v. 0.4

EVASERVE

Module:
(Evaluation of Information Service)
Information Security

http://www.evaserve.fi

Revision history

Version	Date	Author	Comments
0.1	8.6.2005	Arto Laikari	First draft. Outline of module.
0.2	30.6.2006	Jani Suomalainen	Evaluation process structure revised. Text added
0.3	21.9.2006	Jani Suomalainen	Small insertions
0.4	27.11.2006	Jani Suomalainen	Small insertions
0.5	7.2.2007	Jani Suomalainen	Small alterations

# Contents

1 Introduction

The operational safety and access control of information services require the use of strict information security mechanisms and design and implementation observing the information security threats of the entire system. This evaluation module presents and lists the best practises and methods used in evaluating the adequacy and quality of the information security of an information service project, system or service. The document approaches the different information security evaluation components by presenting alternative methods, standards and required directives. The document also tries to show the know-how and references of VTT. The evaluation methods can be used in evaluating all kinds of information systems and telematics projects.

2 Evaluation process

There are different starting points to information security evaluations. The evaluation can be made at the design, implementation or usage phases of a project. The ideal situation is to observe information security already at the design stage of a project so that it supports the implementation and use of the project. Introduction of information security upgrades to a system already in use is usually harder. The scale and depth of the evaluation depend on the available resources.

VTT has taken part in several information security instrument and product information security development and evaluation projects. VTT has also invested in the analyses of information security assemblies by studying the methods and practises of measuring information security. An example is the VTT study [1] of the measurement and evaluation processes of information security commonly used in Finland by the industry and public sectors. VTT has also tried to define the evaluation process of information security aggregates from the information security argument acquisition viewpoint [2].

The evaluation processes of information service information security can be studied according to the method shown in Figure 1. Information security analyses start with defining the protected resources, identifying the threats to them and priorisation of the essential threats through risk analyses. This is followed by defining the threats into information security requirements whose realisation often requires the use of technical protection methods and support of administrative processes. The requirements and realisation can both be evaluated using the existing evaluation standards directing the best practises by offering evaluation frameworks and check lists. The realisations can also be checked for typical design and implementation flaws using different analyse methods and tools. The Figure also shows the relation of the information security evaluation module to other evaluation modules shown as green boxes.
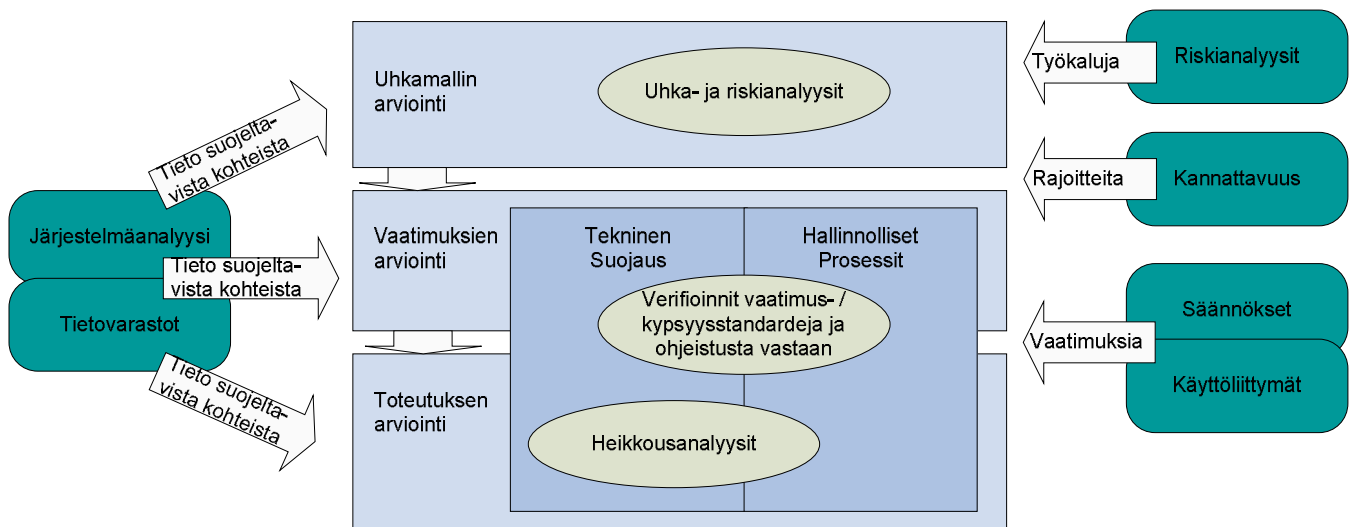
Figure 1. Information security evaluation components and connections to other modules

The high level tasks of the evaluation process have been shown by phase in Table 1. The process is not totally linear but one come back to previous phases if required.

