1495 UNIVERSITY OF ABERDEEN | CELEBRATING 525 YEARS 1495 – 2020

ABERDEEN 2040

Network Security Technology

Introduction to Security

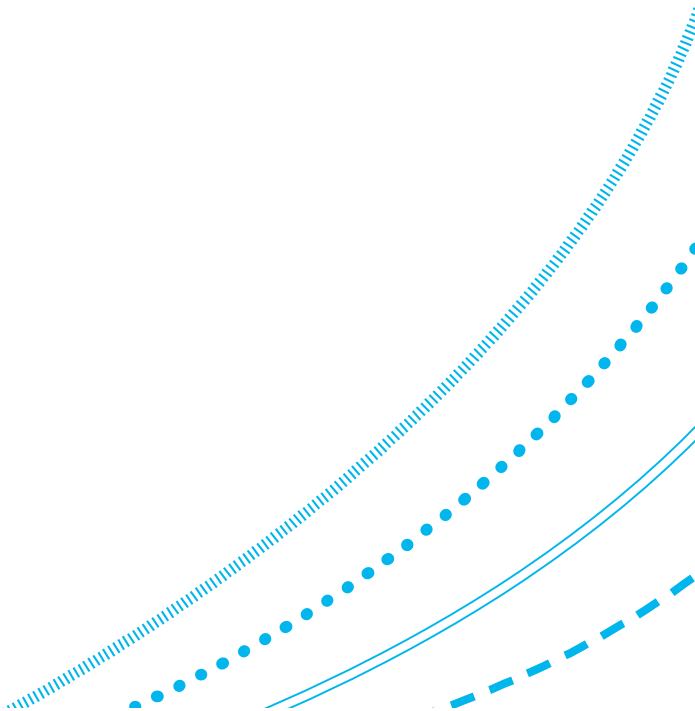
September 2025

Outline of lecture

1. Security applications.
2. Security violations.
3. Security goals: Confidentiality, Integrity, Availability (C.I.A triad).
4. Vulnerability.
5. Key elements.
6. Risk assessment.
7. A method for tackling an information protection problem.

Information security

1. The process of preventing and detecting unauthorised use of your information.
2. The science of guarding information systems and assets against malicious behaviours of intelligent adversaries.
3. Security vs. reliability (e.g. car safety)
    1. Intentional vs. accidental fault/failure.
    2. Baddies in security are arbitrary smart.



Impact of information security

1. Information security is an essential infrastructure technology to achieve successful information-based society.
2. Highly information-based company without information security will lose competitiveness.

Examples of malicious behaviour

1. Fraud: deceiving to get money, goods or service.
2. Theft: stealing from a person or a place.
3. Terrorism: causing damage, disruption and intimidation.
4. Vandalism: damaging or destroying, deliberately and for no good reason.
5. Espionage: stealing info or (commercial) secrets by a spy.
6. Sabotage: causing damage/destruction to gain advantage.

Applications of security

1. For a home or small business:
    1. Mobile phones, tablets
    2. DVD player, pay-TV decoders,
    3. Game consoles,
    4. Prepayment electricity meters,
    5. Internet (SSL, S/MIME, PGP, SSH),
    6. Software license numbers,
    7. Door access cards, car door locks, burglar alarms, etc.

Applications of security (cont'd)

1. Banking:
    1. ATM (Automatic Teller Machines),
        1. The 1st large scale commercial use of crypto.
    2. card authentication codes,
    3. PIN verification protocols,
    4. funds transfers,
    5. online banking,
    6. electronic purses,
    7. digital cash, cryptocurrencies

Applications of security (cont'd)

1. Military:
    1. Identify friend/foe system,
    2. Low probability of intercept and jamming resistant radios and radars,
    3. Weapon-system unlock codes,
    4. Permissive action links for nuclear warheads,
    5. Navigation signals,
    6. GPS

Types of security violations

1. In 1973, James Anderson identified three different types of security violation in computer systems:
    1. unauthorised information release;
    2. unauthorised information modification;
    3. unauthorised denial of use.
2. What we mean by “authorised” or “unauthorised”?
    1. This is defined by the security policy.
3. Why security violations occur:
    1. Inadequate physical controls.
    2. Inadequate controls within the computer system.

