Managing Cybersecurity

Vítor Francisco Fonte, vff@di.uminho.pt, University of Minho, 2024

Security as a Management Decision

- Deployment of security measures is a management decision
- Technical security measures have to work hand in hand with organisational measures to be effective
- Management decisions should be underpinned by some analysis of current risks and threats

Motivation for Attacks

- Financial gain
- Technical challenge (and bragging rights)
- Exact revenge
- Vandalism
- Hacktivism
- Terrorism
- Cyberwar

Attacks and Technical Skill Set

- Technical (e.g. OS, Network, Software, Cryptography, Hardware)
- Non-technical (e.g. Social Engineering)
- Other non-IT related fields of expertise (e.g. Lock-picking)
- All of the above

Profile of an Attacker

- Placement: insider vs outsider
- Level of expertise
- Level of planning
- Level of access to resources
- Protection from international law

Example of Attackers

- Lone attackers, script kiddies
  - Usually run known attacks via already available exploits, …
- Professional criminals / gangs
  - Take control of thousand of computers, SPAM, phishing, DDoS, …
- Governments
  - Huge computing power, crypto-hacking, wiretapping, legal powers, …
- Internet Service Provider
  - Do “spy” on you, may sell (and loose) your data, …
- Insiders
  - Access to assets, usually more damaging than external attackers, …

Security as a “People Problem”

- Cannot be solved by technology alone
- Security must entangle:
  - Legal system defines acceptable behaviour (eg. data protection and computer misuse)
  - Management defines policies and practices within an organisation, to comply with general law and be effective in doing business
  - Organisational policies and practices must translate into security mechanisms put in place by technical experts and staff
  - All users must comply the organisation policies and practices throught the security mechanisms put in place
  - The legal system, the organisation management and technical experts must collaborate in order to achieve effective security

Security and the Organisation

Organisations developing IT services and products

- No clear dividing line between security-relevant components and the rest of a system.
- Security should be addressed as early as possible and at every stage in service and product development:
  - Architectural design and documentation
  - Development and testing
  - Operation and monitoring
  - Source code maintenance and evolution
  - Third-party dependencies

Security and the Organisation

Organisations developing IT services and products

- Developers should be subject to regular security training put in place by the organisation
- Developers should be made aware of the environment in which a service will be deployed:
  - They need to know the expected dangers
  - So that they can highlight the need for protection
  - Even if they do not implement the protection mechanisms themselves
- Developers must be aware that certain categories of sensitive data have to be processed according to specific rules and regulations (e.g. personal data)
- Developers must keep up to date with known coding vulnerabilities

Security Policies

- Security policy:
  - A statement that defines the security objectives of an organisation;
  - It has to state what needs to be protected;
  - It may also indicate how this is to be done.
- Examples:
  - It may regulate access to company premises;
  - It may regulate access to documents;
  - It may stipulate who is authorised to approve commercial transactions on behalf of the company;
  - It may define password formats and renewal intervals.
- Considerable variety in the target of policies and the level of detail they are expressed in.

Security Policies

- A policy has given objectives:
  - **Security policy objective:** A statement of intent to protect an identified resource from unauthorised use.
- How the objectives are to be met can be done first at the level of the organisation:
  - **Organisational security policy:** The set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes resources to achieve specified security policy objectives.
- Organisational policies can be supported by technical means:
  - **Automated security policy:** The set of restrictions and properties that specify how a computing system prevents information and computing resources from being used to violate an organisational security policy.
  - It may define access control lists and firewall settings, the services that may be run on user devices, the security protocols for protecting network traffic, etc.

Measuring Security

- To convince management (or customers, partners) of the benefits of a new security mechanism it would be nice to measure the security of the system before and after.
- It is difficult to reach well-founded management decisions if such information cannot be procured.
- First, values for various security-relevant factors are obtained (**security measurements**).
- Secondly, a set of measurements may be consolidated into a single value that is used for comparing the current security state against a baseline or a past state (**security metrics**).

