



Security Metrics

Erland Jonsson

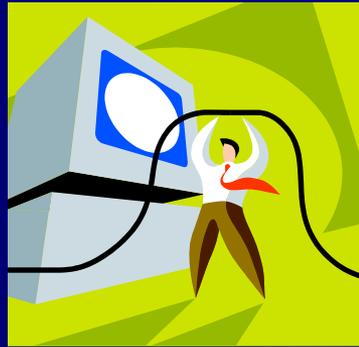
Department of
Computer Science and Engineering
Chalmers University of Technology



Contents

- Motivation
- What is Measurement?
- Measurement Theory and Scales
- Existing Security Metrics and Tools
- Attribute Based Metrics – Based on Protective and Behavioural Attributes
- 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
- Financial regulations (e.g. "Operational Risk" in **Basel-III**) also require precise risk management for technology

Why modelling?

- Quotation 1:
 - “Modelling is fundamental to measurement; without an empirical model or describing observations, measurement is not possible”
(A. Kaposi 1991)

Why metrics?

- Quotation 2:

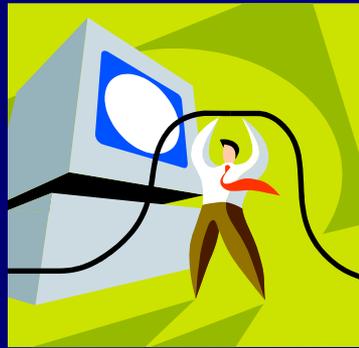
- “...if you can measure what you are speaking about and **express it in numbers you know something about it**; but when you cannot measure it, when you cannot express it in numbers, your knowledge of it is of meagre and unsatisfactory kind”
(Lord Kelvin ~1870)

Why metrics?

Quotation 3:

- “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

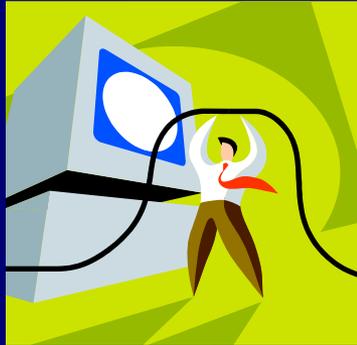
General requirements on measurement operations

- 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

Measurement Scales



Measurement scales



- Measurement 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



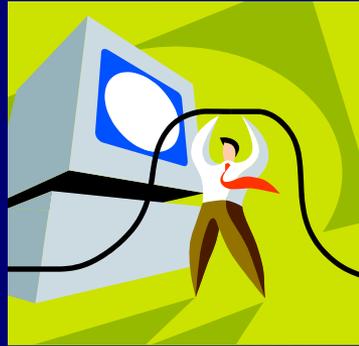
- The **nominal scale** can be used to denote membership of a class for purposes such as **labelling** or colour matching
- The **ordinal scale** is used when measurement expresses **comparitive judgement**
- The **interval scale** is used when **measuring "distance"** between pairs of items of a class 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

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)

Existing Security Metrics



What is Security?



- **SECURITY** (*"prevention of unauthorized access and/or handling"*)
 - A system is considered Secure if it is can protect itself against **intrusions**
 - There is no mathematical or formal definition of the Security of a system.
 - Security is normally defined by its **three aspects: confidentiality, integrity and availability** ("*CIA*")
 - Security **is not only technical**. It is also a function of the environment, human behaviour, etc
 - In most languages the same word is used for **security and safety** (As a matter of curiosity.)

Problems with the security concept



- Security is **not well-defined**. There are different interpretations in different areas
- Security is **multi-faceted**. It consists of a number of diverse and sometimes even contradictory attributes. (For example: integrity and availability)
- Security as a concept denotes the **absence** of something (normally vulnerabilities) rather than the presence of something. (This raises some fundamental problems wrt verification and metrication.)

Why is measuring security hard?



- In order to **measure** something we must define what we measure. i.e. define the **object system** and its characteristics
- Security is a **non-functional** attribute – others are dependability, reliability, safety, etc
- A **non-functional** attribute defines **to which extent a functional attribute is valid** (e.g. a service is delivered)
- As of today, there are **no scientifically solid metrics** of security. Instead, there are a number of informal and/or subjective assessments or rankings.

