Developed and Presented By Dr. Mehrdad S Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Ian Sommerville's Book, and Ross Anderson's Book

SECURITY ENGINEERING

SECURITY ENGINEERING

- Tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data.

SECURITY ENGINEERING

- “Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.” Ross Anderson
- Requires cross-disciplinary expertise: cryptography, computer and network security, computer and network systems and protocols, hardware (computer and network), formal methods, applied psychology, organizational methods and psychology, auditing, forensics and the law.
- Requirements not only based on confidentiality and privacy but also include critical infrastructure assurance:safety for human life and the environment, economic structures, and crime prevention and prosecution.

SECURITY ENGINEERING

- The focus of the Security Engineering discipline is:
  - tools,
  - processes, and
  - methods
- needed to
  - design,
  - implement, and
  - test
- complete systems, and to adapt existing systems as their environment evolves.

SECURITY ENGINEERING

- In my humble opinion, Security Engineering is the hardest discipline

There is requiring a cross-disciplinary knowledge of the following disciplines (at least):

- cryptography and computer security,
- hardware tamper-resistance,
- formal methods,
- psychology, legal issues and forensics,
- financial accounting and audit methods,
- software engineering (including evaluation and testing),
- system engineering and business process analysis,
- military science, and
- information theory.

And this is not a complete list!

SECURITY ENGINEERING

- A huge amount of security systems have critical assurance requirements where failure may
  - endanger human life or cause environmental damage (e.g.nuclear power plant),
  - damage the economic infrastructure (e.g.ATM machines),
  - risk personal privacy (e.g.medical record systems),
  - endanger entire business sectors (e.g.pay TV),
  - facilitate crime (e.g.burglar alarms), and
  - cause negative psychological effects (e.g. perceptions that a system is more vulnerable than it really is)

SECURITY ENGINEERING

- Things are complicated by the flawed conventional view of things:
  - "Software engineering is about ensuring that certain things happen."
    - e.g. "Alice can read this file."
  - "Information Security is about ensuring that certain things do not happen."
    - e.g. "Al Qaida cannot read this file."
- The reality is much more complicated because security requirements vary greatly from one system to another.

SECURITY ENGINEERING

- Real systems typically require tailored combinations of
  - user authentication,
  - transaction integrity and accountability,
  - fault tolerance,
  - message secrecy, and
  - covertness.
- Many (most?) system fail due to designers protecting the wrong things (or protecting the right things in the wrong way).

SECURITY ENGINEERING

- Let's look at three concrete examples to illustrate the large range of security-critical information systems.
  1. Banking.
  2. Military.
  3. Hospitals.
  4. Your home.
- After examining these examples we can attempt some definitions.

SECURITY ENGINEERING

- Example 1 – Bank
- Primary attack object – branch bookkeeping system (master customer accounts), may be centralized but principal is the same just more so because a single compromise effects more customers
- Main threat – bank employees.
- Main defense – good accounting procedures.
- Public interface – ATM, credit/debit cards plus PIN (potential attack vector), uses online/inline and offline
- cryptography.
- Internet interface for customers – Web + (TSL/SSL or VPNs), new primary attack vector (phishing).
- Both Internet and ATM depend on quality secure messaging and secure communication systems.

SECURITY ENGINEERING

- Example 2 – military
- Electronic warfare with jamming, countermeasures, counter-countermeasures are precursors of information warfare on the Internet (denial of service, ~virus, etc).
- Communications - encryption, transmission masking (low-probability-of-intercept, spread spectrum), destination masking.
- Assurance requirements (online and offline) for logistics and inventory management for VERY large systems. Frequently require access hierarchies.
- Weapons systems (particularly nuclear) often require complex multifactor and/or multi-origin access.

SECURITY ENGINEERING

- Example 3 – Hospitals
- Distributed data and delivery systems.
- Special assurance issues – can't lose data, can't store incorrect data or allow to become corrupt, i.e., reliability, and accuracy extremely important Privacy not only restricted to anonymity (hard to without special "scrubbing"), there are also role based privacy requirements.
- Availability of data/services also critical (sometimes, e.g., when in hospital). Think of DoS.

SECURITY ENGINEERING

- The main lesson is a change in mindset to enable us to design more secure systems:
  - we must learn more about how current systems work, and how have systems failed.
- We generally learn a lot more from our failures than our success.

