Information Security Management

Information Security

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 2

Learning Objectives

After this week the students will

- be familiar with the CObIT Information Criteria
- approach a functional understanding of the concept of risk
- see how security requirements and priorities relate to business objectives

HØGSKOLEN I ÅLESUND
Aalesund University College

Outline

Outline

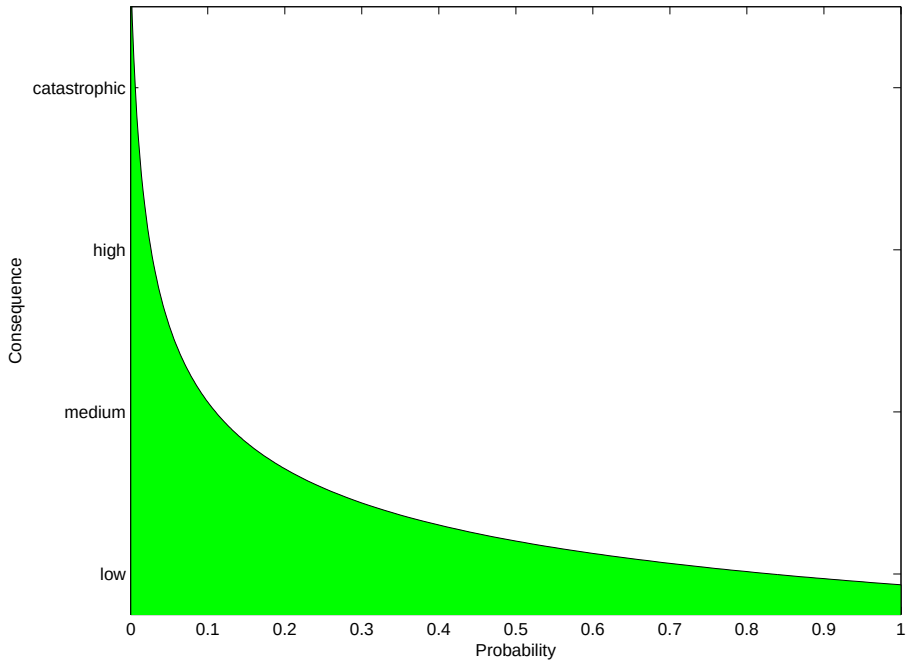
Risk

What is risk?

- Uncertainty about future value
  - ... because of events which may or may not happen
- Two key quantitites
  - Impact or consequence (severity)
  - Probability

Risk appetite

Consequence and Probability



HØGSKOLEN I ÅLESUND
Aalesund University College

Risk Management

Why do we take risk?

Nothing ventured, nothing gained

Den som intet våger, intet vinner

Some common ventures

Web pages

- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff

- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network

- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

HØGSKOLEN I ÅLESUND
Aalesund University College

Some common ventures

Web pages

- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff

- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network

- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

Some common ventures

Web pages
- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff
- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network
- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

Some common ventures

Web pages
- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff
- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network
- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

Some common ventures

Web pages
- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff
- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network
- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

Some common ventures

Web pages
- If you do, you risk break-ins through the web server.
- If you don't, your customers won't find you

Take-home laptops for staff
- If you do, you risk laptops being lost, disclosing confidential information
- If you don't, your staff will do less work.

WiFi network
- If you do, attackers get an additional potential point of entry
- If you don't, your staff will spend more time getting network access for mobile equipment

Does the gain outweigh the risk?

Outline

Information Owner and Risk Owner

- Every asset belongs to some department
  - someone must be responsible for it
- Responsibility demands risk assessment
  - responsible for the impact from any incident
- Asset Owner, Information Owner, System Owner, Risk Owner

Information Owner and Risk Owner

- Every asset belongs to some department
  - someone must be responsible for it
- Responsibility demands risk assessment
  - responsible for the impact from any incident
- Asset Owner, Information Owner, System Owner, Risk Owner

Information Owner and Risk Owner

- Every asset belongs to some department
  - someone must be responsible for it
- Responsibility demands risk assessment
  - responsible for the impact from any incident
- Asset Owner, Information Owner, System Owner, Risk Owner

Fragmentation of Responsibility

The asset owner Does he take responsibility for security?

The security unit Do they understand the value of the assets?

- Effective security work requires understanding of both
  - security measures and threats
  - business processes, assets, and values

Fragmentation of Responsibility

The asset owner Does he take responsibility for security?

The security unit Do they understand the value of the assets?

- Effective security work requires understanding of both
  - security measures and threats
  - business processes, assets, and values

Senior Information Risk Owner

SIRO

- SIRO is required in any British government organisation
- The SIRO has to be a board-level director
  - establishing security awareness at very top of the organisation
  - this is seen as absolutely *essential*
- Member of the board, the SIRO can oversea and influence any department
  - asset owner
  - security
  - IT services

Good idea or Waste

The SIRO

What do you think the SIRO requirement achieves?

- A good SIRO should
  - clarify security risks and implications for chief decision makers
  - relate threats and risks to business processes and purposes
  - ensure that threats and risks are taken into account in all major business decisions
- Where do you find a good and experienced SIRO?
- Will the SIRO just be a scapegoat at hand for when it goes wrong?
- Maybe it is *necessary* and *ineffective* both?

Good idea or Waste

The SIRO

What do you think the SIRO requirement achieves?

