



# Security Metrics – approaches, problems and possibilities

Presented by  
Erland Jonsson

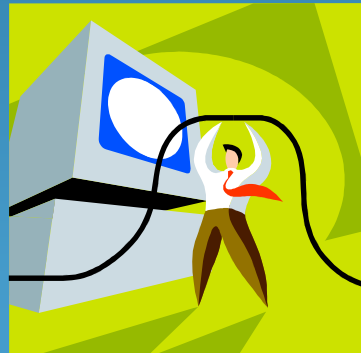


# Contents

- Motivation
- What is Security?
- What is Measurement
- Relational systems
- Measurement scales
- Security Metrics today
- Suggested Security Metrics Research
- Summary



# Motivation

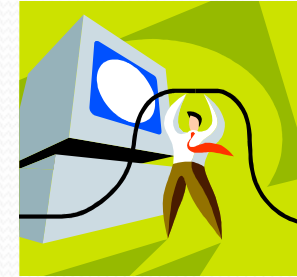


# Motivation



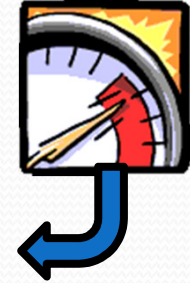
- Security is a major concern in computer-based systems, i.e. virtually **all** systems of today
- A number of standard bodies (e.g. **ANSI 2008**) require risk analysis
- Financial regulations (e.g. "Operational Risk" in **Basel-III**) also require precise risk management for technology
- It is good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

# 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, 1883)

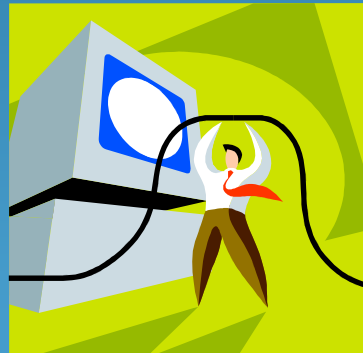
# Why metrics?



Quotation 3:

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

# What is security?





# 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
- Security as a concept denotes the **absence** of something (normally vulnerabilities) rather than the presence of something.

# 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 not only technical**. It is also a function of the environment, human behaviour, legal aspects, etc
- In most languages the same word is used for **security and safety** (As a matter of curiosity.)

# What is Security? - II



- **Security** is normally defined by its three aspects: **confidentiality, integrity and availability** (“CIA”)
- Cp to **dependability**: **reliability, availability, safety, integrity and maintainability** (overlap! – how do we combine them?)
- Sometimes the security concept also includes: **authenticity, accountability, non-repudiation,...**
- Cp **operational security** to security based on **system design characteristics**

# What is Security? - III



You will also find the following approaches:

- Security is the number and strength of a set of (pre-defined) security mechanisms (used in some standards)
- Security is defined in terms of threat level
- Security is described by a set of “security requirements” or policies and the extent to which these are fulfilled (req’s are freely selected )
- Security is defined by a certain Evaluation Assurance Level (EAL) for a Security Target (CC)

# What is Security? - IV



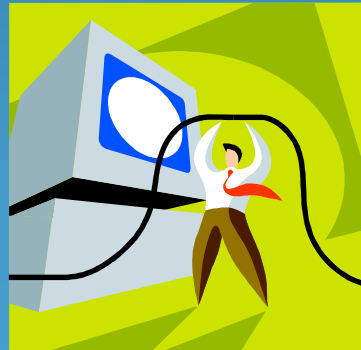
- Security is assessed by means of performing a **Risk Analysis**
- The risk analysis is normally based on *subjective judgement* – hopefully by experts – of how well certain security requirements are met
- Security can also be defined **for specific areas or characteristics**, e.g., **privacy**, **cryptographic strength**

# What is Security? - V

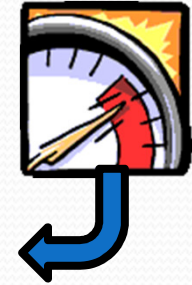


- Security is not a well-defined concept as such –  
- it is ambiguous and multi-faceted. It must be regarded as an umbrella concept
- For a scientific treatment it has to be **split up into more basic entities**, for which exact definitions are possible to make
- I have suggested that **integrity** is the attribute that most closely reflects the notion of **traditional security**

# What is measurement ?



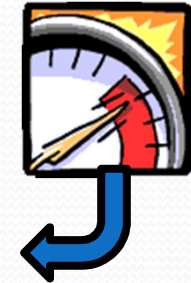
# Definition of measurement



- **Definition:**
  - **Measurement** 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.