The fundamental representation problem



When measuring security the following questions could be posed:

- What is my **definition of security**?
- Which **aspects** of security do I intend to measure? Or some **composite**?
- What is it that I am measuring? (That is, **what kind of data** do I gather?)
- How do I **process these data**? If at all?
- To which extent do the **gathered and processed data represent the metric of security** that I want to capture?

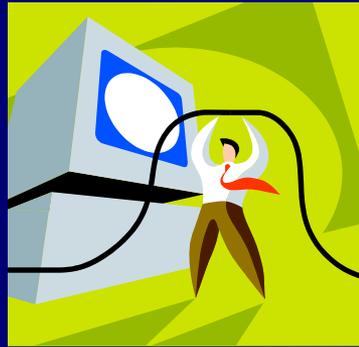
Security Metrication

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**

Existing Security Metrics



Methods for "measuring" 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 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

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 140-2¹).
"The harder to breach the crypto, the stronger it is"
- **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 - 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

Attribute Based Metrics -

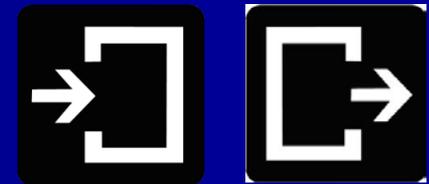
- A Conceptual Model for Security and Dependability



Black Box Approach



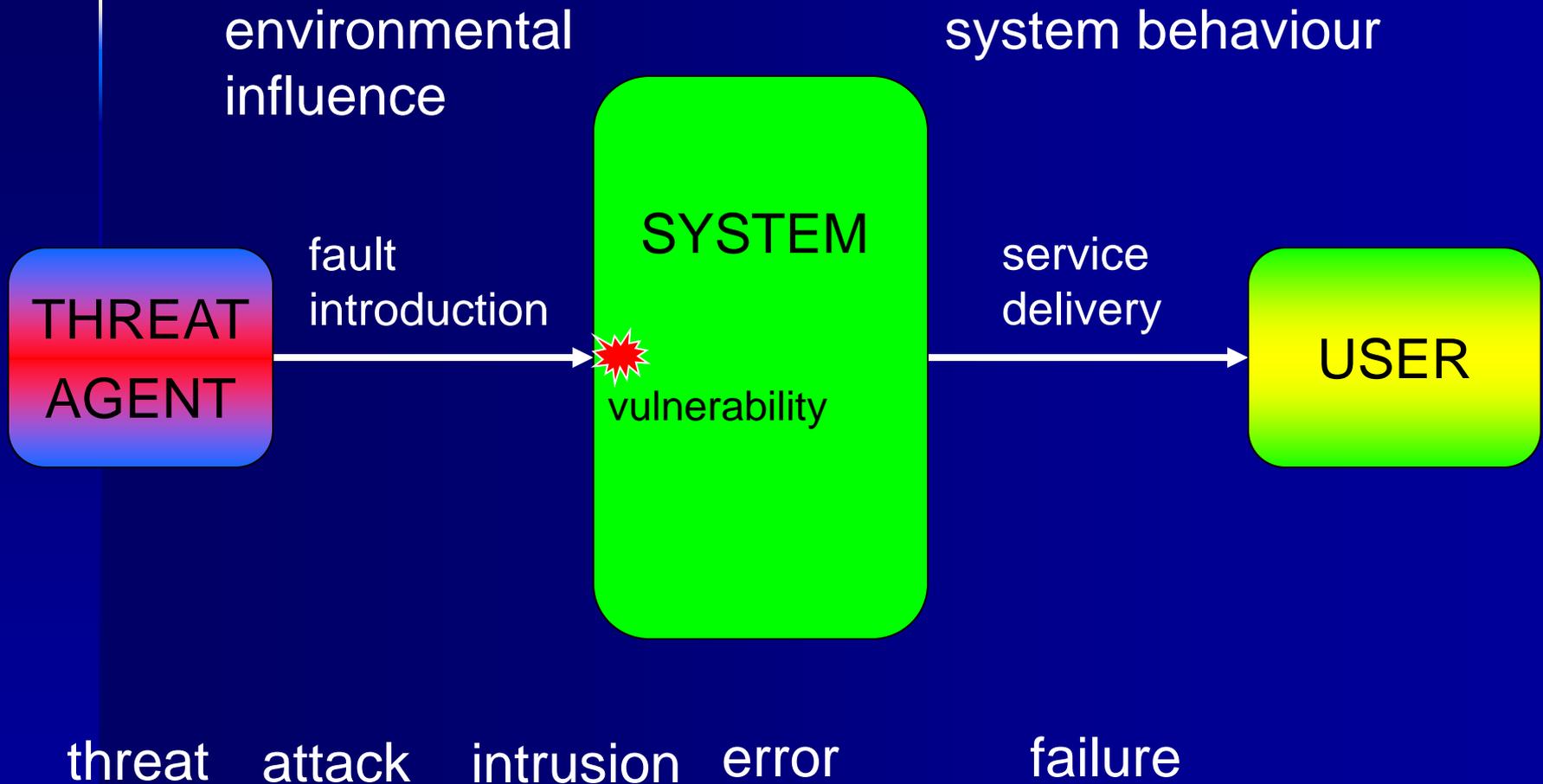
- Our approach is based upon system interaction with the **environment**, i.e. **input and output**