- A good SIRO should
  - clarify security risks and implications for chief decision makers
  - relate threats and risks to business processes and purposes
  - ensure that threats and risks are taken into account in all major business decisions
- Where do you find a good and experienced SIRO?
- Will the SIRO just be a scapegoat at hand for when it goes wrong?
- Maybe it is *necessary* and *ineffective* both?

Good idea or Waste

The SIRO

What do you think the SIRO requirement achieves?

- A good SIRO should
  - clarify security risks and implications for chief decision makers
  - relate threats and risks to business processes and purposes
  - ensure that threats and risks are taken into account in all major business decisions
- Where do you find a good and experienced SIRO?
- Will the SIRO just be a scapegoat at hand for when it goes wrong?
- Maybe it is *necessary* and *ineffective* both?

Good idea or Waste

The SIRO

What do you think the SIRO requirement achieves?

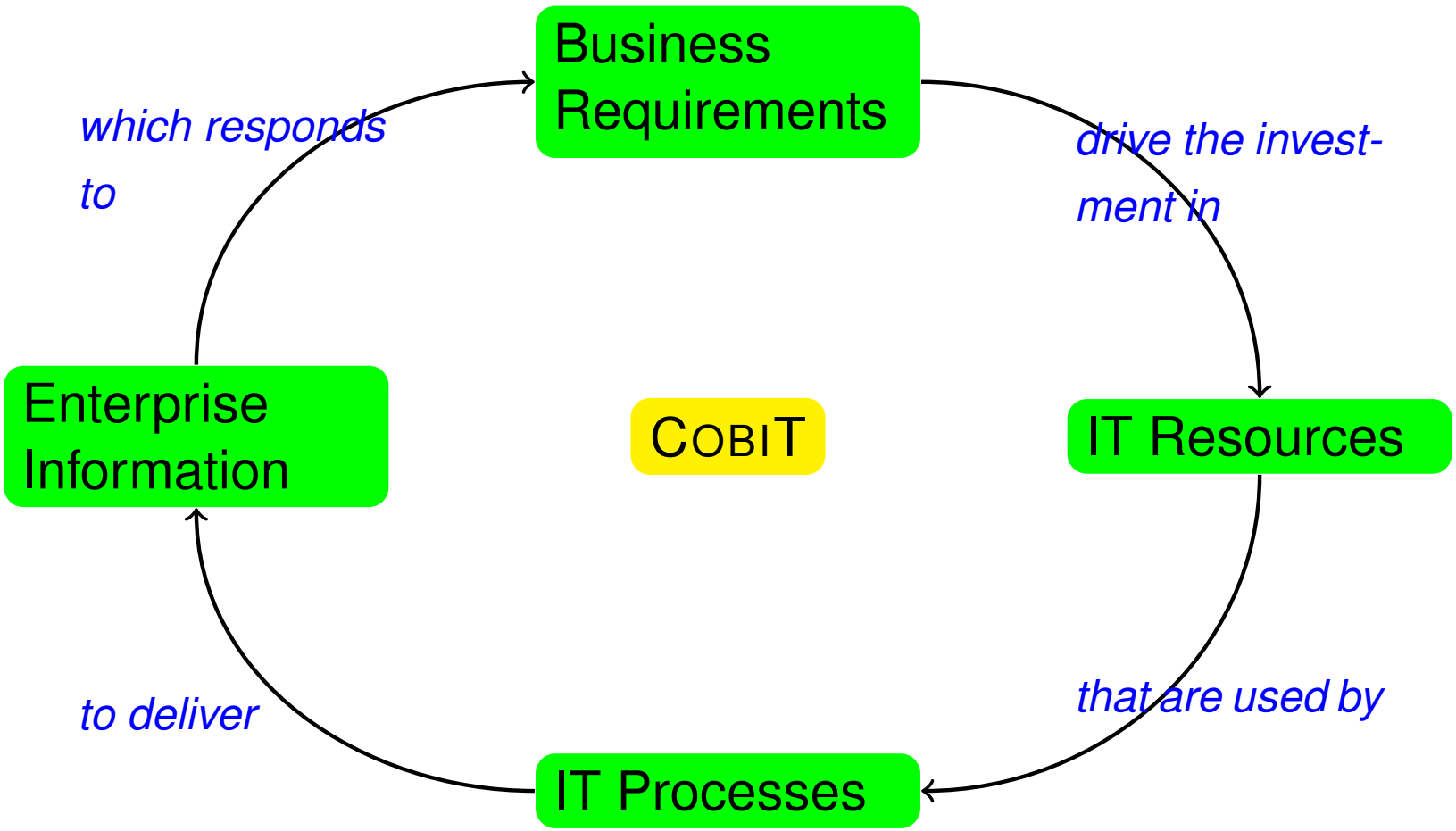
- A good SIRO should
  - clarify security risks and implications for chief decision makers
  - relate threats and risks to business processes and purposes
  - ensure that threats and risks are taken into account in all major business decisions
- Where do you find a good and experienced SIRO?
- Will the SIRO just be a scapegoat at hand for when it goes wrong?
- Maybe it is *necessary* and *ineffective* both?