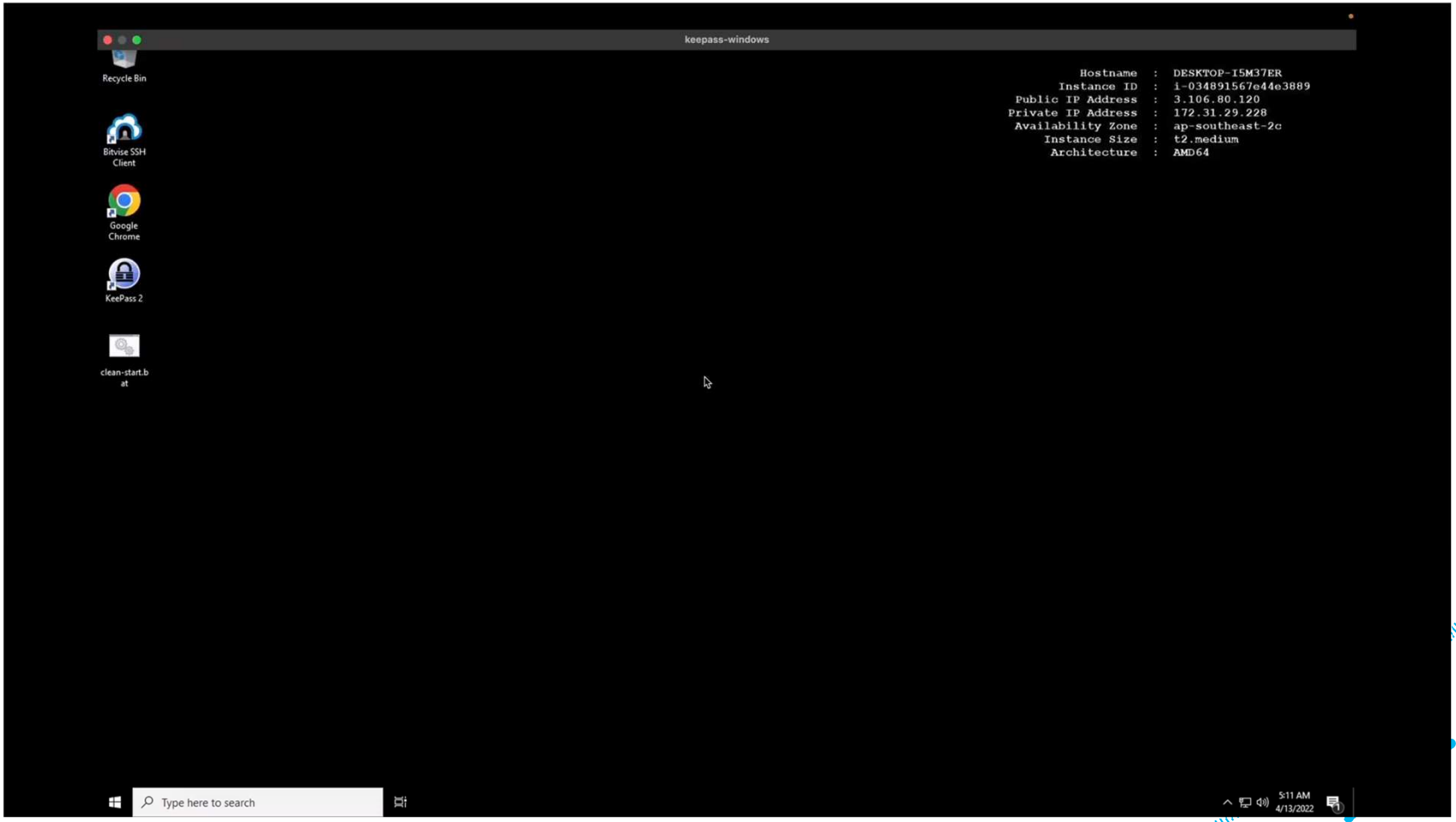
Example: unauthorised information release

1. An unauthorised user reads and copies encrypted passwords from a password file.
2. Then he/she may be able to decrypt passwords offline using brute force (thereby bypassing methods to prevent on-line password cracking).