Table 1. Evaluation process tasks

Task name	Task description
1 Identifying and defining information security critical resources and parts	Acquisition of data of the protected resources and architecture for evaluating threat model and implementation
1.1 Definition of information technology architecture	Studying and outlining the system architecture describing the components, users, actors, data transfer and system functionality
1.2 Definition of evaluation scope and design	Defining the scope and accuracy of the evaluation. (Includes definition of the evaluated components if the entire system is not evaluated). A requirement definition for the evaluation is made and, based on this, an evaluation plan
2 Evaluation of threat model	
2.1 Threat analyses	Identifying the information security threats to the system
2.2 Risk analyses	Evaluating the probability of threat realisation and consequences. Based on this choosing the threats to prevent
3 Evaluation of requirements and implementation	
3.1 Comparing requirements to prevented threats	Checking that the essential threats have been registered into the system as information security requirements
3.2 Comparing requirements to technical and administrative directives	Comparing the information security requirements to literary reference requirement lists
3.3 Comparing implementation to system requirement definitions	Comparing technical implementation and administrative processes to the information security requirements of the system
3.4 Comparing implementation to technical and administrative directives	Comparing technical implementation and administrative processes to general and approved reference practises.

3.5 Weakness analyses	Evaluation of components chosen in the evaluation plan using chosen methods and tools
4 Summary and reporting	Compiling an evaluation report based on the material

3 Identifying and defining information security critical assets and components

The evaluation of information security requires understanding the functionality, total architecture and threats of the system. At the first phase it is essential for information security to recognise the assets and define the scope and depth of the evaluation.

The functionality and architecture of the information system with the descriptions of components, users, roles, actors, data transmissions, interfaces and data flows is studied. The information can be gathered in different ways i.e. questionnaires, interviews, system schematics documents and possibly technical tools. The analyses based on the **System analyses** and **Databases modules** can be used if needed.

The target of the evaluation can be a project, system, design, implementation or use. In some cases the aim may be to develop the entire work method of the organisation while in some cases the evaluation is concentrated only on questions about technical or a single programme or threats from a certain source. The tasks suitable for the situation can be chosen from the presented method and practise areas.

4 Information security threats and risk analyses

The challenge of threat analyses is comprehensive identifying of threats from all existing threats. The definition of threats is based on the understanding of both the evaluated system and the typical information security threats. Workshops are often used in the search for threats. These meetings are attended both by the developers familiar with the product and often responsible also for information security realisation, and by information security evaluators controlling the meeting. The participation of developers in threat definition binds them and increases the probability that perceived problems are actually solved. The threat definition process involving developers can consist of the following tasks [3]:

1. Description of product data flows by the developers enables forward preparation
2. At the workshop the developers identify threats under information security expert control
3. Compilation of threat document
4. Threat document verification meeting
5. Peer verification of threats
6. Corrective actions

The search for information security threats can utilise literary threat examples and most typical threat categories. Classification eases the understanding of the information security situation and helps the systematic search for essential threats and the selection of means of defence. Threat classification can be based on e.g.:

- The component of resource or system under attack or through which the attacks come

- The attack paradigm i.e. the way the invasion or damage is initiated. The attack directions can e.g. be divided into categories of malware, external users and internal users.
- Attack consequences, for example the CIA model (confidentiality, integrity, availability) which is a widely used classification method spanning a large part of threats and whioch can be used as a base for defensive method requirements. Another example of the model based on attack consequences is the STRIDE [4] model of Table 2.

