COMPUTER SECURITY, part I

T. Karvi

October 2007

Information-security classification I

Information security is an extensive subject. Below is a list of different areas of information security. The classification used here is fairly common and widely used in textbooks on information security.

- Administrative security covers measures taken to specify the principles and courses of action of an organisation: security, recovery and standby plans.
- Personnel security covers the personnel risk management and trust issues with the help of job descriptions, user-access specification, as well as security education and monitoring.
- Physical security includes the physical protection of hardware, user and storage facilities, archives, and appliances and materials, as well as protection of network cables.
- Data-communication security covers measures taken to ensure the confidentiality, integrity, and availability of information transmitted over a network.

Information-security classification II

- Hardware security includes security features of hardware assemblage, maintenance, and quality assurance.
- Information collection security includes the identification and security classification of documents, records and files, as well as the management and storage of information media at all stages of processing, from creating them to final deletion.
- Software security covers the security features of operating systems, applications and data-communication software.
- User security consists of the secure user principles of personnel, the monitoring of events impacting on the user environment and data processing itself, as well as the employment of methods that ensure the continuity of usage.

Former information-security education programme of Learning Institute Dipoli I

- Information security as an integrated part of an organisation.
- Legislation and official supervision of information security.
- Identification and management of risks.
- Classification and monitoring of information bodies.
- Development of systems and security of their maintenance.
- Security of hardware and software.
- Encryption methods and their management.
- Data-communications security.
- Personal security.
- Physical security.
- User security and acquisition of information-system services.
- Management of business continuity.
- Control and development of information security.

Security education for security management I

- Security in a corporate environment and security management.
- Identifying and managing security risks.
- A legislative framework for security management.
- Security communications and information, security education.
- Security in production and operations.
- Work security.
- Rescue operations.
- Environmental security.
- Provision and continuity planning.
- Information security.
- IT security.
- Monitoring of facilities and security.
- Security of financial administration and management.

Security education for security management II

- Security of personnel and overseas operations.
- Security Management.
- Security plans and projects.
- Development and management of security.

The basic components that a security protocol is usually built on I

- Confidentiality. Means protecting information from passive attacks (tapping). Usually accomplished by encryption.
- Authenication. This has the goal of verifying that the communicating party is who it claims to be. The technologies used currently are digital signatures and certificates .
- Integrity. The technology is used to ensure that any changes in messages or files are detected. The technologies are based on the use of hash functions They are used to compute an identifier for the information that is shorter than the whole body of information, yet hard to forge.

The basic components that a security protocol is usually built on II

- Non-repudiation. A typical example is where a customer who has placed an order later denies having placed the order, thereby causing the supplier some expenses. This is also accomplished with digital signatures and time stamps.
- Access control. More integrated in traditional data processing than cryptology. Mostly implemented on the level of the operating system and with the help of anti-virus software. When it comes to networks, firewalls are also included in this area.
- Availability. Many applications have been vulnerable to various kinds of attacks, where mass postings are sent to a service provider. The attacks can be averted with the help of verification and encryption, monitoring service requests, firewalls, etc.

The first four items in the list fall under the heading of cryptology
Cryptology is a large and demanding field that includes both the study of codes and algorithms for encryption and development of codes (cryptography) and decryption of codes (crypto-analysis).
A cryptographic system (cryptosystem) is a system built of common, basic cryptographical components, primitives. At the beginning of the course, we will have to study the basics of cryptography, because the protocols are heavily reliant on a few basic methods.

Sub-areas of cryptography I

- Traditional, symmetrical encryption methods based on a shared, secret key are still being elaborated.
- Public key ciphers is still being perfected, as well. Methods of elliptic curves are gradually replacing RSA. A theoretical breakthrough was gained a few years ago when it comes to identity-based public-key encryption.
- Various digital signatures and certificates are issues currently under implementation.
- Hash functions are being studied and improved again at the moment, because recently used hash methods have been cracked.
- The exchange and management of keys is an essential part of cryptography, and many protocols have been developed for them.

