What is Information Security?

Information Security

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 1

Hans Georg Schaathun

- Broad interests in information security
  - Multimedia Security,
  - Steganalysis using Machine Learning,
  - Security in NFC communications
- Background in Coding and Cryptography
- dr.scient. University of Bergen 2002
- Lecturer/Senior Lecturer at University of Surrey 2006–10
- Professor at HiÅ from 1 February 2011

Module Objectives

At the end of the module, the students will be

- be able to identify assets, threats, and risks related to information security
- familiar with legislation and stadards concerning information security
- assess and perform a risk analysis
- develop emergency and contingency plans
- account for how security work can be organised and managed
- describe and assess different security controls and approaches to information security

Work plan

- Weekly 4h session
  - Largely interactive, some lecture, group discussions, exercises etc.
- Weekly 2h session
  - Mainly lecture on new material
- (almost) Weekly exercises
  - submitted in fronter by Monday morning 6am
  - discussed in class – *do bring a copy of your submission*
  - some submissions will be drafts or parts of subsequent exercises
- Final portfolio containing
  - answers to the weekly exercises (possibly revised)
  - a longer case study
  - single PDF document
- Prepare to spend 12h(+) *every* week on the module

Learning method

1. Read a lot
   - Textbooks, newspapers, standards, codes of law, web pages, white papers, etc.
2. Discuss, actively in class
   - help structure and apply the knowledge
   - develop creativity
3. Write down case studies
   - structure and consolidate *your own* thoughts and understanding
   - every week
4. Review your writing
   - peer assessment
   - discussion in class

Session objectives

- Establish a common terminology to discuss (computer) security
- Get a glimpse of the wide range of *threats*

Yellow Stickers Exercise

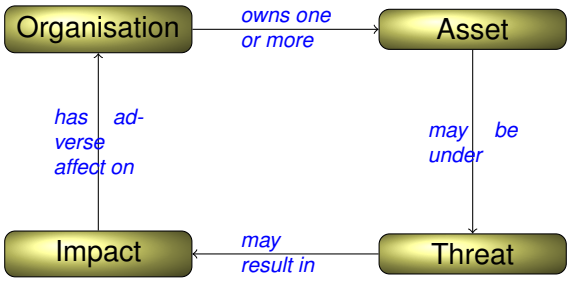
- Sit in groups of 3-5.
- Write down all computer security problems that you can think of.
- One problem per yellow sticker.

What is «Information Security»?

> *... information security is primarily a management problem, not a technical one ...*
>
> *Whitman & Mattord 2005*

- Anti-virus, password systems, encryption, SSL, etc. is important but
- Those solutions are well understood
  - read manuals and take certificates
- More security problems are caused by
  - selecting the wrong solution for the problem
  - misunderstanding of what the problem is
  - misconfiguring a product
  - failure to train staff in proper use and conduct
  - selecting incompatible solution
- Those are the management problems of security

What we protect



What is an organisation?

... who you work for ...

- yourself (or your family)
  - if you think about your home network
- your employer
  - when you are at work
- your client
  - if you are a contractor
- a charity/association
  - if you volunteer to help with *their* computer system

... it is whoever owns the information to be secured ...

What is an asset

- Security is always about protecting something
  - Something of value
  - Something which could be damaged or lost
- This is we call assets
  - Information assets (client details, research results, personal letters)
  - Real assets (money, hardware, software, people, etc.)
  - Intangible assets (brand, goodwill, etc.)
- If you don't know what your assets are
  - you don't know what to protect

Working with Information Assets

- Our focus is on information assets
  - ... but not independent of other assets
- Loss information assets may cause loss of other assets
  - password for your Internet bank (information asset)
- and vice versa
  - your data centre (physical asset) burns down
- Same principles apply to information assets and other assets
- Remember the dependencies

Exercise

1. Return to your groups.
2. Pick a handfull of yellow stickers (not necessarily your own).
3. Choose one organisation (fictional or real) to use as a case study.
4. For each of your yellow stickers, identify assets of that organisation which could be affected by the problem on the sticker.

Impact

impact is a change in the value of your assets, as a result of an event wholly or partly out of your control

- Impact on an asset may be
  - loss of
  - damage to
  - positive effects (e.g. press coverage ⇒ brand awareness)

Examples of Impact

- all your workstations were down for two days, due to a virus attack
- a million credit card numbers where compromised because of a break-in on your servers
- you lost 1000 customers because hackers had redirected your web site to a porn page
- your data centre burnt down
- your project was cancelled due to budget cuts
- your contract with Visa/MasterCard was canceled because you failed to comply to their standards

Obviously, you may not be able to measure the impact accurately. For instance, who knows how many customers you would have had, if not ...

