Security and dependability metrics

Erland Jonsson

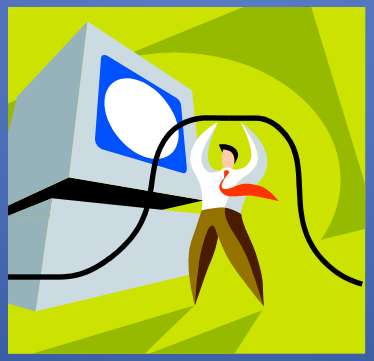
Department of
Computer Science and Engineering
Chalmers University of Technology

150215

CONTENTS

- Motivation
- What is measurement
- Measurement scales
- Existing methods for “measuring” security
- Metrics for dependability/security attributes
  - Protective metrics
  - Behavioural metrics
- Conclusions

MOTIVATION



Motivation

- Security is a major concern in computer-based systems, i.e. virtually ***all*** systems of today.
- It is good engineering practice to be able to verify/validate claimed performance. Obviously, this includes security performance.
- A number of standard bodies (e.g. ANSI 2008) require risk analysis (being one type of metric)
- Financial regulations (e.g. "Operational Risk" in Basel-III) also require precise risk management for technology

Why metrics?

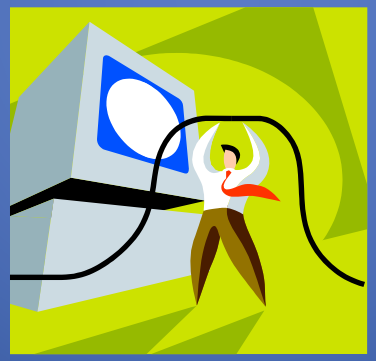
- Quotation 1:
  - "…if you can measure what you are speaking about and express it in numbers you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge of it is of meagre and unsatisfactory kind"
    (Lord Kelvin ~1870)

Why metrics?

Quotation 2:

– “The history of science has been, in good part, the story of quantification of initially qualitative concepts” (Bunge 1967)

WHAT IS MEASUREMENT?



Definition of measurement

- **Definition:**
  - Measurement[1] is the process of empirical, objective encoding of some property of a selected class of entities in a formal system of symbols (A. Kaposi based on Finkelstein)
  - Cp Metrology is the field of knowledge concerned with measurement. Metrology can be split up into theoretical, methodology, technology and legal aspects.

1. We use the terms measurement and metrication interchangeably, as well as measure and metric.

General requirements on measurement operations

- Operations of measurement involve collecting and recording data from observation
- It means identifying the class of entities to which the measurement relates
- Measurements must be independent of the views and preferences of the measurerer
- Measurements must not be corrupted by an incidental, unrecorded circumstance, which might influence the outcome

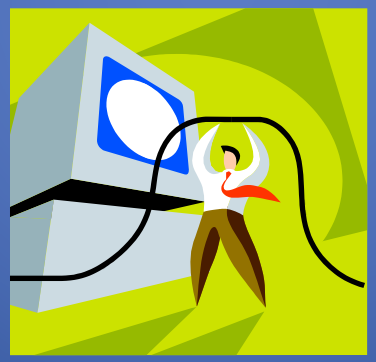
Specific requirements on measurement operations

- Measurement must be able to characterize abstract entities as well as to describe properties of real-world objects
- The result of measurement may be captured in terms of any well-defined formal system, i.e. not necessarily involving numbers

Meaningfulness

- Meaningfulness means that the scale measurement should be appropriate to the type of property measured, such that once measurement has been performed – and data expressed on some scale - sensible conclusions can be drawn from it
- Example 1: Point A is twice as far as point B (meaningless, since distance is a ratio scale, but position is not)
- Example 2: Point A is twice as far from point X as point B (is meaningful)

MEASUREMENT SCALES



Measurement scales

- Mesurement theory distinguishes five types of scales:
  - nominal scale
  - ordinal scale
  - interval scale
  - ratio scale
  - absolute scale
- Here they are given in an ascending order of ”strength”, in the sense that each is permitting less freedom of choice and imposing stricter conditions than the previous one