DEFINING SECURITY BY FUNCTION

- Security can be categorized under the following functional area:
- Risk Avoidance
- Deterrence
- Prevention
- Detection
- Recovery

RISK AVOIDANCE

- An Organization should do a risk assessment that identifies what value and risk each component has to the system in whole and include strategies that reduce the likelihood of behavior/activity that can be damaging.

DETERRENCE

- Deterrence is a common method of control used by government, businesses, and individuals to scare people into thinking twice before performing an action. For example your IP address 132.208.213.10 has been recorded and all activity is subject to monitoring and logging.

PREVENTION

- Information is an asset that requires protection commensurate with its value.
- Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional.
- During the prevention phase, security policies, controls and processes should be designed and implemented.
- Security policies, security awareness programs and access control procedures, are all interrelated and should be developed early on.
- The information security policy is the cornerstone from which all else is built.

DETECTION

- Detection of a system compromise is extremely critical. With the ever increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. There is no full proof “silver bullet” security solution.
- A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm.
- The most important element of this strategy is timely detection and notification of a compromise.
- Intrusion detection systems (IDS) are utilized for this purpose.

RECOVERY

- Recovery strategies should be developed for Information technology (IT) systems, applications and data.
- This includes networks, servers, desktops, laptops, wireless devices, data and connectivity.
- Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis

DEFINITION

- System – anything or everything; product or component thereof, operating system, communications system, applications, staff, users, customers, environment in which embedded.
- Subject – physical person in any role
- Person – human or legal entity (company)
- Principal – an entity that participates in a security system (subject, person, role, equipment, communications
- channel, group of principals)
- Role – a function assumable by different persons
- Identity - (pure) a correspondence between a name and a person (as understood by another person)
- Identity - (vernacular) a name
- Trust - believed to be trustworthy (but may not be)