Table 2. STRIDE [4] model for threat classification

Threat category	Description
Spoofing	The attacker can access the system by using a false identity e.g. stolen or false information.
Tampering	Unauthorised conversion of data can occur either during transfer or while saved
Repudiation	Actions and transactions can be disputed if they do not leave a reliable trace.
Information disclosure	Information disclosure means e.g. unauthorised use of data or unauthorised copying and distribution of data.
Denial of service	Denial of service attacks can occur on the infrastructure, device or application level. E.g. bombarding the server with requests or non-standard messages are possible ways of attacking service availability.
Elevation of privilege	Elevation of privilege attacks are used to gain rights required to implement other attacks.

It is not necessary to block all detected threats. The realisation of defensive measures must also consider the investments used in the defence and the probabilities and impacts of threat occurrence.

Risk analyses studies the probabilities and costs of threat occurrence. The methods used in the risk analyses are discussed more generally in the *risk analyses module*. The management of information security specific risks is discussed in e.g. the **NIST 800-30** [5] directive. The document deals with threat identification methods, risk management and risk prevention methods on a general level. NIST has also produced other guides on best practises in information security [6].

In the field of information security the usual way of analysing risks is to use attack trees [7]. Attack trees enable the illustration and graphical documentation of the different phases of an attack and their relations. Possible problems are the attack trees delusions of a formal charting of all threats and tediousness.

VTT projects connected to the analyses, management and reduction of information security risks are e.g. IRRIIS (IST/Integrated Risk Reduction of Information-based Infrastructure Systems), SHOPS (EUREKA/Smart Home Payment Systems) and ANSO (ITEA/Autonomic Networks for SOHO users). The first one analyses risks against energy distribution and telecommunication networks, the second one risks connected to payment systems and the third the information security threats of heterogenic home networks.

5 Evaluation of requirements and implementation

The evaluations of the information security requirements and implementation of information services is carried out by inspections and analyses of the design and implementation documents and code. The evaluations check that all identified and essential threats are observed both in the requirement definitions and in implementation. Evaluations can also utilise existing directives and reference check lists.

5.1 Technical protection evaluation

The evaluation of the reliability and strength of the information security of an information system depends on the components used so that the system is as strong as its least protected component. Information security is studied from the viewpoint of the implementation and function of the whole system but for evaluation purposes the information security of the entire system can be divided into smaller more manageable sub-components. Information security can e.g. be divided into five sub-systems [8]: auditing, integrity, use control, data flow control and identity control.

Suitable information security requirement definitions can be utilised in analysing single components. E.g. the **Common Criteria** (CC) standard [9] is commonly used in information security evaluation. CC is the framework for the definition of different information security requirements for single products and requirement profiles for product groups. Applying CC is, however, tedious which is why the standard has been mainly used in the evaluation of small information security critical products like smart cards. Information security profiles have, however, been defined also for e.g. firewalls and database programmes.

The most typical information security reliability instrument is the experience from extensive public review and use and the reputation of being a unbreakable and useable method or programme. This instrument is especially suited for evaluating rights management methods and encryption algorithms. . New untested solutions can be evaluated using other proof based on reputation [2]:
- Authors (e.g. programme provider) work practises
- Reputation of other work from author
- Use of quality and information security standards
- External reviews of authors and reviewer reputation

Other examples of reviewer instruments are:
- Usability impacts can be evaluated by calculating the number of required user interactions. User studies can also be used to establish the number and frequency of user actions possibly leading to information security weaknesses.
- The strength of encryption algorithms can be evaluated using mathematical complexity theories. Thus only the uncrackable methods or methods which can be cracked with unrealistic resources can be classified as safe.
- The number of used methods against the same threat measures in certain cases the strength of the system against single weaknesses. The threat of a single information security hole being used to crack the entire system can be decreased by several overlapping information security methods. Practically all single information security methods can be evaded or cracked with enough resources. The use of several methods can therefore increase the resources required by the attacker.
- Availability protection can be evaluated by e.g. the number of methods increasing error tolerance e.g. redundancy.

5.2   Weakness analyses

Many application information security weaknesses are only revealed through use. Products, technologies and practises used for several years are the most tested ones and many of their weaknesses have been eliminated. Weaknesses can, however, also be seeked out using different testing and code analysing methods.