Threat

*A threat is a **potential** for impact*

- Threats are uncertain — may or may not be realised and lead to impact
- Threats are real — must be dealt with before it is realised
- *Security is preparing for the unknown*.
- Once the impact is a fact, you have certainties.
  - disaster recovery is a simpler problem than security
- Identifying and understanding threats is at the heart of security management.

Different threat sources

Adversaries (hackers, thieves, competitors) threatening intentional impact

Users honest but fallible — *accidentally* causing harm

Nature threating with *random* events – fire and flood

To understand the threats, one should understand the threat source and its motivation.

Sample threats

- a user tricked into revealing his password
- break-in where data is modified
- industrial secrets revealed to a competitor
- accidental fire
- different attacks or events may realise the same threat
  - a user may reveal his password because of a phishing attack
  - or because someone looks over his shoulder
- may cause different types of impact
  - a break-in may cause modification the web pages
  - or insert a false transaction (send money to the attacker's Cayman Island account)

Second-order impacts

- A single event may cause more than one impact
- For instance, a phishing attack
  - passwords (asset) is compromised — first-order impact
  - the password itself has no business value
  - however, an adversary knowing the password can cause more second-order impacts:
    - using the password, the attacker can modify the web page (asset)
- First-order impact is the immediate effect on the organisation
- Second-order impact is effects which became possible due to first-order impact
- It is worth distinguishing when impacts are enumerated

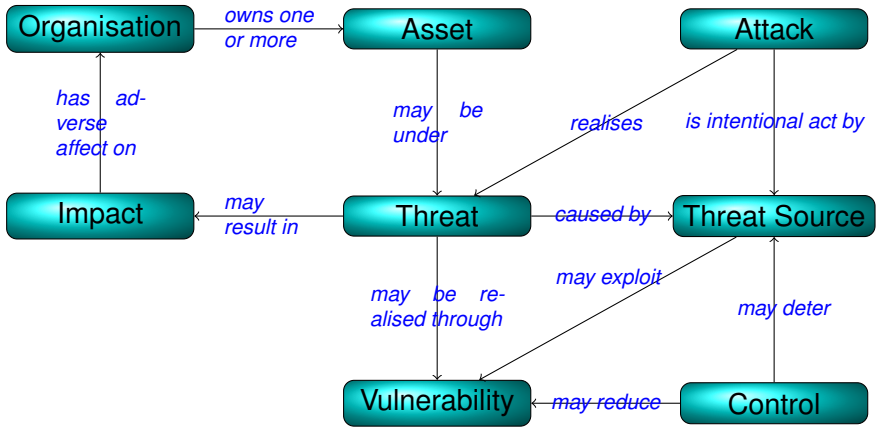
How to analyse threats

- Write clearly. Use as precise words as possible.
- Address each threat in turn.
- For each threat, enumerate possible impacts including the assets involved.
- When threats are related, cross-reference them
  - do not be tempted to discuss several (even related) threats in detail at the same time
- Threats may be related in many ways
  - variations over a theme
  - one threat with first-order impact making a (second-order) threat more imminent
- no good guideline as to what constitutes a single threat, and what would better be described as multiple, related threats.
  - How much time and resources are there for the analysis?

Exercise

1. Return to your groups.
2. Look again at the stickers with a security problem and one or more assets.
3. For each sticker
   - Formulate one threat and one possible impact relating to the security problem and the asset.

A Basic Ontology

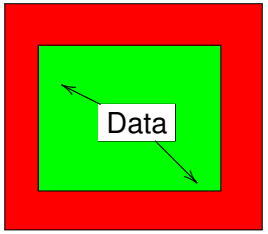


Confidentiality

- Talking of security, we often think of confidentiality.
- Unauthorised entities cannot get information.
- Your asset is secret
  - passwords
  - personal details
  - trade secrets
- Which of your assets require confidentiality?

Complete confidentiality

- Put your asset (e.g. the computer) in a locked steel box,
  - set it in concrete,
  - and sink it in the ocean.



- Is this good enough?
- The information is no good to anyone.

Availability

Definition (Availability)

The system is accessible and useable upon demand by an authorised entity.