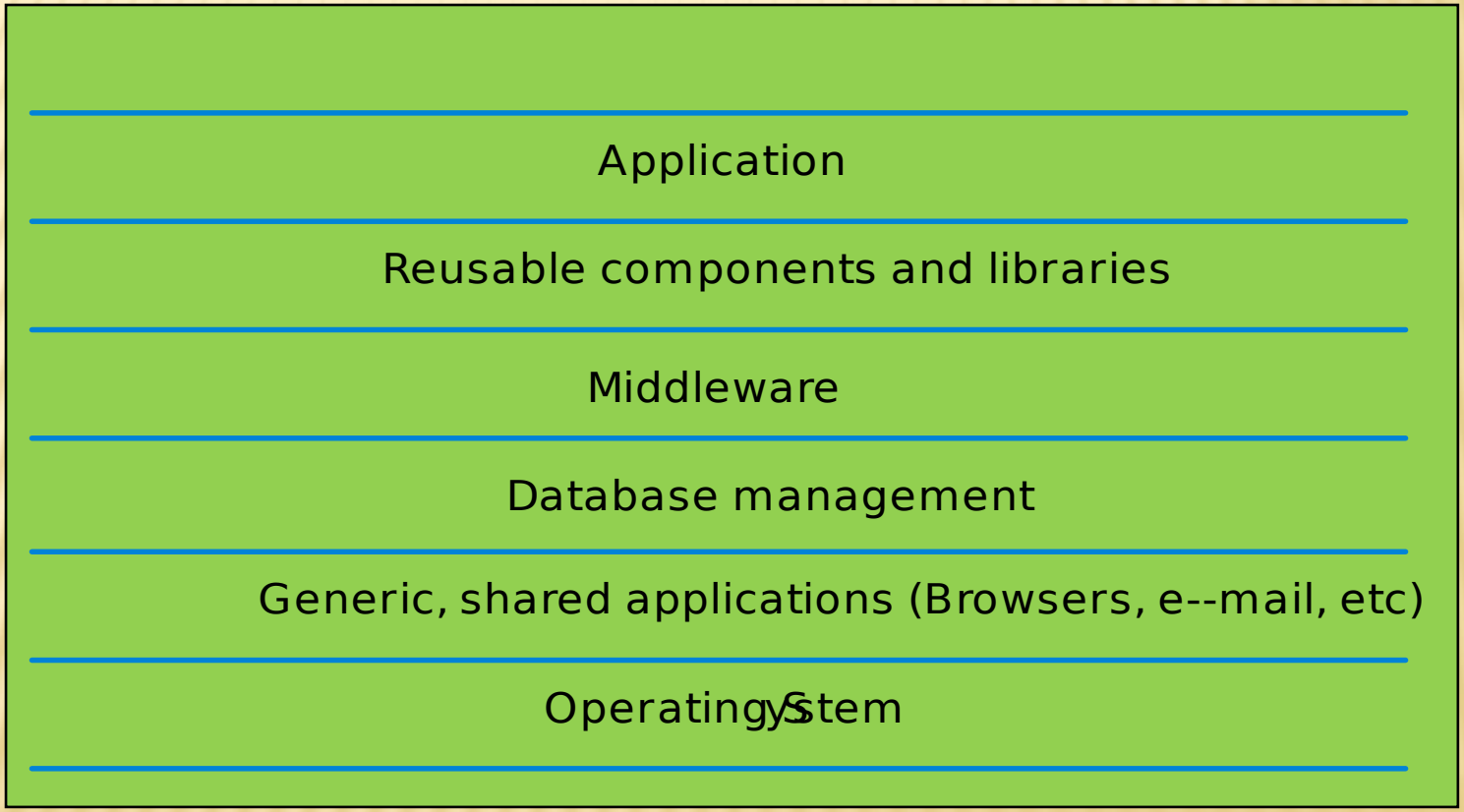
DEFINITION

- Trusted system – is a system is one whose failure can break a security policy
- Trustworthy – a system or subsystem that will not fail
- Secrecy – the effect of the mechanisms used to limit the number of principals who can access information
- Confidentiality – the obligation to protect some other person's or organization's secrets if you know them
- Privacy – the ability or right to protect your personal secrets

APPLICATION/INFRASTRUCTURE SECURITY

- Application security is a software engineering problem where the system is designed to resist attacks.
- Infrastructure security is a systems management problem where the infrastructure is configured to resist attacks.
- Let’s try to focus on application security.

SYSTEM LAYERS



SECURITY CONCEPTS

Term	Definition
Asset	A system resource that has a value and has to be protected.
Exposure	The possible loss or harm that could result from a successful attack. This can be loss or damage to data or can be a loss of time and effort if recovery is necessary after a security breach.
Vulnerability	A weakness in a computer-based system that may be exploited to cause loss or harm.
Attack	An exploitation of a systemÕs vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
Threats	Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
Control	A protective measure that reduces a systemÕs vulnerability. Encryption would be an example of a control that reduced a vulnerability of a weak access control system.

EXAMPLES OF SECURITY CONCEPTS

Term	Definition
Asset	The records of each patient that is receiving or has received treatment.
Exposure	Potential financial loss from future patients who do not seek treatment because they do not trust the clinic to maintain their data. Financial loss from legal action by the sports star. Loss of reputation.
Vulnerability	A weak password system which makes it easy for users to set guessable passwords. User ids that are the same as names.
Attack	An impersonation of an authorised user.
Threat	An unauthorised user will gain access to the system by guessing the credentials (login name and password) of an authorised user.
Control	A password checking system that disallows passwords that are set by users which are proper names or words that are normally included in a dictionary.

SECURITY THREATS

- Threats to the confidentiality of a system or its data
- Threats to the integrity of a system or its data
- Threats to the availability of a system or its data