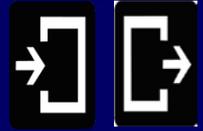
- Input: Environmental influence
 - ***Fault introduction***: malicious, external
- Output: **System behaviour**:
 - delivery of service, denial of service
 - USERS and NON-USERS



A very simple system model



A system model wrt security and dependability

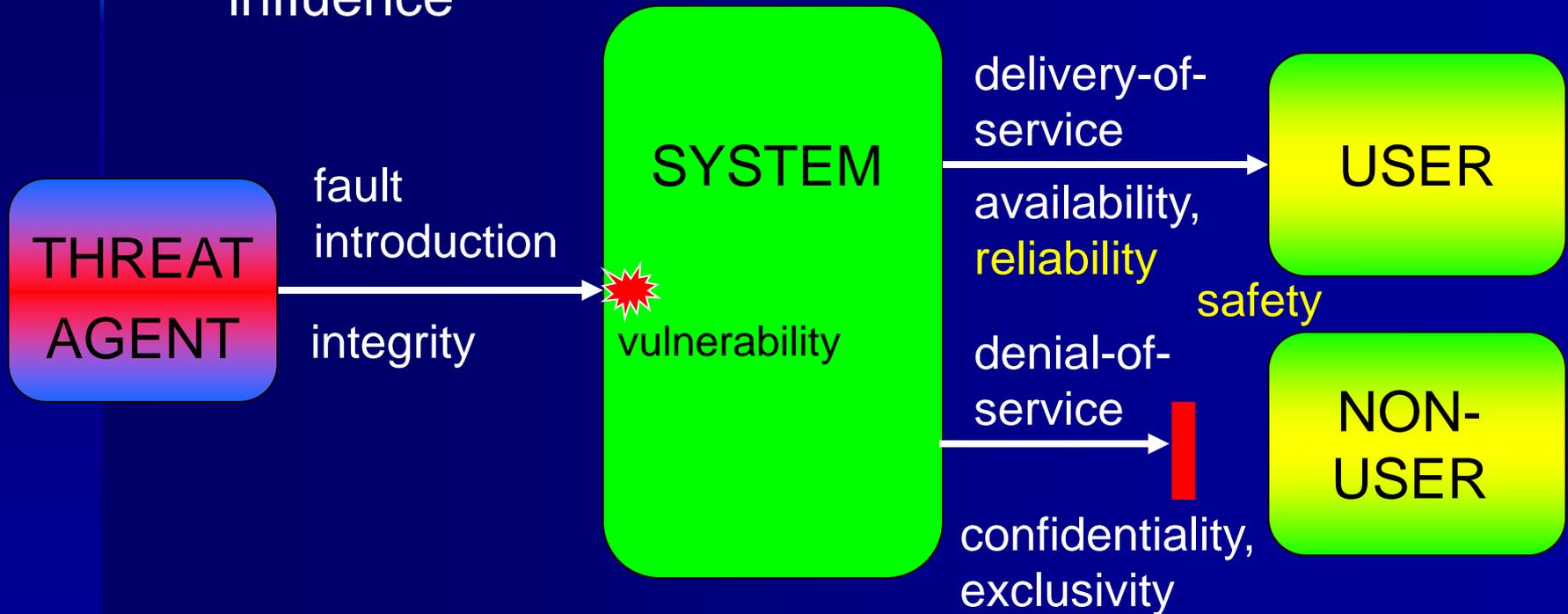


PROTECTIVE ATTRIBUTES

BEHAVIOURAL ATTRIBUTES

environmental
influence

system behaviour

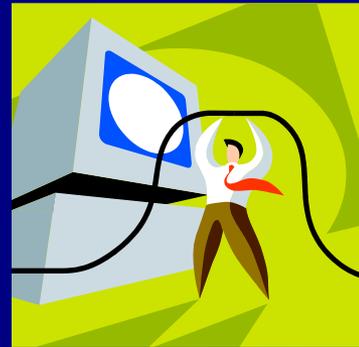


threat attack intrusion error

failure

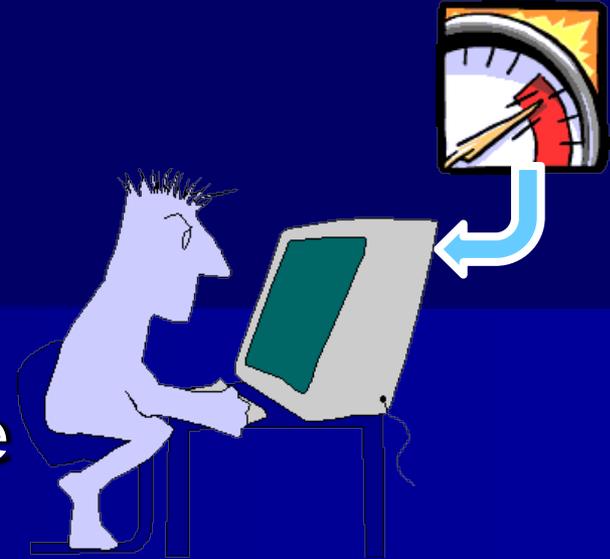
Attribute Based Metrics -

- Security and Dependability Metrication



The overall idea

- **Security** is a composite concept and cannot easily be measure as such
- The same goes for **dependability**
- However, we can combine the two and split them up into **primitive attributes**
- We can more easily define **metrics for these primitive attributes**



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
 - Concept (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)

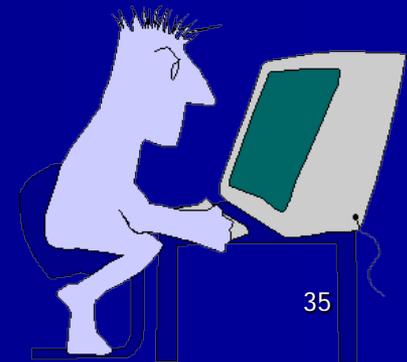


– *System-related metrics*

- 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 **reflects the security** of the system
- Mean Time To Intrusion (MTTI)

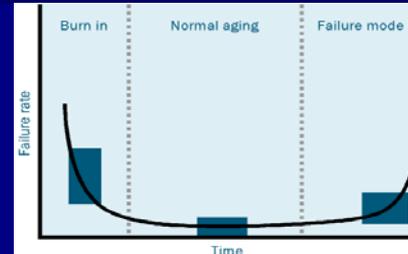


Behavioural Metrics



Behavioural metrics:

Quantify system behaviour



Such measures already exist, e.g. for:

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

But less so for:

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



Causal Chain of Impairments

Threat →

Attack →

Intrusion →

Error

Failure



- Note that a **failure** may (or may not) originate from an **attack**.
- Or vice versa, there can be a **failure without an attack**
- There is an unknown **delay** ($0 \rightarrow \infty$) between the attack and the failure (**latent errors**)
- Thus: **Insufficient integrity behaviour**  **may lead to degraded**

A few observations



- The **end-user** perspective: the user does not care why there is a failure, only that there must be none
- **Safety** is a subset of other behavioural attributes
- The **causal chain** between impairments
- Note that a **failure may** (or **may not**) **originate** from an **attack**
- Or vice versa, there can very well be a **failure without an attack**
- The **time aspect** implies an unknown delay between the attack and the failure (if any) – latent errors

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**
 - **Practicable concrete measurement methods**
 - **Intrinsically measurable components** (“developing components that are inherently attuned to measurement”)



Conclusions



- An overall security metric is **highly desirable**
- We have given **a brief overview** over the state of research and available methods
- 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**

