Foundations of Information Security

Daniel Bosk

Department of Information and Communication Systems,
Mid Sweden University, SE-851 70 Sundsvall.

14th May 2018

- The main purpose of security is to protect assets.
- We define our goals in a *security policy*.
- E.g., who may access what asset and how.
- We then must enforce our policy.

- The main purpose of security is to protect assets.
- We define our goals in a *security policy*.
- E.g., who may access what asset and how.
- We then must enforce our policy.

- The main purpose of security is to protect assets.
- We define our goals in a *security policy*.
- E.g., who may access what asset and how.
- We then must enforce our policy.

Example

- Asset: private photos.
- Policy:
  - Only I can access my photo collection.
  - I can share individual photos to individual persons.
- Enforcement?

Example

- Asset: private photos.
- Policy:
  - Only I can access my photo collection.
  - I can share individual photos to individual persons.
- Enforcement?

- Each of our mechanisms we can say is more or less *trustworthy*.
- A trustworthy mechanism will not break our security policy.
- The aim of this course is to give you an idea of how to determine what is a trustworthy mechanism.

- Each of our mechanisms we can say is more or less *trustworthy*.
- A trustworthy mechanism will not break our security policy.
- The aim of this course is to give you an idea of how to determine what is a trustworthy mechanism.

Protection strategies

Prevention taking measures that prevent your assets from being damaged.

Detection taking measures that allow detection of when, how, and by who an asset has been damaged.

Reaction taking measures that allow to recover assets or recover from damage to assets.

Example (Private property)

Prevention	Locks on doors, window bars, surrounding walls, ...
Detection	Stolen items are missing, burglar alarms, video surveillance, ...
Reaction	Call the police, replace stolen items (insurance?), ...

Example (Private photos)

Prevention	Encrypt, store securely.
Detection	Our photos have leaked.
Reaction	Anything other than get angry?

Example (Private property)

Prevention Locks on doors, window bars, surrounding walls, ...

Detection Stolen items are missing, burglar alarms, video surveillance, ...

Reaction Call the police, replace stolen items (insurance?), ...

Example (Private photos)

Prevention Encrypt, store securely.

Detection Our photos have leaked.

Reaction Anything other than get angry?

Definition (Data and information [Han73])

[Data is the] [p]hysical phenomena chosen by convention to represent certain aspects of of our conceptual and real world. *The meanings we assign to data are called information.* [my emphasis] Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules.

Example

- $x + 1 = 0 \iff x = -1$: the two equations are data, we use the formal rules of mathematics to derive the value of x.
- Timestamps of TCP packets on the network with port set to 80 or 443, formal rules of statistical analysis.

Confidentiality Concerns unauthorized disclosure of information.

Integrity Concerns unauthorized modification.

Availability Concerns unauthorized withholding of information or resources.

Confidentiality

- Unauthorized 'reading'.
- Think about what to hide: the content of a document, or the document's existence?

Privacy

- Privacy is related, but this concerns protection of personal information.
- The users should be in control of their data and of the information about their activities.
- Varying definitions.
- Sometimes used synonymously to confidentiality.

Integrity

- Unauthorized 'writing'.
- Data integrity: 'The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction.'
- Concerns detection and correction of intentional and unintentional modifications of data.

Integrity continued

- Clark and Wilson: 'No user of the system, even if authorized, may be permitted to modify data in such a way that assets or accounting records of the company are lost or corrupted.'
- I.e., make sure that everything is as it is supposed to.
- Integrity is a prerequisite to many other security services.

Availability

- This is the property of being *available and usable* upon demand by an authorized principal.
- Denial of Service (DoS) is an attack on availability which prevents authorized access to resources or the delaying of time-critical operations.
- A very important part of security, unfortunately not many methods for accomplishing this are available.
- Distributed Denial of Service (DDoS) gets much attention, this can also be seen as a reliability problem (unintentional).

Example (DDoS)

- Attackers infect $x \cdot 10^5$ devices (smartphones, IoT-stuff) with malware.
- Attackers commands all devices to send requests to a given address.
- No one can communicate with that address under that load.

Reliability

- Reliability addresses the consequences of unintentional errors.
- On a PC (offline), you are in control of the software components sending input to each other.
- The aim is to avoid mistakes.

Security

- Once online, hostile adversaries can provide input.
- Protection against mistakes is not enough — they will ensure to make them for you.
- And they will do things that you can never accomplish by mistake.

Reliability

- Reliability addresses the consequences of unintentional errors.
- On a PC (offline), you are in control of the software components sending input to each other.
- The aim is to avoid mistakes.

