-key cryptography to establish a shared secret key between the client and the server.
Client and server negotiate version of the protocol and the set of cryptographic algorithms to be used

- A client sends a **ClientHello** message specifying the highest TLS protocol version it supports, a random number, a list of suggested cipher suites and suggested compression methods. If the client is attempting to perform a resumed handshake, it may send a session ID.
- The server responds with a **ServerHello** message, containing the chosen protocol version, a random number, CipherSuite and compression method from the choices offered by the client. To confirm or allow resumed handshakes the server may send a session ID. The chosen protocol version should be the highest that both the client and server support.
- The server sends its **Certificate** message (optional)
- The server sends its **ServerKeyExchange** message (optional)
- The server sends a **ServerHelloDone** message, indicating it is done with handshake negotiation.
- The client responds with a **Certificate** message, which contains the client's certificate.
- The client sends a **ClientKeyExchange** message, which may contain a PreMasterSecret
  This PreMasterSecret is encrypted using the public key of the server certificate.
- The client sends a **CertificateVerify** message, which is a signature over the previous handshake messages using the client's certificate's private key. This signature can be verified by using the client's certificate's public key. This lets the server know that the client has access to the private key of the certificate and thus owns the certificate.
- The client and server then use the random numbers and PreMasterSecret to compute a common secret, called the "master secret"

4.1.1 Firewalls

Packet filters: work at Network and Transport Layer

- Allow the packet to go through
- Drop the packet (Notify Sender/Drop Silently)
- Alter the packet (NAT)

- Log information about the packet

Proxies work at application level
Proxy acts as a server for clients requests (validate client requests)
Proxy act as a client and connects to the destination server
Limitations

- No protection against insider attacks
- Deep packet inspection only works if you do not have encrypted connection
- No detection of protocol tunneling
- No encrypted message filtering

4.1.2 Intrusion detection systems

- **Signature based**
  It Uses known pattern matching to signify attack.
  Advantages: it is fast, easy to implement and update.
  Disadvantages: it cannot detect attacks for which it has no signature
- **Anomaly based**
  It uses statistical model or machine learning engine to characterize normal usage behaviors.
  Advantages: it can recognize authorized usage that falls outside the normal pattern or it can detect attempts to exploit new and unforeseen vulnerabilities.
  Disadvantages: generally slower, more resource intensive compared to signature-based IDS, greater complexity, difficult to configure, higher percentages of false alerts
- **Network based**
  It examines raw packets in the network passively and triggers alerts
  Advantages: easy deployment, unobtrusive, difficult to evade if done at low level of network operation. Disadvantages: different hosts process packets differently, it needs to create traffic seen at the end host, it needs to have the complete network topology and complete host behavior
- **Host based**
  Runs on single host.
  Advantages: more accurate than NIDS, less volume of traffic so less overhead
  Disadvantages: deployment is expensive, what happens when host get compromised?

4.1.3 Honeypot

Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, which are then blocked.

Chapter 5

OS security

Sandbox
Environment in which actions of process are restricted according to security policy.
A sandbox does not emulate computer's hardware, it requires only software support.
Virtual Machine
A program that simulates hardware of computer system and reports results back to Application.
It emulates computer's hardware, it requires hardware support. Guest entity cannot access underlying computer system

Chapter 6

Cloud security

Cloud architecural solutions

- Software as a service eg. gmail,google apps, force.com
- Platform as a service eg. microsoft azure
- Infrastructure as a service eg. Amazon EC2,Rackspace

Cloud scenarios

- runnning one or more applications not supported bu host os
- multiple servers could be run on a single physical server
- duplicating specific environments
- creating a protected environment

Potential objectives

- Network analysis/tampering
- Application data exfiltration/tampering
- Control of VM
- Escape from VM
- Cartography

ASP: application service provider

Reasons for cloud virtualization

- A large server can host many guest virtual machine
- A virtual machine can be more easily controlled and inspected from outside compared to a physical one and its configuration is more flexible.
- A new VM can be provisioned as needed without the need for an up-front hardware purchase.
  VM can easily be relocated from one physical machine to another as needed.

Capacity planning
Capacity must exceed maximum demand if you want to meet demand at all times.
ASP vs Cloud: it is crucial if you know in advance the number of users. **Interesting attack:** a guest OS does not know it is running on a VM so it does not clean memory after use. Several VM coexhist on the same physical machine...