Measurement scales II

- The nominal scale can be used to denote membership of a class for purposes such as labelling or colour matching
- The ordinal scale is used when measurement expresses comparitive judgement
- The interval scale is used when measuring ”distance” between pairs of items of a class according to the chosen attribute
- The ratio scale denotes the degree in relation to a standard, i.e. a ratio. It must preserve the origin.
- The absolute scale used for counting the number of elements in an entity set

Nominal scale

- The nominal scale can be used to denote membership of a class for purposes such as labelling or colour matching
- There are no operations between E and F
- The only relation is equivalence
- One-to-one mapping

Ordinal scale

- The ordinal scale is used when measurement expresses comparitive judgement
- The scale is preserved under any montonic, transformation:

$$x >= y \Leftrightarrow \phi(x) >= \phi(y),$$

  where ϕ is an admissible transformation
- Used for grading goods or rating candidates

Interval scale

- The interval scale is used when measuring ”distance” between pairs of items of a class according to the chosen attribute
- The scale is preserved under positive linear transformation:

$$\phi(x) = \alpha m + \beta, \text{ where } \alpha > 0$$

- Used for measuring e.g. temperature in centigrade or Fahrenheit (but not Kelvin) or calendar time

Ratio scale

- The ratio scale denotes the degree in relation to a standard. It must preserve the origin.
- It is the most frequently used scale
- The scale is preserved under the transformation:

$$\phi(x) = \alpha m \text{ , where } \alpha > 0$$

- Used for measuring e.g. mass, length, elapsed time and temperature in Kelvin

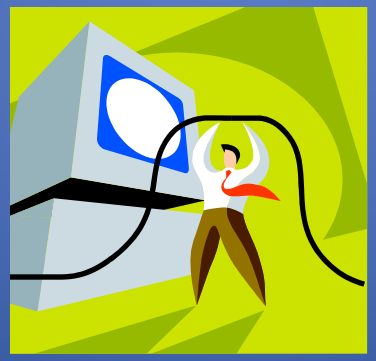
Absolute scale

- The absolute scale is a ratio scale which includes a ”standard” unit.
- The scale is only preserved under the identity transformation:

  $$\phi(x) = x,$$

  which means that it is not transformable
- Used for counting items of a class

EXISTING METHODS FOR MEASURING SECURITY



Which are the existing methods for measuring security?

- as of today, there are no scientifically solid metrics of security. Instead, there are a number of informal and/or subjective assessments or rankings.
- some of them are presented below. They represent different approaches to the metrication problem

Methods for ”measuring[1]” security I

- **Evaluation/Certification** (according to some standard):
  - *classification* of the system in classes based on design characteristics and security mechanisms.
  “The ‘better’ the design is, the more secure is the system”
- **Risk analysis**:
  - *estimation* of the probability for specific intrusions and their consequences and costs. Trade-off towards the corresponding costs for protection.
- **Penetration tests:**
  Finding vulnerabilities by using “Tiger teams”. (But you never find them all….)
- **Vulnerability assessment:**
  - includes methods for finding system vulnerabilities

1. In the sense ”making some kind of quantitative assessment”

Methods for ”measuring” security II

- **Effort-based approach** (based on “simulated” attacks):
  - 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”
- **Weakest adversary**:
  - which is the weakest adversary that can compromise the system?
- **MTTC** (Mean Time To Compromise):
  - calculates the statistical mean time to an intrusion

Methods for ”measuring” security III – special cases

- Cryptographic strength:

  - a statistical metric of the strength of a crypto system based on *the computational effort* for a successful cryptanalysis (FIPS 140-2[1]).
  “The harder to breach the crypto, the stronger it is”
  Cp: Effort-based approach

- Privacy measures:

  - defines to which extent the system will leak personal information

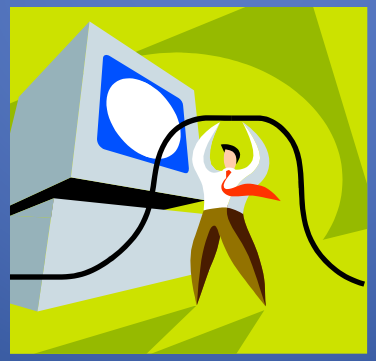
- Fault trees, Worst Case Analyses, ….