Sub-areas of cryptography II

- The group European Network of Excellence in Cryptography lists the following topics for research during 2007-2013 in their July 2006 publication:
  - verifiable security,
  - combining cryptographic protocols,
  - automatic or interactive methods for verifying security,
  - individual protection on the net,
  - light security protocols and energy-efficient cryptography,
  - watermarks.
- Among the more exotic areas, we can mention steganography, covert channels and zero-knowledge proofs. Lately, zero-knowledge proofs, for example, have surfaced in real situations. (PET, privacy enhancing technologies).
- In future, quantum encryption and verification may play a more important role than today. At the moment, verification is fairly slow and expensive to use, which limits its application.

The design of encryption methods requires a surprising amount of algebra (such as the theory of finite fields) and crypto-analysis.

When designing and implementing cryptosystems, we can get away with less basic skills, if we use ready-made encryption primitives. In that case it will suffice to be able to select the proper primitives offering the services required.

Based on them, we can start designing the information-security protocol. However, when implementing the protocol, we need to take so many details into consideration that producing a reliable system usually requires teamwork.

Design difficulties

- We must be extremely careful if we want to construct cryptographic software ourselves.
- In fact, it is best not to start designing and implementing encryption methods or cryptographic protocols unless you are an expert in this field.
- Another recommendation that is often repeated is that, before starting the commercial production of an encryption method, it has been published and studied for at least 3-5 years.

Administration of information security

- In practice, the administration of information security is one of the first things to organize in an organisation that wants to protect itself from information leaks.
- The use of strong encryption methods, for example, will not help if the system has been invaded by a Troyan horse, if passwords are not good, or if the personnel are easy to bribe or blackmail.
- Many features of information-security administration will seem self-evident, but they should be repeated constantly in order to convince each member of the organization to abide by them.
- Administration standard
  - When designing information systems, we can prepare for security risks with the help of the SSE-CMM process model.
  - Information systems can be classified according to the strength of their information security with the help of Common Criteria.
  - The management system security of an organisation's information administration can be measured with the BS7799 standard.

Access control

- Access control is the first thing to arrange in a network environment.
- The first thing to specify in access control is who has access to which parts of the system, i.e. to specify the access policy.
- Then a mechanism, the security mechanism, has to be introduced to implement the selected policy.
- This differentiation of the policy and its implementation mechanism clarifies the specifications. It is possible to use general policy languages, for example, to specify access rights, and they can then be monitored with a direct mechanism afforded by the operating system and applications.

Types of access control

The types of access control can be divided into three or four classes.

Definition

If an individual user can set the user access for an object, it is called discretionary access control or identity-based access control.

With discretionary access control, the access rights are based on subject and object identity. The key word here is identity; the owner of an object limits access by specifying who has access to the object. The specification is based on the identity of the subject.

Definition

In mandatory or rule-based access control, the objects are classified on hierarchical levels according to the safety requirements of the objects (e.g. top secret, secret, confidential), safety levels are set for the subjects, and subjects can access an object if the subject/object pair fulfils the pre-specified security criteria based on hierarchical security levels.

Operating systems, for example, force users to follow mandatory access control in many situations. Neither subject nor owner of an object can specify who has access.

Definition

Originator-controlled access control, Orcon, is based on the specifications of the object originator.

With this policy, the creator of an object, such as a file, decides who has access to the file. The owner of the file cannot change the decision.

We can also define role-based access control. Access will not be given to single subjects, but to roles that different subjects can adopt within the scope of a set of rules. The above-mentioned three access control types can be specified for the roles.
There are several access control mechanisms. The operating system partially handles access control, at least to files. Passwords play an important part in implementing access control.

General information on passwords

- The most common identifying mechanism is based on passwords.
- Passwords seem to offer good protection against unauthorized access, though careless selection and use of passwords may give rise to risks.
- We also have to take some simple facts into consideration in the software, such as that the software may not ask for a username and immediately let the user know that it is incorrect. This would let an intruder know that the username is wrong. It is better to ask for both the username and the password, and then let the user know that one of them is incorrect. This way the intruder will not know which is wrong, the username or the password.

In addition to passwords, other factors can be used to identify users, such as taking the time of day into consideration, e.g. working hours, when it is possible to log in to the system. Access is denied after hours.