Example: unauthorized information modification

1. An unauthorised user changes the password file:
    1. might then insert a new entry in the password file (a “backdoor”) and
    2. subsequently be authenticated by the system;
    3. might simply change the root password.

Kevin Mitnick's password manager hack demo



Pop quiz

1. The password hack demo showed that password managers are not 100% secure.
2. How would you protect your passwords from being stolen?

Goals for computer security

1. Confidentiality - prevention of unauthorised information release (info is accessible only to authorised user);
2. Integrity - prevention of unauthorised information modification;
3. Availability - authorised users should not be prevented from accessing to info and associated assets when required;

Confidentiality

1. Confidentiality is about preventing unauthorised users reading information to which they are not entitled.
2. Traditionally, the notions of security and confidentiality are often confused, e.g.
    1. In a military environment, security was traditionally associated with keeping information secret, e.g. by using ciphers to protect communicated information.
3. Variants of confidentiality:
    1. anonymity, copy protection, information flow control, unlinkability, unobservabability, ...

Integrity

1. In the *context of computing*: preventing unauthorised users writing information to which they are not entitled.
2. In a *general context*: ensuring that the system state has not been modified by those not authorised to do so.
3. In the *context of data communication*: detection of modifications to transmitted data.

Availability

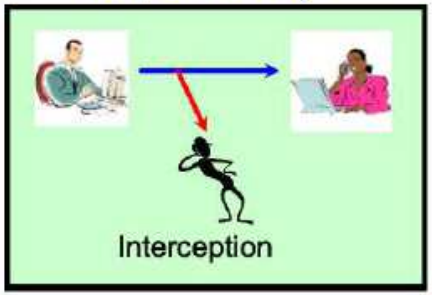
1. Availability can be defined as ensuring that the services provided by a system are accessible on demand by an authorised entity.
2. Availability covers areas beyond the normal scope of security, e.g., fault-tolerant computing.
    1. Fault-tolerance is beyond the scope of this subject.
3. For the purposes of security we are primarily concerned with preventing denial of service attacks by unauthorised entities.
    1. e.g., Internet ’flooding’ attacks, where the attacker(s) overwhelm a server by sending it large numbers of connection requests.

Additional security goals

1. Authentication:
    1. the process of verifying an identity claimed by or for a system entity
    2. example potential authentication protocol: Kerberos protocol
2. Access control (Authorisation):
    1. protection of system resources against unauthorised access
    2. example: ACL
3. Non-repudiation:
    1. protection against false denial of involvement in a communication

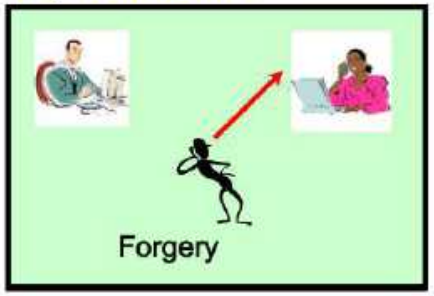
Security needs

Confidentiality



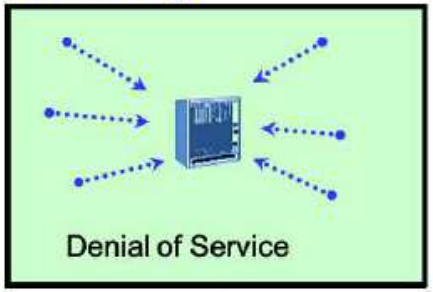
Is Private?

Authentication



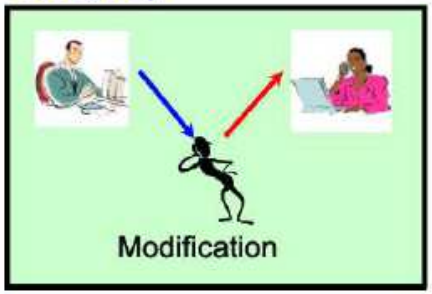
Who am I dealing with?