- Can we maintain availability and confidentiality at the same time?
- *Denial of Service* (DoS) attacks violate availability.
  - E.g. a horde of computers send dummy request to a web server, causing a congestion which prevents legitimate users from using the web services in a timely fasion.
  - No confidentiality at stake – server data are public
  - but not *available* to the public
- Potentially costly damage.

Integrity

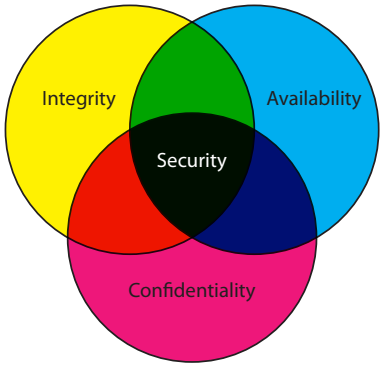
Definition (Integrity)

The state of the system or data can only be changed by an authorised entity.

- If integrity is not ensured.
  - I could change your bank account to send money to my Swiss bank account.
  - We could forge a file to incriminate the PM.
- Integrity problems lead to loss of other assets (money and goodwill)
- You cannot trust your computer.

The three faces of security

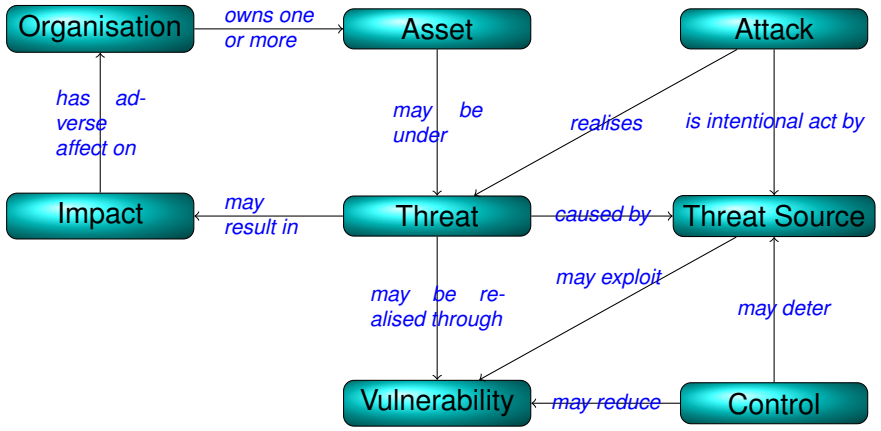
The CIA Triad



Exercise

- Return to your groups.
- Take a handful of yellow stickers (not necessarily your own)
- For each one decide what kind of security problem it is,
  - Integrity, Confidentiality, Availability?
  - Two or three of the above?

A Basic Ontology



Terms so far

Organisation Yourself or the entity you work for.

Assets The values at stake.

Threat Source Entities with an intent or potential to cause damage. (Competitors, organised criminals, petty thieves)

Threats What can go wrong? Potential actions of your Threat Sources

Impact (of an Incident) Realisation of a threat. An actual event (attack or otherwise) damaging the assets.

Threats and Threat Sources

Security incidents happen for a reason

Threat *potential* events and actions which *could* harm the assets

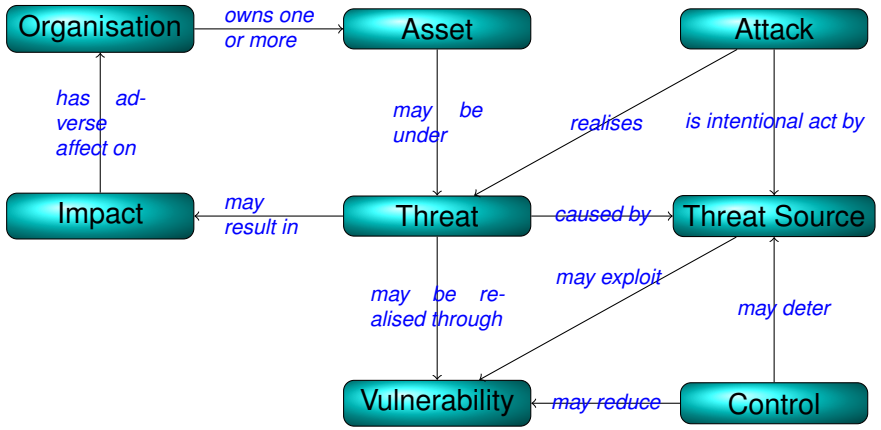
- Potential exists and must be addressed *before* it is realised

Threat Source an entity with a will and potential to cause harm

- A threat source will have a motive
  - hackers – do it for the challenge
  - thieves – do it for gain
  - competitors – want to gain a competitive advantage
  - blackmailers
- Without a motive, there is no threat

How do the threat sources cause damage? And what can we do?