Outline

The CObIT framework

- CObIT — *Control Objectives for Information and related Technology*
- A framework for control (audit) of information systems
- First version 1996
- Information Systems Audit and Control Association (ISACA)
  - Certified Information Systems Auditor
  - Certified Information Security Manager
- IT Governance Institute (ITGI et. 1998) currently publishes CObIT

The Basic CObIT Principle



The CObIT Information Criteria

- CObIT — Control Objectives for IT
- Information Criteria is more than security
- Security is a means to reaching objectives
- A large organisation and its information assets
  - is a fine and complex machinery
  - requires management with attention to all requirements

The CObIT Information Criteria

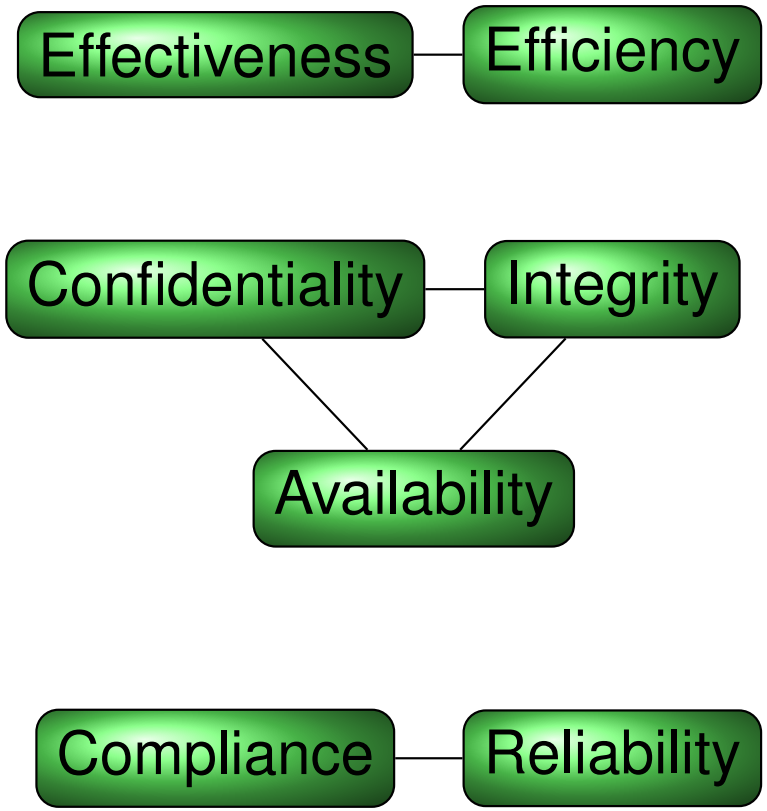
- CObIT — Control Objectives for IT
- Information Criteria is more than security
- Security is a means to reaching objectives
- A large organisation and its information assets
  - is a fine and complex machinery
  - requires management with attention to all requirements

The CObIT Information Criteria

- CObIT — Control Objectives for IT
- Information Criteria is more than security
- Security is a means to reaching objectives
- A large organisation and its information assets
  - is a fine and complex machinery
  - requires management with attention to all requirements

The CObIT Information Criteria

- CObIT — Control Objectives for IT
- Information Criteria is more than security
- Security is a means to reaching objectives
- A large organisation and its information assets
  - is a fine and complex machinery
  - requires management with attention to all requirements



Effectiveness and Efficiency

Effectiveness relevance and suitability of information

- Information has to serve business processes
- accuracy, consistency and usability.

Efficiency information with optimum use of resources

- minimise the cost of providing information and services

The CIA Triad

Security Criteria

Recall from last week ...

Confidentiality against unauthorised disclosure

Integrity against unauthorised modification and falsification

Availability for authorised users

The CIA criteria are largely about maintaining the other criteria in the presence of accidents and adversaries.

Compliance and Reliability

Compliance deals with the adherence to laws, regulations and rontractual agreements

- businesses need to obey the laws of the land
- stick to contracts with clients and suppliers
- observe constent enforcement of own guidelines and policies

Reliability – Reliable Management Information

- appropriate information and metrics to support management of the organisation
- meta-information to allow management of the other criteria
- managing to meet requirements and make surplus

How do you use CObIT?

- Be conscious about why we have the IT system
  - Basc CObIT principle:
    - how IT development interact with business processes
  - Information criteria:
    - key criteria to work for
- Use the principles to choose what risk to take
- The full CObIT material gives a structure management framework
  - may be worthwhile for a large organisation

How do you use CObIT?

- Be conscious about why we have the IT system
  - Basc CObIT principle:
    - how IT development interact with business processes
  - Information criteria:
    - key criteria to work for
- Use the principles to choose what risk to take
- The full CObIT material gives a structure management framework
  - may be worthwhile for a large organisation

How do you use CObIT?

- Be conscious about why we have the IT system
  - Basc CObIT principle:
    - how IT development interact with business processes
  - Information criteria:
    - key criteria to work for
- Use the principles to choose what risk to take
- The full CObIT material gives a structure management framework
  - may be worthwhile for a large organisation

The CIA triad

- CIA is the main security criteria
- remember from last week?

Let's have a closer look at the other four ...

Effectiveness and Efficiency

Effectiveness formålstenlegheit

Efficiency kostnadseffektivitet

- IT systems have to serve a purpose
  - without wasting resources
- Security controls must be balanced against these criteria
  - cost must be less than the risk reduction
  - controls must not render the system ineffective

How do you make the system maximum effective at minimum cost and minimum risk?

Compliance

Adherence to laws, standards, and contracts

Why is compliance a criterion?