Availability



Wish to access!!

Integrity

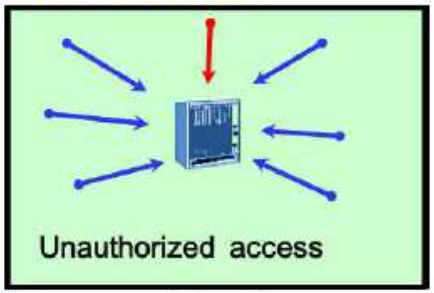


Has been altered?

Non-Repudiation

Who sent/received it?

Access Control



Have you privilege?

Vulnerability

1. A vulnerability is a flaw in the design or implementation of a computer system that could lead to a security violation.
2. Examples include:
    1. program bugs;
    2. configuration errors;
    3. poor choice of passwords;
    4. flawed management of passwords.
3. A vulnerability represents a threat to the security of a system.

Vulnerability (cont'd)

1. A vulnerability might be exploited by an attacker to create a security violation:
    1. The attacker must *know about the vulnerability*:
        1. if an attacker doesn't know of the existence of a potential buffer overrun in a program, then the attacker cannot exploit this vulnerability.
    2. The attacker must be able to *exploit the vulnerability*:
        1. if the computer system can detect buffer overruns at run-time then the vulnerability cannot be exploited.

Personal data

1. What personal data can reveal?
    1. Shopping habits, family status, career, health, finances, sports/hobbies, etc.
    2. Our data is every where and computers are good at collecting it:
        1. Bank: transfers, investments, credit card purchases, taxes.
        2. Telephone: source/destination, time, location.
        3. Shopping/travel: from (online) shops, loyalty programs.
        4. Entertainment: movies watched online.
2. Valuable to sales departments, agencies, employers, ...
    1. but all for criminals
3. Risks: Surveillance, Limitation of Privacy, “Right to be forgotten”, ..
4. Limitations: Regulation vs Self-Regulation

An example: e-voting

1. Potentially a win-win situation for Citizens and Government:
    1. efficiency gain
    2. cost reduction
    3. service improvement

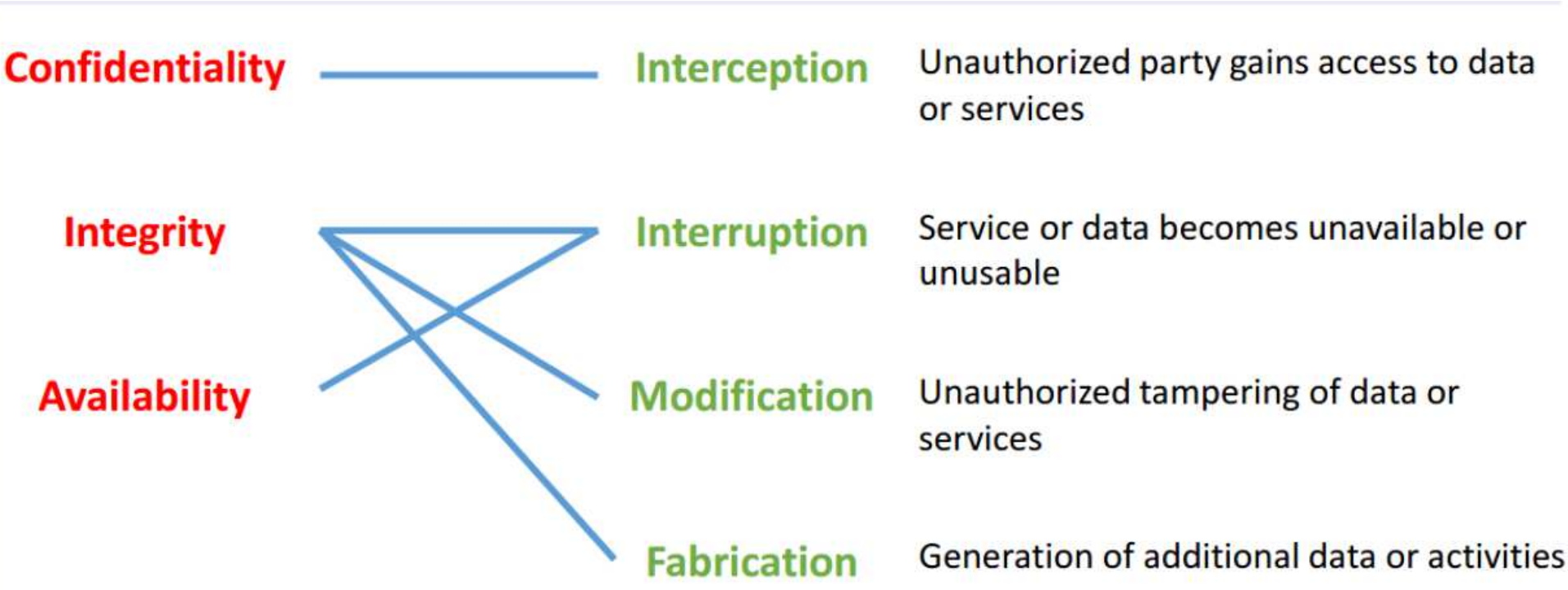
Example: e-voting (cont'd)