A Basic Ontology



Properties of our system

Properties of our system may make it easier or harder for threats to be realised.

Vulnerabilities (lyte) Weaknesses in your system, increasing the probability of realising a threat.

Control The countermeasures you take against the threats, reducing the consequence and/or probability of impact.

A threat scenario

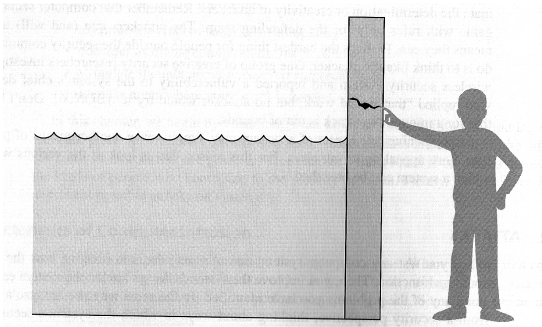


FIGURE 1-1 Threats, Controls, and Vulnerabilities.

Common vulnerabilities

- Users are careless about their passwords
  - Threat: unauthorised access
- Executable code mixed with data (e.g. MS-Word)
  - Threat: viruses and Trojans
- Insufficient input checking in web pages
  - Threat: SQL injection, cross-site scripting, etc.
- Laptops and removable media susceptible to loss
  - Threat: Unauthorised access to data

Controls

Controls are measures taken to reduce the impact and/or probability of unfavourable events.

- Preventive controls make it harder to attack the system
  - reduce the likelyhood of an incident
  - e.g. better-quality locks
- Detection mechanisms are controls intended to reduce the impact of an incident
  - e.g. burglar alarm
- Recovery mechanisms are controls which only become active after the fact
  - yet they must be part of security planning
  - e.g. security guards responding to the alarm
  - backup systems is the most stereotypical example
  - good recovery plans reduce the impact of incidents
- Other reactions after the fact can also be effective controls
  - punishment through disciplinary or legal action can *deter* threat sources
  - reducing the probability

Sample controls

- Users are careless about their passwords (unauthorised access)
- User training
- Reduce the users' access rights
- Biometric access control
- Forbid remote access
  - Physical access control

Sample controls

- Executable code mixed with data (e.g. MS-Word) (viruses and Trojans)
- Only exchange and accept data in pure data formats
- Sandboxed systems for accessing such documents
- Virus scanners
- User training

Sample controls

- Insufficient input checking in web pages (SQL injection, cross-site scripting, etc.)
- Input checking
  - using trusted libraries for the purpose
- Limit the web server's access to data

Sample controls

- Laptops and removable media susceptible to loss (Unauthorised access to data)
- Forbid removal of equipment from premises
- Encrypted file systems
- User training

The flip side of the coin

Medaljens bakside

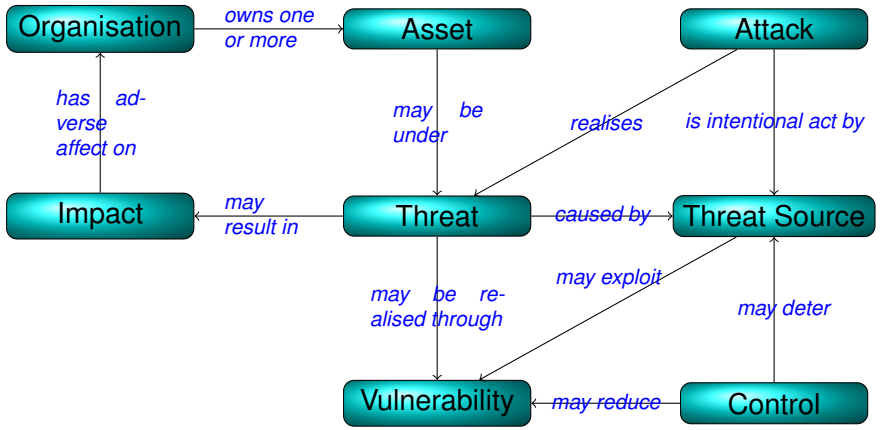
- All controls have a cost
- Not only the cost of implementing it
- Also costs through negative impact on other CObIT criteria
  - reduced availability
  - reduced effectivity
  - reduced efficiency
- Few controls are 100% effective
  - combinations of controls may be necessary