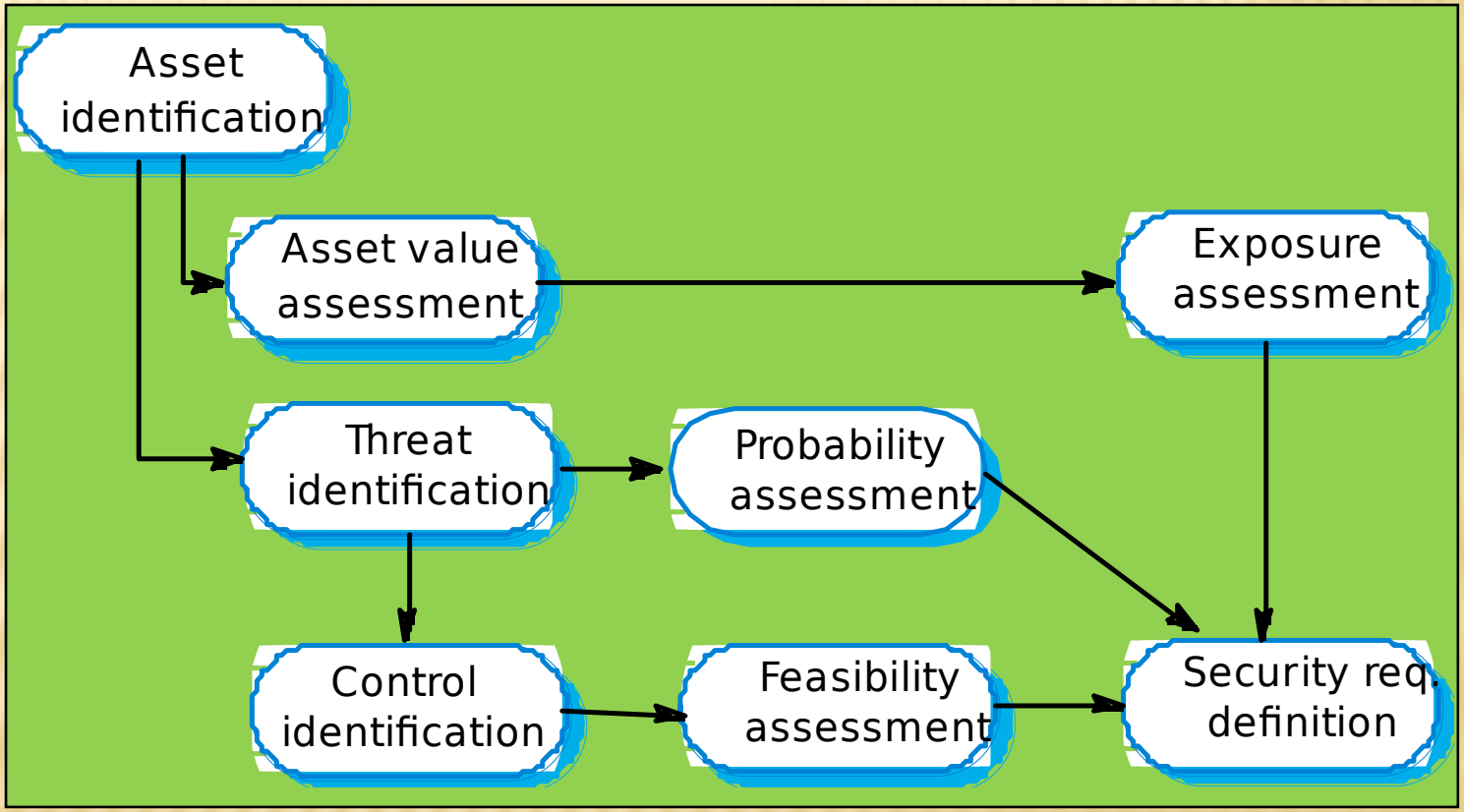
SECURITY CONTROLS

- Controls that are intended to ensure that attacks are unsuccessful. This is analogous to fault avoidance.
- Controls that are intended to detect and repel attacks. This is analogous to fault detection and tolerance.
- Controls that are intended to support recovery from problems. This is analogous to fault recovery.

SECURITY RISK MANAGEMENT

- Risk management is concerned with assessing the possible losses that might ensue from attacks on the system and balancing these losses against the costs of security procedures that may reduce these losses.
- Risk management should be driven by an organisational security policy.
- Risk management involves
  - Preliminary risk assessment
  - Life cycle risk assessment

PRELIMINARY RISK ASSESSMENT



ASSET ANALYSIS

Asset	Value	Exposure
The information system	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
The patient database	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
An individual patient record	Normally low although may be high for specific high-profile patients	Low direct losses but possible loss of reputation.

THREAT AND CONTROL ANALYSIS

Threat	Probability	Control	Feasibility
Unauthorised user gains access as system manager and makes system unavailable	Low	Only allow system management from specific locations which are physically secure.	Low cost of implementation but care must be taken with key distribution and to ensure that keys are available in the event of an emergency.
Unauthorised user gains access as system user and accesses confidential information	High	Require all users to authenticate themselves using biometric mechanism. Log all changes to patient information to track system usage.	Technically feasible but high cost solution. Possible user resistance. Simple and transparent to implement and also supports recovery.

SECURITY REQUIREMENTS

- Patient information must be downloaded at the start of a clinic session to a secure area on the system client that is used by clinical staff.
- Patient information must not be maintained on system clients after a clinic session has finished.
- A log on a separate computer from the database server must be maintained of all changes made to the system database.