Measuring Security

- Some values can be established objectively (e.g. number of open ports) but not all (e.g. reputation of a company).
- Sometimes, the result of a measurement can directly be used as a metric (e.g. the number of software vulnerabilities flagged by an analysis tool).
- Ideally, a security metric gives a quantitative result that can be compared to other results, not just a qualitative statement about the security of the product or system being analysed.
  - A *product* is a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
  - A *system* is a specific IT installation, with a particular purpose and operational environment.

Measuring Security

- Measurements of a product are indicative of its potential security.
- But even a secure product can be deployed in an insecure manner.
  - E.g. an easily guessable password, for example, does not offer much protection.
- It is a task for security management to ensure that the security features provided are properly used.

Measuring Security of a Product

- Number of security flaws (bugs) detected as a security metric:
  - Tracking the discovery of flaws over time may serve as the basis for predicting the time to the discovery of the next flaw
  - Usually assume that the detection of flaws and the invocation of buggy code are governed by a given probability distribution given
- Measure the attack surface of a product:
  - Number of interfaces to outside callers
  - Number of dangerous instructions in the code

Measuring Security of a Product

- These proposals are measurements in the sense that they deliver quantitative results.
- It is open to debate whether they really measure security:
  - How relevant is the number of security flaws?
- It is open to debate whether such metrics could be the basis for a meaningful security comparison of products:
  - How common are two products that serve exactly the same purpose?
- It has been suggested that these metrics should be treated as *quality metrics* best used for monitoring the evolution of individual products

Measuring Security of a System

- Look at the actual configurations of the products deployed.
- In a system with access control features, look at the number of accounts with system privileges or the number of accounts with weak passwords.
- In a networked system, look at the number of open ports or at the services accessible from outside and whether the currently running versions have known vulnerabilities.
- For computer networks, you may measure the connectivity of nodes in a network to assess how quickly and how far attacks could spread.

Alternative Measurements of Security

- Try to measure security by measuring the cost of mounting attacks.
  - The time an attacker has to invest in the attack, e.g. analysing software products.
  - The expenses the attacker has to incur, e.g. computing cycles or special equipment.
  - The knowledge necessary to conduct the attack.
- However:
  - The cost of discovering an attack for the first time is often much larger than the cost of mounting the attack itself.
  - When attack scripts are available, attacks can be launched with very little effort or knowledge of the system vulnerabilities being exploited.

Alternative Measurements of Security

- Focus on the assets in the system given and measure the risks these assets are exposed to.
- We have at best metrics for some individual aspects of security:
  - The search for better metrics is still an open field of research.

Security Standards

- Some industry branches have prescriptive security management standards that stipulate what security measures have to be taken in an organisation:
  - E.g. regulations for the financial sector, or rules for dealing with classified material in government departments
- Other management standards are best described as codes of best practice for security management.
  - The most prominent of these standards is ISO 27002.

ISO 27002

Main topics

- **Security policy.** Organisational security policies provide management direction and support on security matters.
- **Organisation of information security.** Responsibilities for security within an enterprise have to be properly organised.
- **Asset management.** To know what is worth protecting, and how much to spend on protection, an enterprise needs a clear picture of its assets and of their value.
- **Human resources security.** Your own personnel or contract personnel can be a source of insecurity.
- **Physical and environmental security.** Physical security measures (fences, locked doors, etc.) protect access to business premises or to sensitive areas (rooms) within a building.
- **Communications and operations management.** The day-to-day management of IT systems and of business processes has to ensure that security is maintained.
- **Access control.** Access control can apply to data, services, and computers. Particular attention must be applied to remote access.
- **Information systems acquisition, development, and maintenance.** Security issues have to be considered when an IT system is being developed.
- **Information security incident management.** Organisations have to be prepared to deal promptly with security incidents.
- **Business continuity management.** Put measures in place so that your business can cope with major failures or disasters.
- **Compliance.** Organisations have to comply with legal, regulatory, and contractual obligations, as well as with standards and their own organisational security policy.

ISO 27002

- ISO 27002 is not a technical standard for security products or a set of evaluation criteria for products or systems.
- Compliance with ISO 27002 can be an onerous task.
- The current state of an organisation regarding the standard has to be established and any shortcomings identified have to be addressed.