Different Threat Sources

- Three main classes of threat sources
  - Adversaries – sentient beings with an intention to cause harm
  - Honest, but fallible users – accidentally causing harm
  - Random events – accidents like flood and fire
- Common distinction

  Security against intentional attacks, i.e. adversaries
  Useability user interface design to avoid human error
  Reliability against random events
- Fuzzy boundaries between the three
- Similar protection mechanisms
  - Arson and accidental fire
- Incident in one area leads to vulnerabilites in others
  - Useability problems ⇒ misconfigured security mechanisms

A Basic Ontology

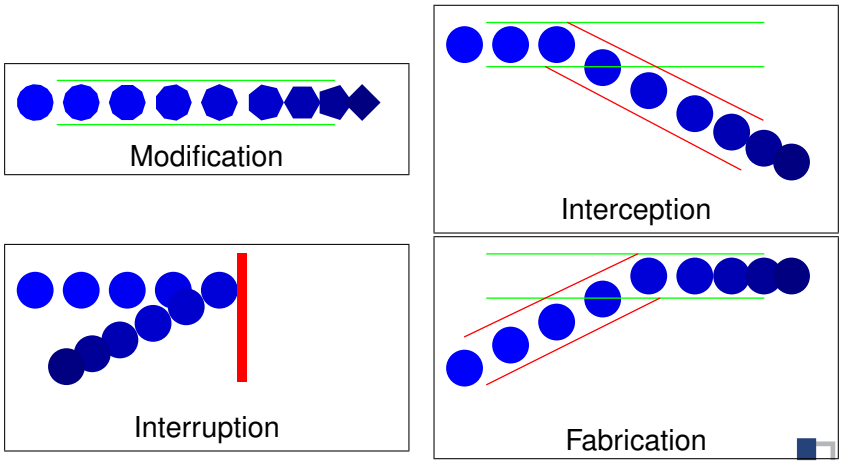


Attacks

- *Attack* is a word which is hard to avoid
- Special case of incident or event
  - We are interested in the impact of the event/attack/incident
- Concerns *intentional* impact only
  - i.e. a sentient attacker is the threat source

Attack types

- Attacks is an important group of incidents (impact)



What is Risk?

Probability How often do we expect the threat to be realised?

Impact (Consequence) How serious would the realisation of a threat be? What would be the damage to the assets?

Risk Product of consequence and probability. Say *expected (average) damage*.
«Risk» is a difficult concept to grasp — we will revisit it again and again.

Assessing a threat, both the probability and severity of possible impact matter. Remember both!

How do you secure this?

Ambiguity

- Unambiguous discussion of security is essential
- Most words are ambiguous
- No universal definition of key terms, like *threat* or even *security*

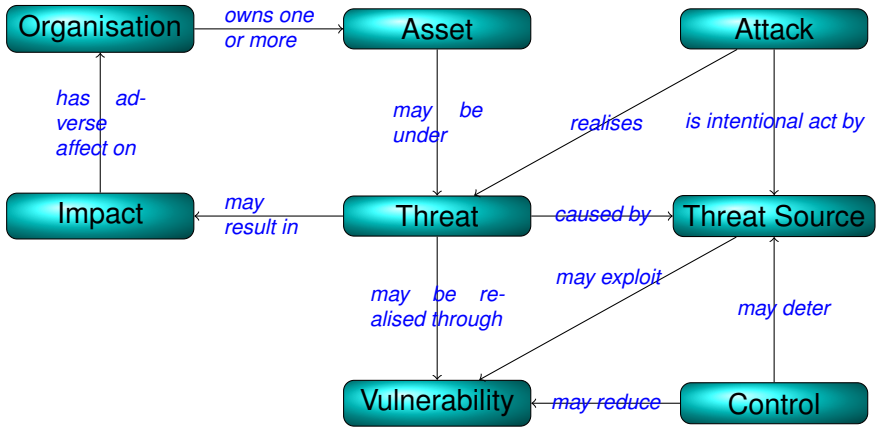
In this module we will use the ontology discussed today.

- When you read, make sure that you read the definitions.
- Do not trust you intuition.
- Do not assume that the present author agrees with a previous one.

Presenting *secure solutions*

- Never say *this product is secure*
  - ... it is secure *against* something
  - what scenario is it intended for?
  - which threats have been addressed?
  - which potential threats have not been controlled?
  - for which applications is it unsuitable?
- Never say *this feature increases security*
  - which threat does it control?
  - which vulnerability is reduced?

A Basic Ontology



The three faces of security

The CIA Triad