1. Federal Information Processing Standard - used to accredit cryptographic modules

Methods for ”measuring” security IV – standards, methods and tools

- ISO/IEC 27004: Information security management – Measurement- measures the effectiveness of Information Security Management System processes and controls
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):
  - is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. [CERT]
- OSSTMM (Open-Source Security Testing Methodology Manual):
  - is a document of security testing methodology and a set of rules and guidelines for which, what, and when events are tested [ISECOM]
- CVSS (Common Vulnerability Scoring System):
  - CVSS is an industry standard for assessing the severity of computer system security vulnerabilities

SUGGESTED FOR METRICS OF DEPENDABILITY /SECURITY ATTRIBUTES



Security Metrication Basic Methodology

1. Define the concept
2. Define suitable attributes for metrication
3. Select method for assessing the magnitude of these attributes
4. Select method for how to do this assessment in a practical way

Security Metrication Basic Methodology –

- example 1: encryption mechanism

1. Define the concept -> confidentaility
2. Define suitable attribute for metrication -> strength of encryption mechanisms
3. Select method for assessing the magnitude of this attribute -> based on design characteristics
4. Select a method for how to do this assessment in a practical way -> break attempts and evaluation of design

Security Metrication Basic Methodology –

- example 2: system security

(in some sense)

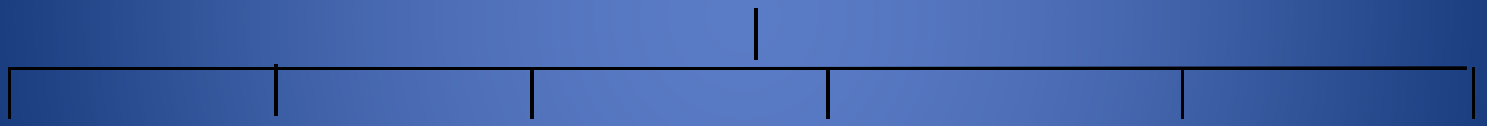
1. Define the concept -> ”system security”
2. Define suitable attribute for metrication
   -> the effort expended to make breaches
3. Select method for assessing the magnitude of this attribute
   -> based on controlled intrusion experiments
4. Select a method for how to do this assessment in a practical way -> use students to perform such an intrusion campaign and log activities

Security-Dependability Metrication

- It is suggested that security can be measured by means of measuring the different security attributes
- Since there is an overlap between the concepts of security and dependability, dependability attributes will also be included
- This method will not result in a metric of composite security, but only metrics of its attributes
- It is not obvious that the metrics for these attributes can be merged into an overall security metric. Rather, this is a matter of definition

INTEGRATED SECURITY and DEPENDABILITY ATTRIBUTES

BEHAVIOURAL DEPENDABILITY ATTRIBUTES



Reliability **Availability** Safety Maintainability **Confidentiality** **Integrity**

"other" attribute

protective attribute

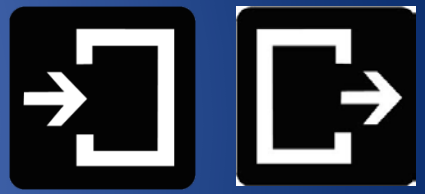
Security-Dependability Metrication

- As the security and dependability attributes are **divided** into two types:
  - protective
  - behavioural

  the corresponding metrics will be divided in the same way.
- You could also think of defining a metric for correctness
- Sometimes other aspects are proposed as sec-dep attributes, e.g. maintainabilty, authenticity and non-repudiation, etc

Black Box Approach

- Our approach is based upon system interaction with the **environment,** i.e. **input and output**



- Input: Environmental influence
  - ***Fault introduction***: malicious, external
- Output: **System behaviour**:
  - delivery of service, denial of service
  - USERs and NON-USERs

