

Towards Trustworthy ERMS ONERA-CERT

Gérard Eizenberg
Gerard.Eizenberg@cert.fr

Plan

- Experience in Information Technology Security
- From Risk Analysis to a Security Target
- How to reach trustworthy **ERMS**
- Possible Security Assistance

Information technology security

- **Confidentiality**
Prevention of the unauthorised disclosure of information
- **Integrity**
prevention of the unauthorised modification of information
- **Availability**
prevention of the unauthorised withholding of information or resources

(source ITSEC = Information Technology Security Evaluation Criteria)

Sometimes added: **Accountability**

ONERA experience in information technology security

- Formal Expression of rules, of rights, of rights on rights (e.g. delegation), of specifications, of secure system behaviour
 - example :
 - formal statements of parts of Defense regulations
 - information flow models (for multilevel security)
- Design and architecture of secure systems and applications
 - Goal : correctness / specifications
 - example :
 - multilevel secure LAN
 - secure Object Oriented Databases
- Security verification
 - example :
 - cryptographic protocols prover
 - security verification of the COPICAT design (ESPRIT Project)

in contexts where malicious actions must be considered

From risk analysis to a security target

All risk analysis methods include : Assets, threats, vulnerabilities, risks

Threat = adverse event that could affect the system

Vulnerability = likelihood of damage resulting from the occurrence of a threat

Risk = combination of threat and vulnerability

From:

- a "security environment" including laws, contracts, organisational security policies, customs, ...
- technical and economical constraints
- threat or risk analysis

one derives a "security target"

From risk analysis to a security target: examples of threats

GENERAL THREATS

- Unauthorised acquisition of an image (resp. image bank, thesaurus)
NB: unauthorised acquisition by any means: disclosure, copy, repudiation
- Unauthorised modification of an image, of a credit account
- Unauthorised distribution of images without mention of the origin
- Unauthorised disclosure of private usages (Privacy)

DETAILED THREATS

- A user gain the unauthorised ability to assume the identity of another user
- A user modifies the use-rights to make possible unauthorised access ...
- A user destroys an audit trail

From risk analysis to a security target: examples of vulnerabilities

The thief of an image bank will:

- use it for his/her pleasure
- make it accessible for his whole company
- include it in a pirate server located in a "Right protection paradise" and make it accessible on the web for free or business

Security target

- Threats
- Security objectives, including:
 - non-IT security objectives
 - IT security objectives
- Security requirements; security functions
- Required security mechanisms
- Rating of minimal strength of mechanisms
- Evaluation level

COMPOSE THE SECURITY TARGET

Security objectives

7 classes:

- Identification and Authentication
- User data protection
Access controls, Confinement, Watermarking
- Communication protection
 - Non repudiation of origin
 - Non repudiation of reception
- Security Audit
- ERMS Access
- Privacy
- Protection of the Trusted Security functions

Security objectives: details

- AU_1: The user activities shall be monitored and the security violations shall be deterred.
- CO_1: It shall be possible to have a proof of the identity of the originator (Non-Repudiation of Origin)
- CO_2: It shall be possible for the originator of a material to prove that he/she is the effective one.
- CO_3: It shall be possible to have a proof of the identity of the recipient of transmitted information (proof of receipt).
- DP_1: There shall not be unauthorised copies of protected materials.
- DP_2: There shall not be unauthorised observation of protected materials and of usage related information such as use right credits and charges, statistics, payment information and contracts.
- DP_3: There shall not be unauthorised alteration of protected materials, of the identifiers, of the use right credits and charges, of the contracts information and of the payment information (integrity).
- DP_4: All the accesses shall respect the ERMS Policy. In particular, it shall be possible to control the accesses on the base of the role played by the user.
- AC_1: Prior to identification and authentication, any user shall be warned of the ERMS Security Policy.
- AC_2: The ERMS shall display an advisory warning message to potential users pertaining to appropriate use. One banner shall state the ERMS Security Policy.
- IA_1: The identity of each user shall be established and it will be ensured that each user is indeed who he/she claims to be.
- P_1: The users' privacy needs shall be satisfied, while still allowing the system flexibility as far as possible to maintain sufficient control over the operation of the system.
- SF_1: Integrity shall be provided to the Security Functions mechanisms and data.
- SF_2: The adequation between the internal access rules and the ERMS security policy will be ensured

How to reach trustworthy ERMS

Problem: How to convince (or be convinced) that one ERMS enforces the claimed protection efficiently ?

Solutions:

- 1- Trust in the ERMS provider
- 2- Security evaluation

N.B. The Insurance solution comes back to the second one

Trust in the ERMS provider

- The cheapest solution

If a company entrusts the ERMS provided by another company, will its clients also entrust it ?

Security evaluation

In most cases, the customer will not perform it by itself

Need for an independent evaluation body

Need for standard evaluation criteria:

- in Europe: Information Technology Security Evaluation Criteria (June 1991)
- in North America: draft Federal Criteria (1993)
- Common Criteria current process:
 - Version 1.0 (January 1996)
 - Version 2.0 (end 1997, submitted to ISO SC27/WG3)
 - ISO standard (end 1999)

N.B. Consistency of C.C. with previous ones.

Security evaluation

The Common Criteria include the Protection Profile concept :

"A reusable and complete combination of Security Objectives, functional and assurance requirements with associated rationale"

Reasonable bet : ERMS Protection Profiles will be built in the future. It is worth to be in advance in that process.

A set of security requirements has already been selected by COPEARMS.

Possible security assistance from ONERA

- Simple risk analysis
- Selection of security objectives, security requirements, security functions, security assurances
- Audit of an existing design / security objectives and assurances
- Assistance in protection methods