Security

- Once online, hostile adversaries can provide input.
- Protection against mistakes is not enough — they will ensure to make them for you.
- And they will do things that you can never accomplish by mistake.

- To make software more reliable, it is tested against typical usage patterns.
- To make software more secure, it has to be tested against non-typical usage patterns.
- Testing against non-typical usage patterns might be difficult.

1. Where to focus security controls?
2. Where to place security controls?
3. Complexity or assurance?
4. Centralised or decentralised control?
5. Blocking access to the layer below?

Focus and placement of control

- Focus of control may be on data, operations, or users.
- If we look at the control of integrity, its requirements may refer to rules on:
  - Format and content of data items, e.g., account balance must be integer.
  - Operations that may be performed on a data item, e.g., credit, debit and transfer.
  - Users who are allowed access to a data item, e.g., account holder and bank clerk.

Complexity or Assurance

- Generic mechanisms are simple, applications are usually feature rich.
- The fundamental dilemma:
  - Simple generic mechanisms may not match specific security requirements.
  - To choose the right features from a rich selection, you need to be a security expert.
  - Security-unaware users are at a loss.

Centralized or decentralized controls

- Within the domain of a security policy, the same controls should be enforced everywhere.
- Having a centralized entity to do this makes it easy to achieve uniformity, however, this entity may become a bottleneck.
- A distributed solution might be more efficient, however, then you must ensure they all enforce consistently with each other.

- Every security mechanism defines a *security perimeter*.
- The parts of a system which can malfunction without breaking the mechanism are said to be outside the perimeter.
- The parts of the system that can disable the mechanism are within the perimeter.

- Attackers will try to bypass security mechanisms.
- How do you ensure an attacker cannot get access to the layer below the security mechanism?

- Recovery tools, read the sectors directly from the disk; logical access control is implemented in the operating system.
- Buffer overruns, a value assigned to a variable is too large for the memory buffer allocated; memory allocated for other variables may be overwritten.
- Side-channel analysis, look at the time different operations take to perform, look at power consumption.
- JavaScript to perform security checks? The client can use a Web page without JavaScript enabled.

- We have two major schools of gaining new knowledge: deduction and induction.
- Both are used, but have different strengths and weaknesses.

Definition (Deduction)

- This stems from logic and mathematics.
- State axioms.
- Use the axioms and formal rules (logic) to infer knowledge.

Example (System and adversarial model)

- The system model captures the core properties of the system.
- The adversary model captures the capabilities of the adversary attacking the system.
- We use these models as axioms and try to show security deductively.

Note

- Cryptography is the area which uses most stringently the deductive method.
- In many areas of security it is not possible use the full strict formalism required in maths.
- To do deduction one needs simple building blocks with few properties.
- Thus, in many papers, it's informal, rather than, formal arguments in the deduction.
- And occasionally, we find vulnerabilities.

Note

- Cryptography with it's perfect deduction isn't problem free either.
- The axioms must match the real world, which is hard.
- Sometimes things are over-simplified.

Definition (Induction, hypothesis testing)

1. Form hypothesis.
2. Perform experiment and collect data.
3. Analyse data.
4. Interpret data and draw conclusion.
5. Depending on conclusions, return to 1.

Note

- There are requirements on the induction process.
- The experiment must test a hypothesis which is both *testable* and *falsifiable*.
- The experiment must have exactly *one variable*.
- The experiment must be *reproducible* and *results repeatable*.

Example (Testable and falsifiable)

- Implies observability and measurability.
- Hypothesis: Prayer increases contact with one's deity.
- Not falsifiable: We cannot observe divine communication, no experiment could prove the result wrong.

Example (Testable and falsifiable)

- Hypothesis: This software is secure.
- Not measurable: What is secure?

Example (Testable and falsifiable)

- Implies observability and measurability.
- Hypothesis: Prayer increases contact with one's deity.
- Not falsifiable: We cannot observe divine communication, no experiment could prove the result wrong.

Example (Testable and falsifiable)

- Hypothesis: This software is secure.
- Not measurable: What is secure?

Definition (Quantitative methods)

- Explores quantitative relationships.
- Here it might be difficult to isolate single variables.
- E.g., when studying humans.

Definition (Qualitative methods)

- Doesn't use quantitative methods such as statistics.
- Used to explore phenomena in-depth.
- Especially useful for finding direction in usability research.

[Han73] Per Brinch Hansen. *Operating system principles*. Prentice-Hall, Inc., 1973.