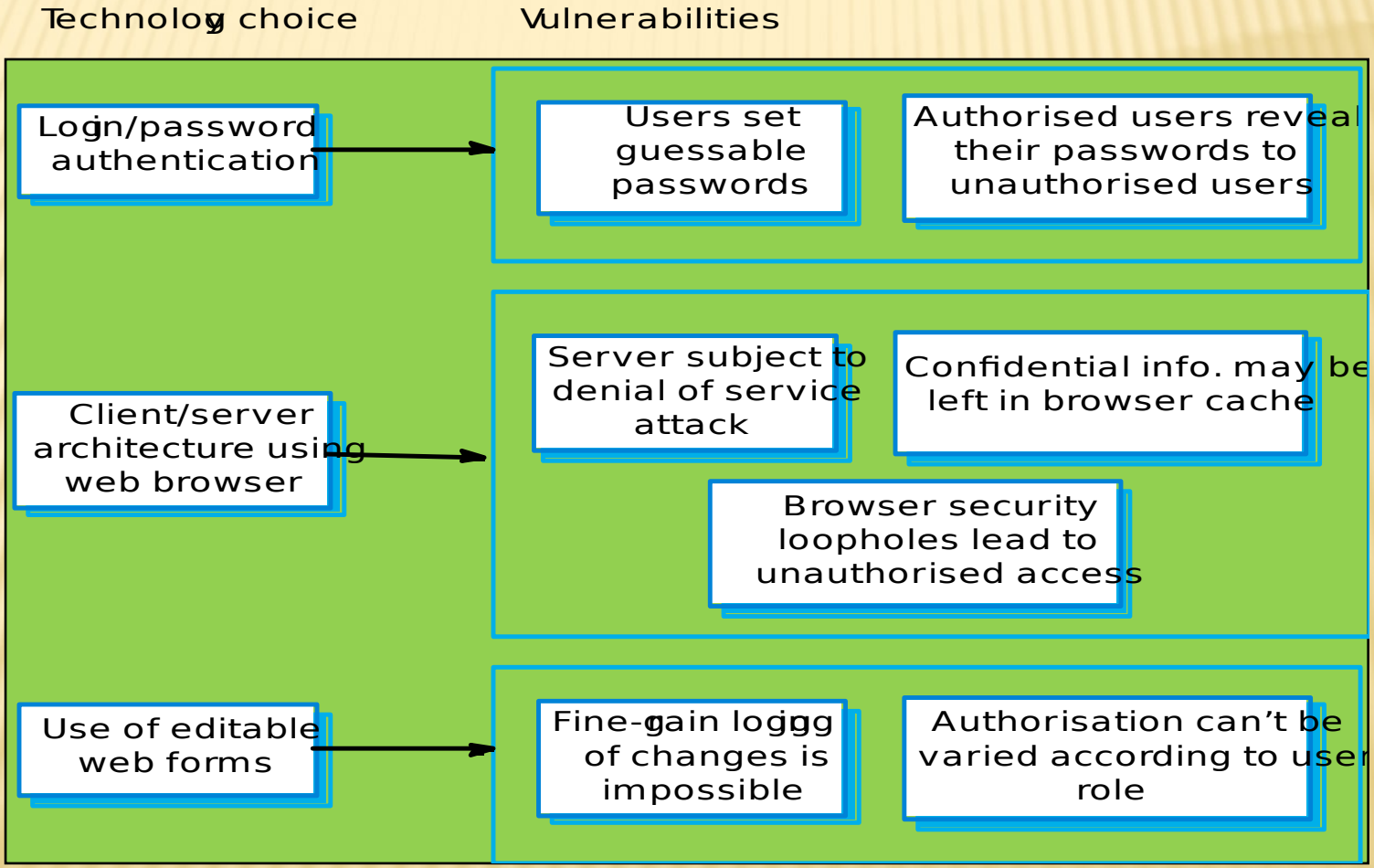
LIFE CYCLE RISK ASSESSMENT

- Risk assessment while the system is being developed and after it has been deployed
- More information is available - system platform, middleware and the system architecture and data organisation.
- Vulnerabilities that arise from design choices may therefore be identified.

EXAMPLES OF DESIGN DECISIONS

- System users authenticated using a name/password combination.
- The system architecture is client-server with clients accessing the system through a standard web browser.
- Information is presented as an editable web form.

TECHNOLOGY VULNERABILITIES



KEY POINTS

- Security engineering is concerned with how to develop systems that can resist malicious attacks
- Security threats can be threats to confidentiality, integrity or availability of a system or its data
- Security risk management is concerned with assessing possible losses from attacks and deriving security requirements to minimize losses