- Breaking the law, you may be shut down
- Breaking contracts, you will loose business partners
  - e.g. you cannot process credit card transactions without following the standards set by the credit card companies
- Keeping standards, can make you look more serious and professional
  - legal protection in case of an incident: you did the best you could
  - goodwill from customers and business partners

Punishment and compensation may add to the impact in the case of an incident.

Compliance

Adherence to laws, standards, and contracts

Why is compliance a criterion?

- Breaking the law, you may be shut down
- Breaking contracts, you will loose business partners
  - e.g. you cannot process credit card transactions without following the standards set by the credit card companies
- Keeping standards, can make you look more serious and professional
  - legal protection in case of an incident: you did the best you could
  - goodwill from customers and business partners

Punishment and compensation may add to the impact in the case of an incident.

Reliable management information

- Reliability refers to *reliable management information*
- Requirement to make *well-informed* decisions
- Partly a meta-criterion
  - how well is confidentiality/integrity/availability ensured?
  - how do you know?
  - what can you do to improve it?
- Possible overlap with effectivity
  - information system must be effective for management purposes

Reliable management information

- Reliability refers to *reliable management information*
- Requirement to make *well-informed* decisions
- Partly a meta-criterion
  - how well is confidentiality/integrity/availability ensured?
  - how do you know?
  - what can you do to improve it?
- Possible overlap with effectivity
  - information system must be effective for management purposes

Reliable management information

- Reliability refers to *reliable management information*
- Requirement to make *well-informed* decisions
- Partly a meta-criterion
  - how well is confidentiality/integrity/availability ensured?
  - how do you know?
  - what can you do to improve it?
- Possible overlap with effectivity
  - information system must be effective for management purposes

Reliable management information

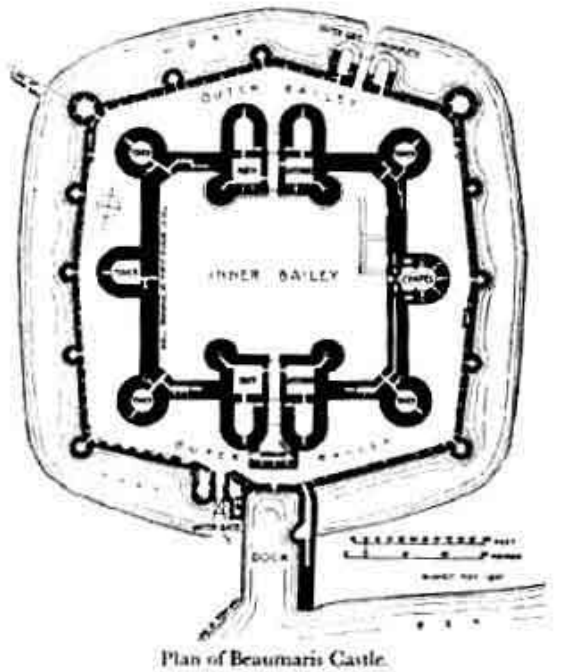
- Reliability refers to *reliable management information*
- Requirement to make *well-informed* decisions
- Partly a meta-criterion
  - how well is confidentiality/integrity/availability ensured?
  - how do you know?
  - what can you do to improve it?
- Possible overlap with effectivity
  - information system must be effective for management purposes

Outline

Outline

Classic Security Measure

- Walls protect the City
- Strict Access Control
- Concentric walls
  - different classification levels



Plan of Beaumaris Castle.

Trust within the City Walls

Whom do you have to trust under a wall-type defence?
Whom do you protect against?

Assumption

A City Wall defence assumes

1. *The enemy is outside the walls*
2. *We can trust anyone inside the walls*

Trust within the City Walls

Whom do you have to trust under a wall-type defence?
Whom do you protect against?

Assumption

A City Wall defence assumes

1. *The enemy is outside the walls*
2. *We can trust anyone inside the walls*

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Security Perimeter

- City Walls form a perimeter
- The perimeter defines the scope of the security mechanism
- Protection against threats originating outside the perimeter
- No protection againts inside threats

Watch out for security perimeters when you discuss controls!

Perimeter Security

- Perimeter Security (or Perimeter Defences) refer to
  - wall-like mechanisms
  - protecting a large system/organisation
  - ... like a city wall
- Simple organisation:
  - concentrate all your resources on the perimeter
  - maintain complete control of who and what is in the city
- Other examples:
  - high-security buildings
  - system-level access control
  - fire-walls
- Most data centres are secured this way

Perimeter Security

- Perimeter Security (or Perimeter Defences) refer to
  - wall-like mechanisms
  - protecting a large system/organisation
  - ... like a city wall
- Simple organisation:
  - concentrate all your resources on the perimeter
  - maintain complete control of who and what is in the city
- Other examples:
  - high-security buildings
  - system-level access control
  - fire-walls
- Most data centres are secured this way

Perimeter Security

- Perimeter Security (or Perimeter Defences) refer to
  - wall-like mechanisms
  - protecting a large system/organisation
  - ... like a city wall
- Simple organisation:
  - concentrate all your resources on the perimeter
  - maintain complete control of who and what is in the city
- Other examples:
  - high-security buildings
  - system-level access control
  - fire-walls
- Most data centres are secured this way

Perimeter Security

- Perimeter Security (or Perimeter Defences) refer to
  - wall-like mechanisms
  - protecting a large system/organisation
  - ... like a city wall
- Simple organisation:
  - concentrate all your resources on the perimeter
  - maintain complete control of who and what is in the city
- Other examples:
  - high-security buildings
  - system-level access control
  - fire-walls
- Most data centres are secured this way

Outline

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
  2. you don't want or need to deal with outsiders

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

The fall of the wall

Why don't modern cities have walls?