Attacks on passwords

Below is a list of typical attacks on passwords:

- Try every possible password.
- Try many possible passwords.
- Try passwords that are typical for a specific user.
- Scan the system for a list of passwords.
- Ask a user.

Time estimates

- If passwords consist of letters A-Z and they can be 1-8 characters long, there are a total of $26^9 - 1 \approx 5 \times 10^{12}$ possible passwords.
- If the computer tries out one password per millisecond, it would take 150 years to go through all the possible passwords.
- If each try would only take one microsecond, it would only take two months to try them all. This is no longer an unreasonably long time. This is why the software is usually programmed to identify a user slowly, though the user does not observe the slowness. However, the method of trying every possible password described above becomes impossible.

Bad passwords

- People choose passwords that are fairly easy to remember. This helps crackers.
- There are about 80,000 words in English, for example, a very small number for a computer.
- If a password resembles words in a natural language, it is also easier to crack. In Finnish, for example, there cannot be very many consonants in a row.
- Furthermore, people tend to select words or phrases that mean something to them personally: the names of their children, friends, celebrities, sportsmen, etc.
- Simple replacements, where one character of a word is replaced with another character, do not improve the security radically.

Attack strategies against passwords

Below is a list of how an attacker may try to guess passwords. It is fairly easy to program this method.

- no password
- same as username
- user's name or derivative of it
- normal word plus normal names or conjugations
- short dictionary
- full thesaurus
- general foreign-language dictionary
- short dictionary with modified words; upper-case and lower-case letters exchanged, replacements (e.g. o instead of O).
- same as above but in foreign languages
- full run-through with lower-case letters
- full run-through with full character set

List of usernames and passwords

- When a user's access rights are checked, the computer compares the username and password with the data stored on it. This is why there must be a list of usernames and passwords stored on the computer.
- In some systems, the list consists of a file containing a table. It is evident that the file has to be protected very carefully.
- The protection can be implemented by giving file access only to the operating system.
- On the other hand, not all the modules of the OS need to have access to the password file. Unfortunately, there are operating systems that have not been divided into different modules for security reasons, but all the OS modules can access the password file.
- This means that, if the attacker finds a weak point in the operating system, he gains access to all information in the system. Thus it is better that only modules that really need the data have access to passwords.

- To avoid having the password file recovered from e.g. a backup copy or a memory dumping, the password file is usually encrypted.
- When comparing the username and password entered, it is not a good idea to decrypt them at any point. Instead, we should proceed so that the entered information is first encrypted, then compared with the password file.
- In this way, it is not as important to keep the password file out of reach of other users as if it was unencrypted, but naturally it is good to keep it well protected anyway.

Salting

- There is always a possibility that two users select the same password. If Aapo and Bertil, for example, both select the password 'aprilsfool' and Bertil has access to the password file, he will notice that Aapo has the same password.
- Unix solves this problem by expanding the password with so-called salt.
- Salt is a 12-bit number created from the system time and process ID. This will most likely make it unique for each user.
- The salt is added to the user's password when selecting it. If Bertil's password is pw, the system will enter $E(pw + salt_B)$ into the password file, i.e. the original password with the salt added, and then it will be encrypted.
- The salt is also stored with Bertil's username and encrypted password.

- It is very laborious or practically impossible to decrypt a good encryption.
- An attacker may also find out the password directly. People often write down their passwords on a memo that is left near the computer.
- The password may also be shared among the members of a group, which may pose a risk.
- Furthermore, it is possible that an attacker poses as a manager or IT-department worker and asks for the password under some pretence.

Selecting passwords

In order to counteract the attempts described above, it is recommended that users take the following into consideration when selecting their passwords:

- Use other characters in addition to the letters A-Z.
- Select long passwords. The combinatory explosion starts after the password exceeds 5-6 characters.
- Avoid real names and words.
- Select an unlikely password. Develop your own mnemonic rule to remember the password.
- Change passwords regularly. This will counteract long-term, systematic password-cracking attempts.
- Do not write down your password. This rule is gradually losing its tenability, though, since the number of passwords is increasing to the point where some kind of bookkeeping is necessary, but store your passwords carefully.
- Do not tell anyone else your password.