The testing of practical strength of information security can also involve the use of experienced testing and data breach experts – hacker teams. These testers try different known attacks with varying parameters in order to find weaknesses that can be exploited by also the real attackers. There are tools available for the testing of information security of single products, especially net applications, which automate attacks. E.g. VTT has participated in the development of the Protos [10]. the tool generates a great number of messages of different form which can be used in revealing weaknesses in web servers.

Programme errors are an important single reason for information security problems. Potential errors can be searched by going through the programme code either using programme investigations or using static or dynamic analysis tools. The problem of automatic tools is their inaccuracy and evaluation of information security by searching for programme errors is tedious. Programme operation can also be verified using formal methods which try to prove mathematically the flawless operation of the programme. The formal modelling of programmes is, however, tedious and the methods are unsuitable for the reliability evaluation of complex programmes.

5.3   Safety process evaluation

In addition to individual technical solutions the information security of services consists of administrative activities such as directives, training, monitoring CERT and manufacturer vulnerability bulletins, software updates and activities at the materialisation of threats. There are standards for total information security and the compatibility of the parts with the system can be evaluated.

The **ISO 17799** (BS 7799) standard [11] defines the directive for the management of total information security. The standard consists of ten sub-areas:

1. Security policy
2. Security organization
3. Assets classification and control
4. Personnel security
5. Physical and environmental security
6. Computer and network management
7. System access control
8. Systems development and maintenance
9. Business continuity planning
10. Compliance

Other information security management evaluation standards are:
- SSE-CMM (Systems Security Engineering Capability Maturity Model, ISO/IEC 21827) [12] standard defines and specifies the evaluation of information security process maturity.
- INFOSEC IA-CMM
- IS Program Maturity Grid
- Murine-Carpenter SW Security Metrics

VTT has developed and small and medium sized companies use an evaluation method – the "**ketterä"** information security management system development method [13]. The method is a ISO 17799 compatible way to develop the information security processes of a company. The method consists of the following phases: meeting with the management, information security policy, strategic safety (personnel and physical safety), operative safety, continuity planning, directives, training and measurements. The method has been used in connection with e.g. the EUREKA/SHOPS project.

6   Reporting

The evaluation results can be presented as a written report. The report presents the evaluated parts of the information service, evaluation phases and the methods and standards used. The results can include the identified weaknesses and deviations from the generally accepted practises and residual risks i.e. the impacts and probabilities of un-prevented threats. The report can also list and recommend corrective actions.

References

1   Jorma Kajava, Reijo Savola. Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes. The European University Information Systems Conference (EUNIS). 2005.

2   Reijo Savola, Juha Röning. Towards Security Evaluation based on Evidence Information Collection and Impact Analysis. The International Conference on Dependable Systems and Networks (DSN-2006). 2006.

3   Peter Torr. High-Level Threat Modelling Process. Microsoft. blogs.msdn.com/ptorr/archive/2005/02/08/368881.aspx

4   J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, Anandha Murukan. Improving Web Application Security: Threats and Countermeasures. Microsoft. 2003. msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh02.asp

5   Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. Special Publication 800-30. 2002. csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

6   NIST Computer Security Special Publications. National Institute of Standards and Technology. csrc.nist.gov/publications/nistpubs/index.html

7   Bruce Schneier. Modeling Security Threats: Attack Trees. Dr. Dobb's Journal. 1999. www.schneier.com/paper-attacktrees-ddj-ft.html

8   J.J. Whitmore. A method for designing secure solutions. IBM Systems Journal, vol 40, no 3, 2001.

9   Common Criteria. www.commoncriteriaportal.org

10 Rauli Kaksonen. A functional method for assessing protocol. Implementation security. VTT Technical Research Centre of Finland. VTT Publications : 448. 2001. www.vtt.fi/vtt_show_record.jsp?target=julk&form=sdefe&search=42220.

11 International Organization for Standardization. ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management. www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.

12 SSE-CMM home page. www.sse-cmm.org/index.html.

13 Jarkko Holappa, Timo Wiander. PK-Yrityksen Tietoturvakehikko. Ketterä tietoturvan hallintajärjestelmän kehitysmenetelmä. 2006.