- Walls work very well when
  1. you trust your insiders
     - large populations cannot be controlled
     - ... complexity becomes overwhelming
  2. you don't want or need to deal with outsiders
     - why don't we trust a Greek bearing gifts?
     - the walls prevent trade

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

From City Walls to Lock and Key

- The wall gave a small, safe community in hostile surroundings
- In growing cities, trust becomes harder
- The fall of the walls coincide with two other events
  - Standing armies making the surroundings safer
    - creating an outer perimeter
  - Locked doors securing private dwellings
    - creating an inner perimeter

Look up the Jericho Forum (bringing down the walls of Jericho).

Outline

Common problems

A summary

- Fragmentation of responsibility
  - asset owner vs. security consultant
- *One-size fits all* approach of perimeter defences
  - reducing effectivity or efficiency where risk is low
  - inadequate controls where risk is high

How do we solve them?

The fundamental dilemma

IBM Whitepaper view

- Ambivalent attitude to security in businesses
  1. security problems cause serious losses
     - money
     - reputation
  2. security does not contribute to business processes
     - it becomes a pure cost, like insurance and estates
- Security is important, but it has to be cheap
- Value for money is immeasurable in security ...

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

The Manager's Perspective

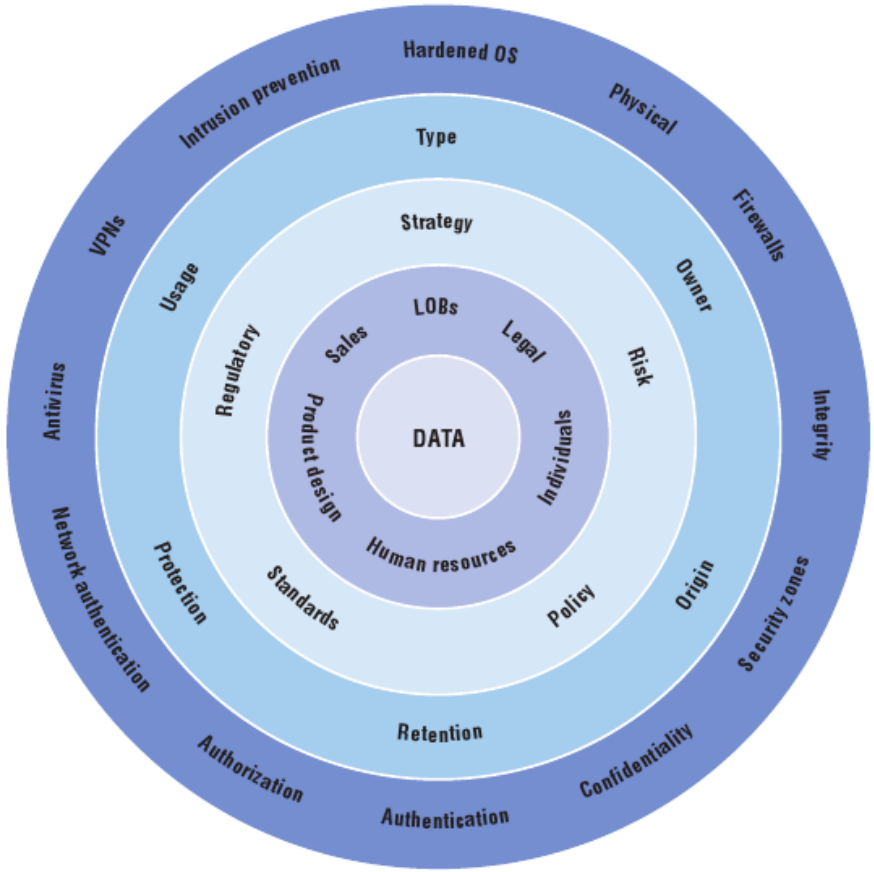
An example

- We want to buy insurance
- A firewall is good insurance
  - it prevents, maybe, 95% of attacks on a global scale
  - if it fails, we can say we followed best *'industry practice'*
- What potential attacks do we face?
  - are they typically attacks which can be prevented?
  - maybe we only face the top 5% attacks?
- The manufacturer does not know the business.
  - Products designed for a general market.
- Insurance assumes that all clients are average or typical
- Businesses rarely are typical.

Data-Centric Security

Figure from IBM's white paper

- Data is the centre of security
- Regulations on data usage
- Who owns the data?
- Who needs the data?
- Who may change the data?
- Security policy for each data asset



The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

The limits of perimeters

- Perimeter defences protect systems
  - Build a firewall around the business
  - Separate the insiders from the outsiders
- Problems with Perimeter Thinking
  - People need to leave the safety of the walls
  - Information needs to leave the safety of the walls
  - One-size-fits-all – no granularity
    - wasting resources on low-value assets
    - failing adequate controls of high-value assets
  - Insider threats

Need to know

- The *Need to know* principle
  - or *principle of least privilege*
- If you don't need it, you don't get it
  - if in doubt, prohibit

Why would we use this principle?

