Introduction

Alessandro Armando

Computer Security Laboratory (CSec)
DIBRIS, Università di Genova

Computer Security

Outline

Where? Everywhere!

Computing: The net is the computer!

Must assure selective access to machines, programs, data, computational resources, etc.
Privacy of data, activities, ...

Banking: ATMs, home banking, etc.

Access to accounts, integrity of data, nonrepudiation of transactions, ...

Telecommunications: e.g., mobile (GSM) networks

Confidentiality of communication, location information, ...

(E-)Government: government on line!

Outline

Information Security

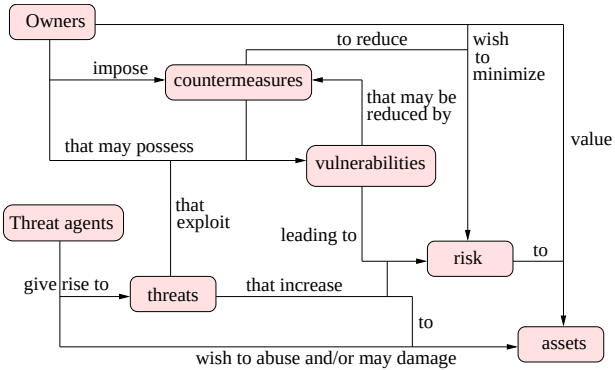
- **Computer security** deals with the prevention and detection of unauthorized actions by users of a computer system.
  - **Authorization** is central to definition.
  - Sensible only relative to a **security policy**, stating who (or what) may perform which actions.
- **Information security** is even more general. It deals with **information** independent of **computer systems**.
  Note that information is more general than data. Data conveys information. But information may also be revealed, without revealing data, e.g., by statistical summaries.
- Constitutes a basic right: protection of self (posessions, ...).

Information Security: Key Concepts

- Security concerns the protection of **assets** from **threats**.
  Threats are the potential for abuse of assets.
- **Owners** value their assets and want to protect them.
  Threat agents also value assets, and seek to abuse them.
- Owners analyse threats to determine which ones apply; these are the **risks** that can be costed. This helps the selection of **countermeasures**, which reduce the **vulnerabilities**.
- Vulnerabilities may remain, leaving some residual risk; owners seek to minimise that risk, within other constraints (feasibility, expense).

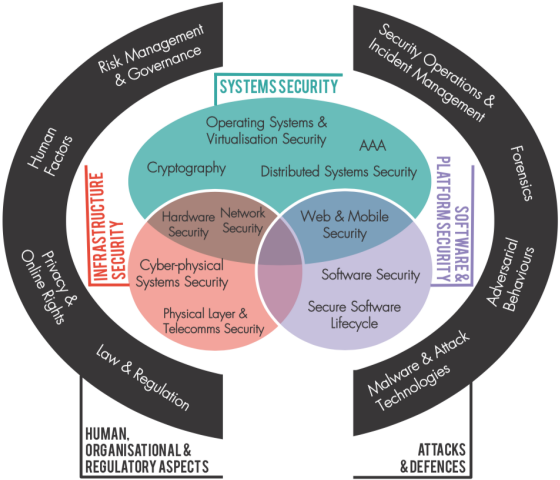
Note: Threats may come from malicious or accidental human activities; usually we focus on malicious activity.

Information Security: Key Concepts



- Classification depicts fundamental concepts and interrelationships.
- Policy (here implicit) defines authorized actions on assets, i.e., what constitutes abuse.

The Cybersecurity Body of Knowledge (www.cybok.org)



Outline

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security properties

confidentiality	*information is not learned by unauthorized principals*
integrity	*data has not been (maliciously) altered*
authentication	*principals or data origin can be identified accurately*
availability	*data/services can be accessed when desired*
accountability	*actions can be traced to responsible principals*

- Usually we want to protect all properties in specific ways.
- Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**.
- The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Protection countermeasures

- **Prevention.** Try to prevent security breaches by system design and employing appropriate security technologies as defences.
  For example, using a firewall to prevent external access to corporate intranets.
- **Detection.** In the event of a security breach, we try to ensure that it will be detected. Logging and MACs (file hashes to detect alteration) are primary methods of detection, although *intrusion detection* systems which actively watch for intruders are more common.
- **Response.** In the event of a security breach, we must respond or recover the assets. Responses range from restoring backups through to informing appropriate concerned parties or law-enforcement agencies.

Confidentiality, privacy and secrecy

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: *privacy* pertains to confidentiality for individuals, whereas *secrecy* pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of *anonymity*, keeping one's identity private.
- Example violations: your medical records are obtained by an employer without your consent.

Confidentiality, privacy and secrecy

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: *privacy* pertains to confidentiality for individuals, whereas *secrecy* pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of *anonymity*, keeping one's identity private.
- Example violations: your medical records are obtained by an employer without your consent.

Confidentiality, privacy and secrecy

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: *privacy* pertains to confidentiality for individuals, whereas *secrecy* pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of *anonymity*, keeping one's identity private.
- Example violations: your medical records are obtained by an employer without your consent.

Confidentiality, privacy and secrecy

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: *privacy* pertains to confidentiality for individuals, whereas *secrecy* pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of *anonymity*, keeping one's identity private.
- Example violations: your medical records are obtained by an employer without your consent.

Integrity

Data has not been maliciously altered

- Integrity has more general meanings elsewhere, but in computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so.
- Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.
- Example violation: an on-line payment system alters an electronic cheque to read 10.000 Euro instead of 100 Euro.

Integrity

Data has not been maliciously altered

- Integrity has more general meanings elsewhere, but in computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so.
- Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.
- Example violation: an on-line payment system alters an electronic cheque to read 10.000 Euro instead of 100 Euro.

Integrity

Data has not been maliciously altered

- Integrity has more general meanings elsewhere, but in computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so.
- Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.
- Example violation: an on-line payment system alters an electronic cheque to read 10.000 Euro instead of 100 Euro.

Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email or stealing credentials.

Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email or stealing credentials.

Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email or stealing credentials.

Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email or stealing credentials.

Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email or stealing credentials.

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance.
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance.
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance.
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance.
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.

Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.

Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.

Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.

Outline

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.

Managing security: implementing a solution

- A *security analysis* surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A *threat model* documents the possible threats to a system, imagining all the vulnerabilities which might be exploited.
- A *risk assessment* studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks.
- A *security policy* addresses the threats, and describes a coherent set of *countermeasures*.
- The costs of countermeasures is compared against the risks, and juggled to make a sensible trade-off.
- This allows a *security solution* to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.