Regulating information security I

- In most western countries, a parallel has been drawn between cryptographic products and arms, and strict export regulations have been in place.
- This has given rise to some perplexity, since it is fairly easy to implement strong, well-known encryption methods.
- The international Wassenaar arrangement covers dual-use items, i.e. products for both military and civilian end users.
- The Wassenaar arrangement replaced the COCOM regulations (discontinued in 1994).
- At the end of 1998, 33 major industrial countries - Finland among them - agreed on joint export control under the Wassenaar arrangement. Let us emphasize that the Wassenaar export list was not an export ban, but a control list requiring licensing.

Regulating information security II

- At the moment, Finnish legislation contains export control legislation consisting of the EU council regulation (EC) 1334/2000 and complementary Finnish legislation (the act on export control of dual-use items 562/1996 and the Council of State regulation 924/2000).
- In Finland, the unit for export control at the trade policy department of the Ministry for Foreign Affairs is in charge of the export control of dual-use items.
- It is also the licensing body for export of dual-use items (except the products in category 0 of appendix I of the EU council regulations, nuclear-specific items. Their export control is based on the nuclear power legislation and the licensing body is the Ministry of Trade and Industry and/or the Radiation and Nuclear Safety Authority STUK).

Regulating information security III

- Appendix I of the EU regulation (a list of dual-use items and technologies) is available on the website of the Ministry for Foreign Affairs at

  http://formin.finland.fi/palvelut/kauppa/vientivalvonta (in Finnish)

  under 'Vientivalvonnan alaisuuden selvittäminen.'
- Information protection, including encryption products, are listed in part 2, group 5.
- All items that are under export control are listed under 'Tuotehakemisto.'
- There is also a list of controlled items, software and technology on the EU's website

  http://ue.eu.int/pesc/ExportCTRL/fi/index.html
  http://ue.eu.int/pesc/ExportCTRL/en/index.html

Regulating information security IV

under 'Security-related export controls.'

- The Ministry of Foreign Affairs has also published a handbook in two parts, Vientivalvonta I and II (3/2004). It is available at the Edita bookstore, Annankatu 44, or the Edita Netmarket at www.edita.fi.

The EU regulation

Appendix I of the EU regulation is a combination of the following product lists of international export-control arrangements:

- The Wassenaar Arrangement (WA): http://www.wassenaar.org/
- The Australia Group (AG): http://www.australiagroup.net/
- The Missile Technology Control Regime MTCR: http://www.mtcr.info/
- The Nuclear Suppliers Group (NSG): http://www.nuclearsuppliersgroup.org

To mention one detail, the export of symmetric encryption items to third countries is allowed only if the key is under 56 bits long. It is fairly easy to crack such encryption with massive enough equipment.

Patents

- Information-security items, especially different encryption algorithms, are patented. Most products have been patented at the end of the 1970s or early 80s, so some patents have expired or are about to expire.
- US patents are valid for 17 years from the date of patenting and 20 years from being submitted to the patent office.
- The first important patent to expire is the Diffie-Hellman method for key agreement, which expired on 29 April 1997. S/MIME, for example, was quick to exploit this opportunity.
- The public-key encryption method RSA expired on 20 September 2000.
- The licensing policy of the Canadian Certicom company (over 130 patents) is efficiently blocking the dissemination of public-key methods based on elliptic curves.

Legislation on information security in Finland I

There is legislation on information security incorporated into many acts in Finnish legislation. They are listed below:

- The Constitution of Finland, basic rights and liberties (731/1999)
- The Personal Data Act (523/1999)
- The Act on the Openness of Government Activities (621/1999)
- The act on electronic transactions in administration (12/2003, only in Finnish/Swedish)
- The Act on Electronic Signatures (14/2003)
- The Act on the Protection of Privacy in Working Life (759/2004)
- The regulation for the Council of State (262/2003, only in Finnish/Swedish)
- The archiving act (831/1994, only in Finnish/Swedish)
- The State Budget Decree (1243/1992)