- Underprivileged users will flag it
  - problems can be solved quickle
- Overprivileged users will may exploit it
  - you might not even notice
  - or not before it is too late

Security in Context

- Any effective security programme must focus on
  - assets and their value
  - the assets' place in the prganisation
- We cannot build a wall around the business
  - the business has to be within a world of hazards
- Security must be part of the processes
  - protecting the business in a world of hazards
  - ... not shield it from the world

Outline

Outline

Sårbarheit

Vulnerability

Constant talk about the society being more vulnerable.

- Sårbarheit is a buzz word in Norway
  - *Sårbarhetsrapporten*
- Warning! Two uses of the word «vulnerability»
  - A *vulnerability* (lyte)
    - a weakness to be exploited by a threat
  - The *vulnerability* (sårbarheita) of an organisation (or community or nation)
    - The general state of being susceptible to damage

Sårbarheit

Vulnerability

Constant talk about the society being more vulnerable.

- Sårbarheit is a buzz word in Norway
  - *Sårbarhetsrapporten*
- Warning! Two uses of the word «vulnerability»
  - A *vulnerability* (lyte)
    - a weakness to be exploited by a threat
  - The *vulnerability* (sårbarheita) of an organisation (or community or nation)
    - The general state of being susceptible to damage

What is Vulnerability?

Why have we become more vulnerable?

We put too many eggs in one basket

Power Grid Security

- Power Grid Security is a hot topic in security
  - information security *and* other security
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Power Grid Security

- Power Grid Security is a hot topic in security
  - information security *and* other security
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Power Grid Security

- Power Grid Security is a hot topic in security
  - information security *and* other security
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Increasing Impact

Why could the (major) WikiLeaks incidents not happen 15 years ago?

- What happened?
- How was that possible?

Increasing Impact

Why could the (major) WikiLeaks incidents not happen 15 years ago?

- What happened?
  - Individuals removed gigabytes of data from military bases
- How was that possible?

Increasing Impact

Why could the (major) WikiLeaks incidents not happen 15 years ago?

- What happened?
  - Individuals removed gigabytes of data from military bases
- How was that possible?
  - It fits on a USB stick in a pocket

Increasing Impact

Why could the (major) WikiLeaks incidents not happen 15 years ago?

- What happened?
  - Individuals removed gigabytes of data from military bases
- How was that possible?
  - It fits on a USB stick in a pocket
- Why not 15 years ago?

Increasing Impact

Why could the (major) WikiLeaks incidents not happen 15 years ago?

- What happened?
  - Individuals removed gigabytes of data from military bases
- How was that possible?
  - It fits on a USB stick in a pocket
- Why not 15 years ago?
  - You would need a car load of magnetic disks or tapes

The Risks of Email

What are the risks of email?

- Used to uncritical use
  - personal use and small-talk
- Used for business operations
  - internal (confidential) use
  - external use
- Easy to make mistakes
  - misclicking addresses
  - misconceiving origin
  - keeping the risks in mind
- Threats include: SPAM, phishing, spoofing, eavesdropping

Old threats in new wrapping

- Espionage is about tapping information
  - modern technology gives more information to tap
  - more information in one place
  - equipment to tap more information at once
- Sabotage is about destruction
  - modern installations put more eggs in one basket
  - information technology can give a single point of failure
- Data mining can exploit otherwise harmless information
  - the collection is more than the sum of the parts
  - individual pieces of information may be harmless
  - massive databanks may give detailed information about individuals or organisations

Vulnerability and Risk

- Larger systems: more impact per attack
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Vulnerability and Risk

- Larger systems: more impact per attack
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Vulnerability and Risk

- Larger systems: more impact per attack
- Interconnection: hit one system means hit them all
- Increasing dependency on technology
  - A computer virus or worm can take out a power station
    - e.g. stuxnet (2010)
  - Hospitals and food supply depend 100% on electric power
    - 50 years ago, many more functions could operate without power

Outline

Outline

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

Remember to look for the perimeters when we discuss controls ...

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

Remember to look for the perimeters when we discuss controls ...

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

Remember to look for the perimeters when we discuss controls ...

HØGSKOLEN I ÅLESUND
Aalesund University College

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

Remember to look for the perimeters when we discuss controls ...

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

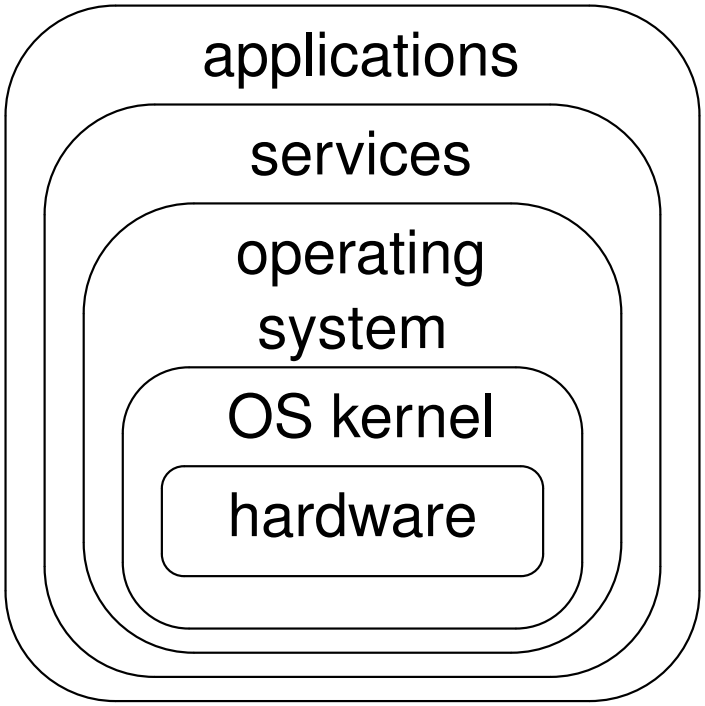
Remember to look for the perimeters when we discuss controls ...