1. Security considerations:
    1. How will the system ensure that only registered voters vote?
    2. How will it ensure that each voter can only vote once?
    3. How does the system ensure that votes are not later changed and are correctly counted?
    4. How are votes kept private and identities secret?
    5. System availability? Functional correctness?

Information security analysis

1. Key elements
    1. Assets: what we want to protect
        1. Hardware, Software, Data, Users
        2. Some are easily replaceable, other not.
    2. Vulnerability: a weakness that could be exploited to cause harm.
    3. Threat: a set of circumstances that could cause harm.
    4. An attack is performed exploiting a vulnerability of the system.
    5. Countermeasure: action, device, procedure, or technique that remove or reduce a vulnerability.

Security threats



Example: Confidentiality

1. Asset: E-mail message
2. Vulnerability: E-mail is not a letter but rather a post card
3. Threat: Everyone can read it along the way! (interception)
4. Countermeasures:
    1. protect the communication (network security)
    2. protect the message content (encryption)

Example: Integrity

1. Asset: financial records (bank transfer)
2. Vulnerability:
    1. a defective software component allows unauthorized insider users to read and write records from the database
3. Threat:
    1. the payment amount can be changed (**Modification)**
    2. **an unauthorized payment can be generated (Fabrication)**
4. Countermeasures:
    1. protect the integrity of the records (digital signature)
    2. protect the access to the system (access control)

Example: Availability

1. Asset: online store (Communication with a server)
2. Vulnerability:
    1. there is no limit to the number of parallel transactions a user can begin
3. Threat:
    1. denial of service (Interruption)
4. Countermeasures:
    1. Authenticate the user and do not allow beginning a new transaction unless the previous one is terminated or aborted (secure software engineering)
    2. Limit the number of incoming connections from the same network address (network security)

Security: Intuitive strategies

1. Prevention: take measures that prevent your assets from being damaged
    1. E-commerce as example: encrypt your orders, rely on the merchant to perform checks on the caller, don't use internet (? ‿¨)...
2. Detection: take measures so that you can detect when, how and by whom an asset has been damaged.
    1. An unauthorised transaction appears on your credit card statement!
3. Reaction: take measures so that you can recover your assets or to recover from a damage to your assets.
    1. Complain, ask for a new card number, etc.