Two different Types of Metrics

- **Protective metrics** (INPUT)
  - embodies the notion of protection
  - most important characteristics of security (i.e. integrity)
  - status today: not much available

- **Behavioural metrics** (OUTPUT)
  - relates to system behaviour
  - dependent on protective security
  - status today: many metrics exist, at least for the service delivery
  - metrics (MTTF etc)

Protective Metrics

Protective metrics should quantify:

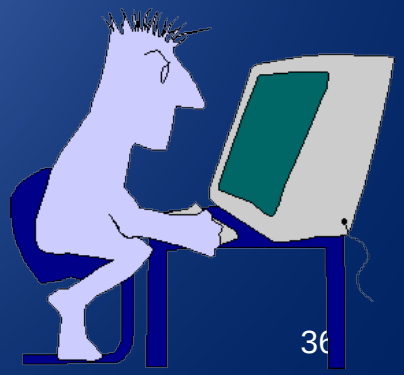
- the extent to which the system is able to protect itself against unwanted **external influence,** i.e. integrity

Two types of protective metrics (at least)

- *System-related (e.g. based on Protective Mechanisms)*
- *Threat agent-related (e.g. based on Attacker Effort)*

Protective Metrics (cont'd)

- ***System-related metrics***
  - measures the strength of the ***protection mechanisms***
  - combined strength of security mechanisms
  - However, no absolute guarantee of higher integrity with stronger mechanisms (as security is absence of vulnerabilities)
- ***Threat Agent-related metrics***
  - measures the ***effort expended*** by an attacker to make a breach into the system, i.e. to compromise integrity
  - effort could include factors such as time, skill level, attacker reward
  - the effort expended to make an intrusion is a metric of the security of the system
  - Mean Time To Intrusion (MTTI)



Behavioural Metrics

Behavioural metrics:

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

Such measures already exist, e.g. for:

- **Reliability:** MTTF
- **Availability:** MTTF/(MTTF+MTTR)
- **Safety:** MTTCF

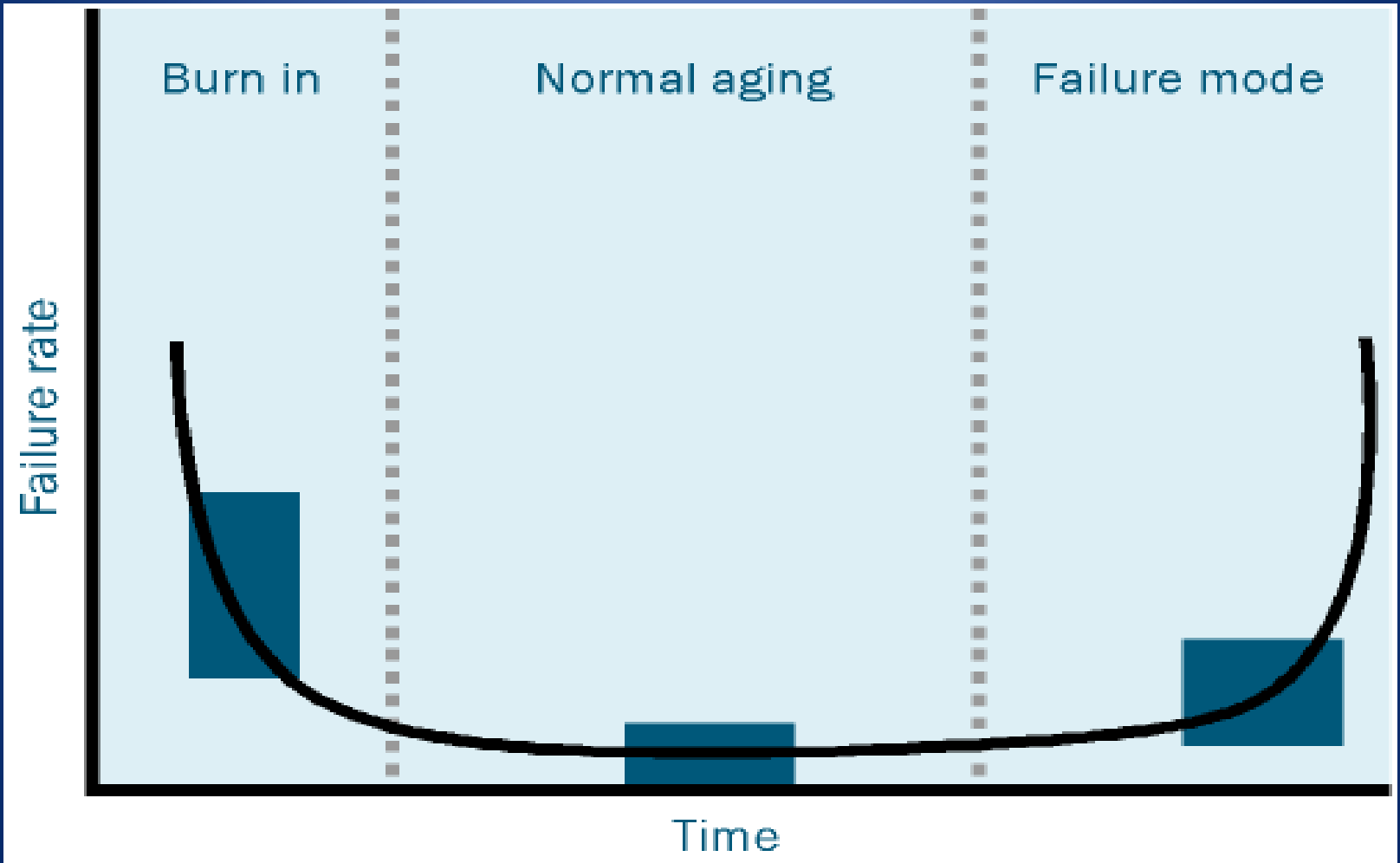
But less so for:

- **Confidentiality**
- **Exclusivity**

Metrics for Reliability

- RELIABILITY *("continuity of service")*
  - The reliability R(t) of a system SYS can be expressed as:
    R(t) = Prob (SYS is fully functioning in [0,t])
  - A metric for reliability R(t) is MTTF, Mean Time To Failure, normally expressed in hours
  - This metric is valid in the steady-state, i.e. when the system does not change or evolve

The Bathtub Curve



Metrics for Availability

- AVAILABILITY *("readiness for usage" - incorporates maintainability (repair))*
  - The availability A(t) of a system SYS can be expressed as:
    A(t) = Prob (SYS is fully functioning at time t)
  - A metric for the average, steady-state availability is A = MTTF/(MTTF+MTTR), where MTTR is the constant repair rate.
  - It is normally expressed in %.
  - A certain %-value may be more or less serious depending on the "failure distribution" ("burstiness")

Metrics for Safety

- SAFETY *("avoidance of catastrophic consequences")*
  - The Safety S(t) of a system SYS can be expressed as: *S(t) = Prob (SYS is fully functioning or has failed in a manner that does cause no harm in [0,t])*
  - Thus safety is reliability wrt malign failures
  - A metric for safety S(t) is MTTCF, the Mean Time To Catastriphic Failure, defined similarly to MTTF and normally expressed in hours.

Metrics of correctness

- metrics of correctness should give a value to what extent the system is “correct” in some sense
- such metrics could be especially relevant for databases
- metrics of correctness are not well defined (?), at least 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

Security metrics research –
- suggested areas

- NIST suggests the following security metrics research areas:
  - Formal models related to security metrics ("the absence of formal models has hampered progress")
  - Historical data collection and analysis
  - AI assessment techniques
  - Praticable concrete measurement methods
  - Intrinsically measurable components ("developing components that are inherently attuned to measurement")

Conclusions

- We have given a brief overview of available metrication methods and the state of research
- We have suggested that **security** (and dependability) is best measured by **measuring its non-functional attributes**
  - ***Protective metrics***
    - ***System-related metrics (protection mechanism-based)***
    - ***Threat-related metrics (effort-based)***
  - ***Behavioural metrics***
- **Integrity** is the essence of traditional **security**
- An overall security metric would be highly desirable