Security Perimeters

- We discussed perimeters in terms of perimeter defences
  - let's extend the concept of a *perimeter*
- Every security control defines a perimeter
  - Abstract or Concrete perimeters
- Only by recognising the perimeter can we understand
  - ... which threats we control (outside)
  - and which entities we have to trust (inside)
- This will become clearer as we proceed

Remember to look for the perimeters when we discuss controls ...

The Man-Machine Scale



- Where on the scale do you put your controls (perimeters)?

Example

Operating System Access Control

- OS requires username and password
  - on the console when the box boots
  - on remote login

'Where' is the security perimeter?
What is inside and what is outside?

- Perimeter defence between software and terminal (keyboard/screen)
  - software inside; user outside
- No defence between software and core hardware (harddisk)
  - the perimeter is not closed!

Example

Operating System Access Control

- OS requires username and password
  - on the console when the box boots
  - on remote login

  'Where' is the security perimeter?
  What is inside and what is outside?

- Perimeter defence between software and terminal (keyboard/screen)
  - software inside; user outside
- No defence between software and core hardware (harddisk)
  - the perimeter is not closed!

Example

Operating System Access Control

- OS requires username and password
  - on the console when the box boots
  - on remote login

  'Where' is the security perimeter?
  What is inside and what is outside?

- Perimeter defence between software and terminal (keyboard/screen)
  - software inside; user outside
- No defence between software and core hardware (harddisk)
  - the perimeter is not closed!

Example

Operating System Access Control

- OS requires username and password
  - on the console when the box boots
  - on remote login

  'Where' is the security perimeter?
  What is inside and what is outside?

- Perimeter defence between software and terminal (keyboard/screen)
  - software inside; user outside
- No defence between software and core hardware (harddisk)
  - the perimeter is not closed!

Example

Operating System Access Control

- OS requires username and password
  - on the console when the box boots
  - on remote login

  'Where' is the security perimeter?
  What is inside and what is outside?

- Perimeter defence between software and terminal (keyboard/screen)
  - software inside; user outside
- No defence between software and core hardware (harddisk)
  - the perimeter is not closed!

Perimeter Observation

Operating System Access Control

- Multi-dimensional
  - there is a physical dimension – hardware
  - there is a more abstract dimension – software
- A user is outside the security perimeter
  - until a successful login
- The OS surrounds the entire system in a software sense
  - attacks through software interfaces are prevented
- The hardware is also inside the OS perimeter
  - but the OS does not control the hardware
  - (except peripheral devices, like the terminal)

Perimeter Observation

Operating System Access Control

- Multi-dimensional
  - there is a physical dimension – hardware
  - there is a more abstract dimension – software
- A user is outside the security perimeter
  - until a successful login
- The OS surrounds the entire system in a software sense
  - attacks through software interfaces are prevented
- The hardware is also inside the OS perimeter
  - but the OS does not control the hardware
  - (except peripheral devices, like the terminal)

Perimeter Observation

Operating System Access Control

- Multi-dimensional
  - there is a physical dimension – hardware
  - there is a more abstract dimension – software
- A user is outside the security perimeter
  - until a successful login
- The OS surrounds the entire system in a software sense
  - attacks through software interfaces are prevented
- The hardware is also inside the OS perimeter
  - but the OS does not control the hardware
  - (except peripheral devices, like the terminal)

Perimeter Observation

Operating System Access Control

- Multi-dimensional
  - there is a physical dimension – hardware
  - there is a more abstract dimension – software
- A user is outside the security perimeter
  - until a successful login
- The OS surrounds the entire system in a software sense
  - attacks through software interfaces are prevented
- The hardware is also inside the OS perimeter
  - but the OS does not control the hardware
  - (except peripheral devices, like the terminal)

Vulnerabilities in lower layers

City walls can be flown over or dug under.

- The OS can control vulnerabilities in the software layers
- Hardware is a lower and therefore unprotected layer
  - we can dig under the defence, through hardware

Can you think of examples of how to dig under the OS access control?

Vulnerabilities in lower layers

City walls can be flown over or dug under.

- The OS can control vulnerabilities in the software layers
- Hardware is a lower and therefore unprotected layer
  - we can dig under the defence, through hardware

Can you think of examples of how to dig under the OS access control?

Vulnerabilities in lower layers

City walls can be flown over or dug under.

- The OS can control vulnerabilities in the software layers
- Hardware is a lower and therefore unprotected layer
  - we can dig under the defence, through hardware

Can you think of examples of how to dig under the OS access control?