Risk assessment

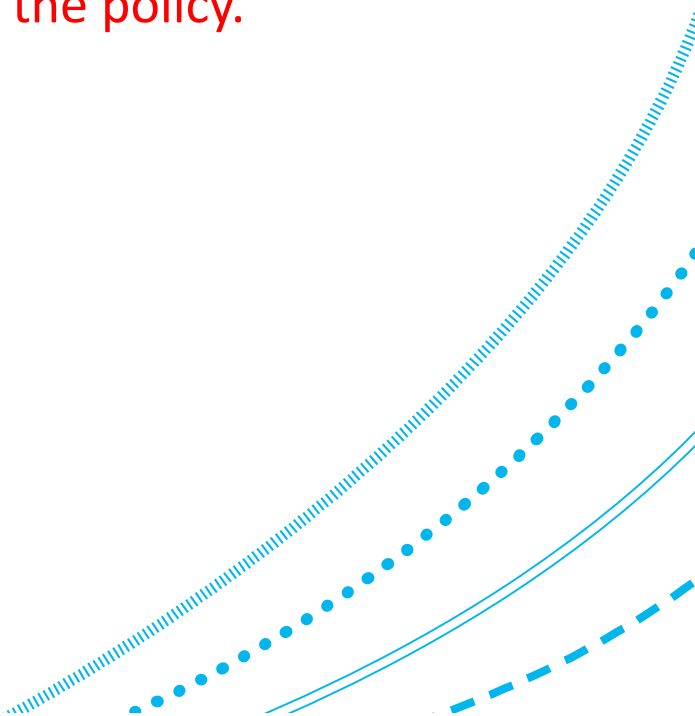
1. The challenge for the IT and Operations managers in this type of environment is to:
    1. properly analyse the threats to and vulnerabilities of an information system,
    2. identify the potential impact that the loss of information or capabilities of a system would have on the business, and, based upon these analyses,
    3. identify appropriate and cost-effective counter-measures.

Risk assessment (cont'd)

1. There are a number of ways of judging the security features of a computer system:
    1. can the operating system and hardware implement memory protection?
    2. is it possible to identify authorised users?
    3. is it possible to define and enforce a discretionary security policy?
    4. is it possible to define and enforce a mandatory security policy?
    5. is it possible to store and protect audit information?
    6. can it be proved that the system meets the above requirements?

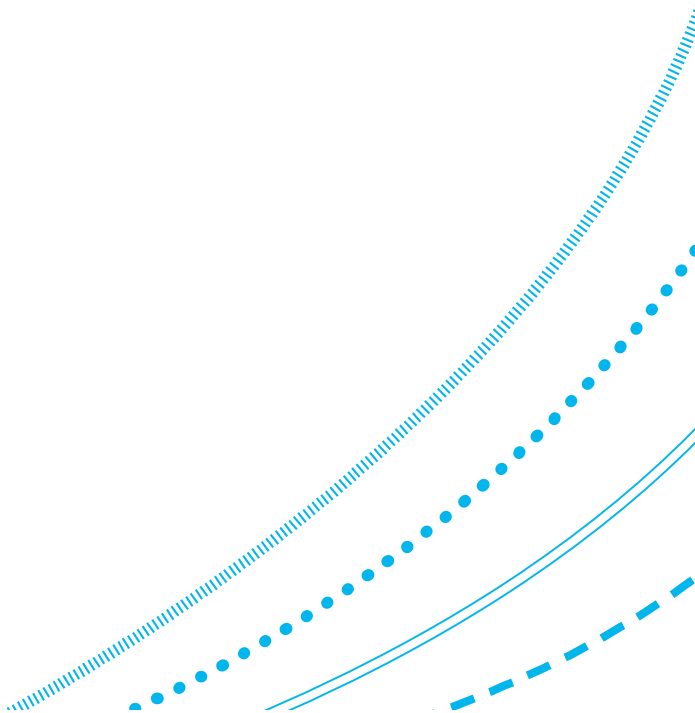
Tackling an information protection problem

1. Drawing up a threat model via security requirement analysis.
2. Formulating a suitable security policy modelling what ought to be protected.
3. Implementing specific protection mechanisms to enforce the policy.



Threat model

1. Identify assets to be protected and their value.
2. Identify vulnerabilities, threats and risk priorities.
3. Identify legal and contractual requirements.



Security policy

1. Which activities are or are not authorised, which states are or are not required, and which information flows are or are not prohibited.
2. Precise and even formal definition of such protection goals; can be procedural instructions for employees.
3. Should be well documented and followed.

Protection mechanism

1. Hardware protection mechanisms.
2. Secure operating systems.
3. Secure coding.
4. Capabilities and access control lists.
5. End user security training.
6. Response to breaches.