Dependability and Security
Metrics and Evaluation

Presented by

Erland Jonsson
Department of Computer Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

WHY MODELLING? - WHY METRICS?

Quotations:

- "Modelling is fundamental to measurement; without an empirical model or describing observations, measurement is not possible" (A. Kaposi 1991)
- "The history of science has been, in good part, the story of quantification of initially qualitative concepts" (Bunge 1967)

WHY MODELLING? - WHY METRICS?

Quotations:

- "....if you can measure what you are speaking about and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge of it is at best meagre and unsatisfactory." (Lord Kelvin)
- "It is good engineering practice to be able to verify claimed performance" (Jonsson 2010)

METHODS FOR "MEASUREMENT" OF SECURITY

- **Risk analysis:**
  - *estimation* of the probability for specific intrusions and their consequences and costs. Trade-off towards the corresponding costs for protection.
- **Evaluation/Certification:**
  - *classification* of the system in classes based on design charactersitcs and security mechanisms. "The 'better' the design is, the more secure the system"
- **Operational Metrics (based on the intrusion process):**
  - a statistical metric of system security based on *the effort* it takes to make an intrusion. "The harder to make an intrusion, the more secure the system"

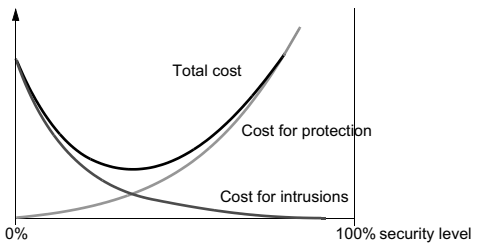
RISK ANALYSIS - BASIC METHODOLOGY

Basic methodology for risk analysis:

1. Identify **assets**
2. Determine **vulnerabilites**
3. Estimate **likelihood of exploitation**
4. Compute expected annual "**loss"** (due to intrusions)
5. Survey applicable **methods of protection** and their costs
6. Project annual savings (make **trade-off**)

RISK ANALYSIS - COST TRADE-OFF

Make a trade-off between costs!



SECURITY POLICY and SECURITY PLAN

- A **security policy** states:
  - the organization's goals regarding security, i.e., which *assets* must be protected against which *threats*
  - where the *responsibility* for security lies
  - the organization's *commitment* (e.g., money, personnel)
- Make a **security plan!** It defines how the company addresses its security needs. It covers the following items:
  - security policy (~ definition of the goal)
  - current state
  - recommendations (~ how goals can be accomplished)
  - accountability (who is responsible for carrying out the plan)
  - time schedule
  - continuing attention (specifies periodic reviews)

CERTIFICATION ACCORDING TO A SECURITY STANDARD

- **Evaluation** is assessing whether a product has the *security properties* claimed for it
- **Certification** is the formal assessment of the result of an *evaluation.*
- **Accreditation** is deciding that a (certified) product *may be used* in a given application
- Certification is made wrt to some established standard, such as the CC ("Common Criteria").
- The goal of the certification:
  - assess the trust of the system's correctness. (How secure is it?)
  - assess the quality of the evaluation. (How do we know?)

  Document it!!

METHODS FOR CERTIFICATION

There are (at least) three fundamentally different methods of certifcation.

1. **Penetration analysis:**
   A "Tiger Teams", i.e. a group of very skilled specialists tries to "crack" the system to find "all" vulnerabilties.
2. **Informal validation:**
   Testing and checking the system. Includes e.g.:
   - requirements checking
   - design and code reviews
   - software module and system testing
3. **Formal verification:**
   The operating system is reduced to a mathematical "theorem", which is proven.

EVALUATION STANDARDS

Earlier evaluation criteria:

- TCSEC (Trusted Computer Security Evaluation Criteria)
- ITSEC (Information Technology Security Evaluation Criteria)
- FC (Federal Criteria)
- Canadian, Japanese, etc

Evaluation criteria on the module level:

- In some cases we need to evaluate a specific security module. The FIPS 140-2 is an evaluation standard for cryptographic modules.
- It provides four increasing, qualitative security levels.

COMMON CRITERIA

- The Common Criteria[1] (CC) is aimed to be common to all countries. It defines a security evaluation methodology.
- It became the "official" evaluation standard in the USA in 1998. (TCSEC was discontinued in 2000.)

Central terms:

- Target of Evaluation (TOE):
  An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
- Evaluation Assurance Level (EAL):
  A package consisting of assurance components that represent a point in the predefined assurance scale

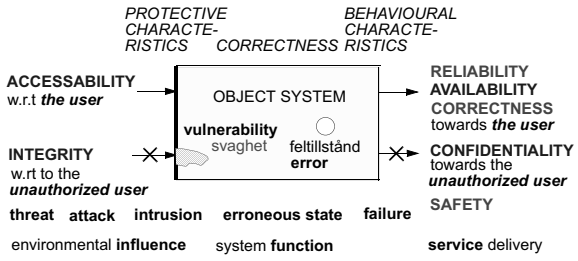
1. Common Criteria for Information Technology Security Evaluation

COMMON CRITERIA

Central terms (cont'd):

- Protection Profile (PP):
  An implementation-independent set of security requirements for a category of TOEs
- Security Target (ST):
  A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
- Security Functional Requirements (SFR):
  The translation of the security objectives for the TOE.
- TOE Security Function (TSF):
  A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the SFR. (cp Trusted Computing Base)

DEPENDABILITY ATTRIBUTES vs OBJECT SYSTEM



BEHAVIOURAL METRIC

Behavioural metrics are well-known (except for confidentiaity):

- A **behavioural metric** describes to what extent the system delivers its service to its User(s) or denies service to its Non-user(s).

☞ Thus, **reliability, safety** and **confidentiality** could be covered by the same (vectorized) **metric** using Markov modelling

PROTECTIVE METRICS

Protective metrics could be based on studies of the system in operation, e.g. the intrusion process:

- A **protective metric** describes the **ability of a system to resist attacks** during operation, i.e., to prevent faults from entering into the system, thus creating an error in the system.
- A deliberate intrusion or a security breach could normally be regarded as a fault

☞ Hypothesis:
A system is more secure the more **effort** it takes to make an intrusion into the system

METRICS OF CORRECTNESS

Metrics of correctness:

- Measuring correctness is very hard
- Not only are there huge practical problems, but it is also a matter of lack of fundamental definitions

☞ Thus, I know of no methods for measuring correctness

CONCLUSIONS (general):

- The areas of Dependability and Security have traditionally evolved separately and there is a lack of coordination between them regarding concepts, terms, tools etc
- Dependability and Security reflect two different approaches to the same fundamental research area
- Dependability and Security must be integrated into one common context in order for us to be able to properly address the problems involved

CONCLUSIONS (specific):

- We have suggested an ***integrated system model*** for Dependability and Security, describing the system in terms of ***correctness*** as well as ***protective*** and ***behavioural characteristics***
- Dependability and Security metrics can be defined in accordance
- Protection methods and mechanisms have been related to the system model
- Intrusion detection is a mechanisms that introduces the “product-in-a-process” concept for the system