Hardware attacks

- Boot the box from a removable medium (USB stick)
  - mount the harddrive and edit the password as superuser
- The box should only boot from the authorised harddrive.
- Remove the harddrive and mount it on a different box
  - replace the password file as superuser
- Physical locks on the cabinet
- In both cases we run an unauthorised OS
  - with access to assets of the authorised OS

Hardware attacks

- Boot the box from a removable medium (USB stick)
  - mount the harddrive and edit the password as superuser
- The box should only boot from the authorised harddrive.
- Remove the harddrive and mount it on a different box
  - replace the password file as superuser
- Physical locks on the cabinet
- In both cases we run an unauthorised OS
  - with access to assets of the authorised OS

Hardware attacks

- Boot the box from a removable medium (USB stick)
  - mount the harddrive and edit the password as superuser
- The box should only boot from the authorised harddrive.
- Remove the harddrive and mount it on a different box
  - replace the password file as superuser
- Physical locks on the cabinet
- In both cases we run an unauthorised OS
  - with access to assets of the authorised OS

Hardware attacks

- Boot the box from a removable medium (USB stick)
  - mount the harddrive and edit the password as superuser
- The box should only boot from the authorised harddrive.
- Remove the harddrive and mount it on a different box
  - replace the password file as superuser
- Physical locks on the cabinet
- In both cases we run an unauthorised OS
  - with access to assets of the authorised OS

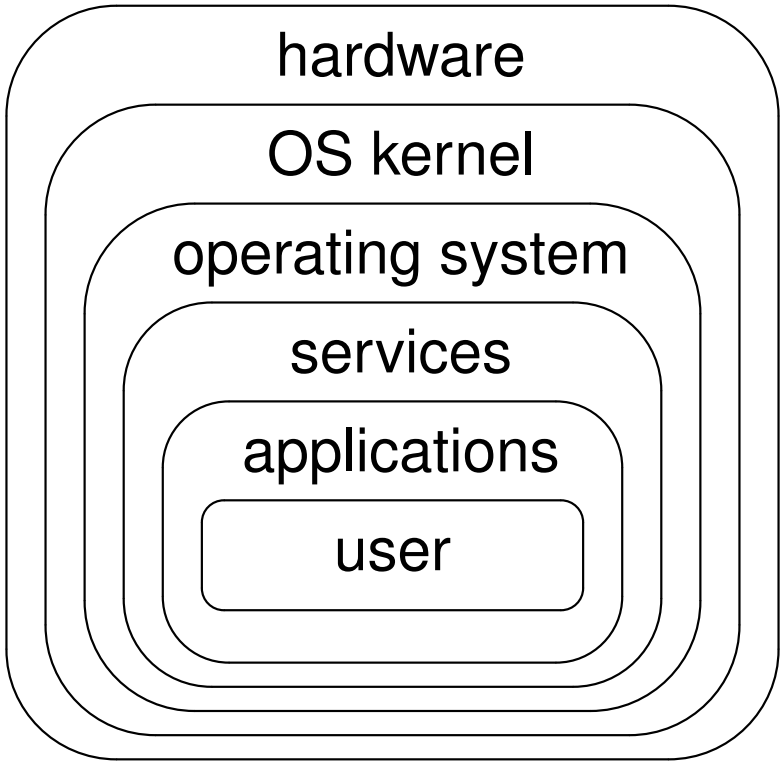
Hardware attacks

- Boot the box from a removable medium (USB stick)
  - mount the harddrive and edit the password as superuser
- The box should only boot from the authorised harddrive.
- Remove the harddrive and mount it on a different box
  - replace the password file as superuser
- Physical locks on the cabinet
- In both cases we run an unauthorised OS
  - with access to assets of the authorised OS

Outline

The Man-Machine Perimeters

- The onion model might have been drawn like this.



- Now, the user is the lower layer

Digging through the human layer

How can you exploit the user to circumvent security?

- Bribery ; Blackmail ; Extortions
- Evesdropping ; Surveillance
- Phishing

Not to speak of carelessness ...

- Passwords stuck under the keyboard
- Easy-to-guess passwords

Digging through the human layer

How can you exploit the user to circumvent security?

- Bribery ; Blackmail ; Extortions
- Evesdropping ; Surveillance
- Phishing

Not to speak of carelessness ...

- Passwords stuck under the keyboard
- Easy-to-guess passwords

Digging through the human layer

How can you exploit the user to circumvent security?

- Bribery ; Blackmail ; Extortions
- Evesdropping ; Surveillance
- Phishing

Not to speak of carelessness ...

- Passwords stuck under the keyboard
- Easy-to-guess passwords

Digging through the human layer

How can you exploit the user to circumvent security?

- Bribery ; Blackmail ; Extortions
- Evesdropping ; Surveillance
- Phishing

Not to speak of carelessness ...

- Passwords stuck under the keyboard
- Easy-to-guess passwords

Digging through the human layer

How can you exploit the user to circumvent security?

- Bribery ; Blackmail ; Extortions
- Evesdropping ; Surveillance
- Phishing

Not to speak of carelessness ...

- Passwords stuck under the keyboard
- Easy-to-guess passwords

Controls in the human layer

How can you protect against the attacks in the human layer?

Outline

Information Security

A definition?

Definition

Information security is protection against breach of confidentiality, integrity and availability of the information processed by the system and the system in itself

- Information Security must be managed in a much wider context
- *Information Assets Management*
  - subject to many criteria including CIA (cf. CObIT)

Look up common threats in the book (Ch. 2). You are probably familiar with most already.

In this module your challenge is to put them into context.

HØGSKOLEN I ÅLESUND
Aalesund University College