Chapter 7

Assessment

7.1 UTM

Terminology
UAV: Unmanned Aerial Vehicles
UAS: Unmanned Aerial System
UTM: UAS Traffic Management

What? "The UTM will provide authentication, airspace design, airspace corridors, and dynamic geofencing, weather integration, constraint management (congestion prediction), sequencing and spacing as needed, trajectory changes to ensure safety, contingency management, separation management, transition locations and locations with NAS, and geo-fencing design and dynamic adjustments".

Why? Many civilian applications of Unmanned Aerial Systems (UAS) have been imagined ranging from remote to congested urban areas, including goods delivery, infrastructure surveillance, agricultural support, and medical services delivery
However, key infrastructure to enable and safely manage widespread use of low-altitude airspace and UAS operations therein does not exist

Airspace classification

- Class A
  above 18,000 feet including the airspace overlying seas within 12 nautical miles

- Class B
  from the surface to 10,000 feet above the nation's busiest airports

- Class C
  from surface to 4,000 feet above airports with operational control tower, serviced by a radar approach control, and sizeable operations or passengers.

- Class D

from the surface to 2,500 feet above airports that have an operational control tower.

- Class E
  None of the above but still controlled (eg military areas)

- Class G
  Unregulated one. Typically below 1,200 feet from surface and 5+ miles away from airports

Current problems

- Lost link
  Happens frequently even on military grade aircrafts
  Key requirements is predictability of what happens after that

- Latency
  Both Link latency and operator latency

- Levels of automation Low automation makes difficult to predict what happens after link is lost
  High automation makes difficult to predict what happens if some gear is malfunctioning

- Measured response
  UAV similar to Manned in time (takes time for the operator to react) but lack sense of place (fly upside down and don't understand that)

- Detect and avoid

7.1.1 UTM models

UTM service provider viewpoint

- **Portable UTM system**
  Arrive, set-up, operate, and leave (be able to move from one location to another)
  Support humanitarian, agricultural and other applications

- **Persistent UTM system**
  Sustained, real-time, and continuous operations
  Sample application: manage national parks, good transportation between cities, small goods transportation in urban areas

UAS owner viewpoint

- **Remotely piloted vehicle**
  Normal airplane
  Pilot is just going to an office instead of boarding the plane

- **Remoted piloted fleet**
  Separation and Management control automated

  1. Vehicle to vehicle communications

2. Vehicle to service communications
3. Most routing, separation management, congestion optimization automated

Operators only intervene in offnominal cases

7.1.2 UTM Service Operational Requirements

- Airspace management and zone separation
  reduce risk of accidents, impact to other operations, and population's concerns
  Vertical and horizontal

- Integration of meteo data
  Avoidance of severe weather/wind areas

- Congestion management (and possibly prediction)
  Currently done with routes negotiations and centralized air traffic management

- Maintain safe separation (mission safety)
  Avoidance of terrain and man-made artifacts
  Avoidance of other aircrafts (classical notion of separation)

- Authenticated operations
  avoid unauthorized airspace use

7.1.3 Role of UAS fleet manager

- **Cloud based UTM Service**
  UAS manager accesses through internet

- **Initial set-up**
  Generates and files a nominal trajectory
  Adjusts trajectory in case of other congestion or pre-occupied airspace
  Verified for fixed,human made, or terrain avoidance
  Verifies for usable airspace and any airspace restrictions
  Verifies for wind and weather forecast and associated airspace constraints

- **Run-time control**
  Monitors trajectory progress and adjust trajectory if needed
  Supports contingency (rescue)

- **Allocated airspace changes dynamically as needs change**

7.1.4 Role of UTM service provider

- **Authentication** Similar to vehicle identification number, approved applications only

- **Airspace design, adjustments and geo-fencing**
  Corridors, rules of the road, altitude for direction, areas to avoid

- **Communication, navigation and surveillance**
  Needed to manage congestion,separation, performance characteristics and monitoring conformance inside geo-fenced areas.
- **Separation management**
  May require sensing infrastructure and avoidance infrastructure
  Part of this infrastructure may be on aircrafts
- **Weather integration** Wind and weather detection and prediction for safe operations
- **Contingency management**
  Not in NASA scenario but somebody must do it.

7.1.5 UTM services according to NASA

Regulatory Services

- **Security services**
  Vehicle registration
  User authentication
  Flight monitoring
  System health monitoring
- **Flight services**
  Flight planning
  Scheduling and demand management
  Separation assurance
  Contingency management
- **UAS fleet owner is bound by response Information Services**

  1. Airspace definition
  2. Weather information
  3. Terrain and obstructions
  4. Traffic operations

  UAS fleet owner use them to optimize its plan

Chapter 8

True stories

Google engineer's David Braksdale

HBGary

Confused deputy

John Rusnak