Legislation on information security in Finland II

- The act on identification cards (829/1999, only in F/S)
- Amendment of population register act (527/1999, only in F/S)
- The Communications Market Act (393/2003)
- The act on civil servants (750/1994, only in F/S)
- The penal code and act on amendment of the penal code (769/1990, 578(1995, 951/1999, only in F/S)
- The Emergency Powers Act (1080/1991)
- The act on the planning committee for defence financing (238/1960, only in F/S)
- The act on securing maintenance and supplies (1390/1992, only in F/S)
- The Coercive Measures Act (450/1987, 403/1995, 1026/1995, 22/2001)
- The Act on Background Checks (177/2992)

Legislation on information security in Finland III

- The Act on the Protection of Privacy in Electronic Communications (516/2004)
- The act on international information-security obligations (588/2004)

Key legislation I

The penal code and the coercive measures act contains legislation that most affects information security.

The penal code:

- Chapter 38, Section 3, message interception
- Chapter 38, Section 4, aggravated message interception
- Chapter 38, Section 5-7, interference in data communications
- Chapter 38, Section 8, computer break-in
- Chapter 35, Section 1.2, criminal damage
- Chapter 34, Section 9a, criminal computer mischief
- Chapter 28, Section 7, unauthorised use
- Chapter 28, Section 8, aggravated unauthorised use

The Coercive Measures Act:

Key legislation II

- information rights of police authorities
- Section 2, prerequisites for communications tapping (listening in/recording messages in secret to find out the contents of the message)
- section 3, prerequisites for communications surveillance (extracting secret identification data from messages)

In addition, copyright legislation also covers software products.

Authorities I

The key authorities when it comes to information security are

- The Parliament
- The Prime Minister's Office
- The Ministry for Trade and Industry
- The Ministry of Finance
- The Ministry of Transport and Communications
- The National Archives Services
- The Ministry of Justice
- The National Emergency Supply Agency
- The Ministry of Defence
- The National Bureau of Investigation
- The Ministry of the Interior
- The Data Protection Board

Authorities II

- The Ministry of Labour
- The National Audit Office of Finland
- The Ministry for Foreign Affairs
- The Communications Regulatory Authority

Directions for information security in Finland I

- The Ministry of Finance publishes a set of directives for information security, VAHTI, which is constantly updated. The directions are supposed to cover all areas.
- The Ministry has given civil service organisations directives for over 20 years and the procedures have been intensified since 1999.
- The directions contain good information on security routines and checklists. The directives are widely used outside the civil service, as well; city councils, companies, organizations, and international cooperation.

At the moment, the VAHTI series contains about 30 extensive directives. You can read them at the following URLs:

- www.vm.fi/vahti
- www.finansministeriet.fi/datasakerhet
- www.financeministry.fi/security

Directions for information security in Finland II

The newest VAHTI directives are

- Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 Management of abnormal information-security situations, VAHTI 3/2005
- Sähköpostien käsittely, VAHTI 2/2005 Handling e-mail, VAHTI 2/2005
- Information security and management by results, VAHTI 1/2005
- Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004
  Ensuring the security of key information systems in government administration, VAHTI 5/2004
- Datasäkerhet och resultatstyrning, VAHTI 4/2004
  Information security and management by results, VAHTI 4/2004
- Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
  General instructions for protection against malware, VAHTI 3/2004

Directions for information security in Finland III

- VAHTI tietoturva-CD, toukokuu 2004
  VAHTI information-security CD, May 2004
- Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
  Information security and management by results, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma, VAHTI 1/2004
  Development plan for government administration information security, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
  Instructions on risk evaluation to promote information security in government administration, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
  Instructions on arranging information-security education in the civil service, VAHTI 6/2003

Directions for information security in Finland IV

- Käyttäjän tietoturvaohje, VAHTI 5/2003
  Users' information security instructions, VAHTI 5/2003

Lately, the Ministry for Trade and Industry has also actively promoted information security.

To name one example, the LUOTI project is aimed at developing a set of directives on trust and information security in companies and corporate cooperation.

One of the main goals is the security of digital television. A pool of experts is also in the works, where companies can gain information about information security issues.