# 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 measurer**
- Measurements must **not be corrupted** by an **incidental, unrecorded circumstance**, which might influence the outcome

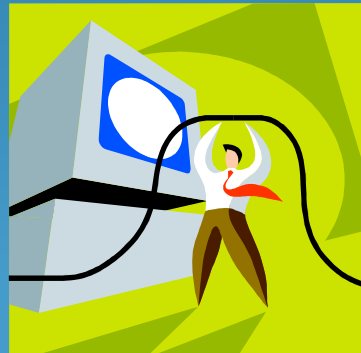
# Specific requirements on measurement operations



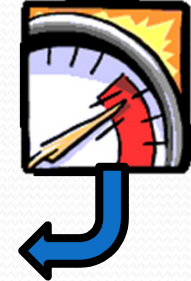
- Measurement must be able to **characterize abstract entities** as well as to **describe properties** of real-world objects
- The result of measurement may be captured in terms of **any well-defined formal system**, i.e. not necessarily involving numbers

# Relational systems

- from measurement theory



# Relational systems



- There are two types of relational systems:
  - the **empirical** relational system
  - the **formal** relational system
- These two relational systems gives the theoretical basis for **defining measurement scales**

# Empirical relational system



- Let  $A = \{a, b, c, \dots, z\}$  be the target set and  $\kappa$  the chosen key property
- Ex.  $A$  is the set of schoolchildren in a class and  $\kappa$  is the property of their height.
- Now let  $A = \{a, b, c, \dots, z\}$  be the model of  $A$  which describes each child in terms of the property height
- The empirical relational system comprises this model set together with all the operations and relations defined over the set

# Empirical relational system (con't)



- We can now attempt to describe the **empirical relational system** as an **ordered set**  
 $E = (A, R, O) = (A, \{r_1, r_2, r_3\}, \{o\})$ , where
- **R** is a set of relations:
  - $r_1$  = taller than
  - $r_2$  = the same height as
  - $r_3$  = heads and shoulders above, and
- **O** is a set of binary operations:
  - $o$  is the operator "standing on the head of"

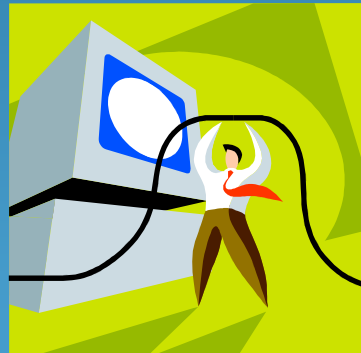
# Formal relational system



- We can now attempt to describe the formal relational system as a nested set  $F = (A', R', O')$
- The formal relational system  $F$  must be capable of expressing all of the relations and operations of the empirical relational system  $E$
- The mapping from  $E$  to  $F$  must actually represent all of the observations, preserving all the relations and operations of  $E$
- If this is true we say that the mapping  $A \rightarrow A'$  is a homomorphism and  $F$  is homomorphic to  $E$

# Scaling and scale types

- from measurement theory



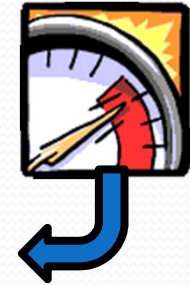


# Scale of measurement



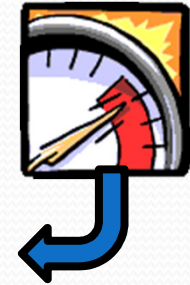
- Assume that:
  1. The set  $A$  models the target set  $A$ , wrt to  $\kappa$
  2. We have the empirical system  $E = (A, R, O)$  and the formal system  $F = (A', R', O')$
  3.  $m$  is a homomorphic mapping from  $E$  to  $F$
- Then  $S = (E, F, m)$  is called the **scale of measurement** for the key property  $\kappa$

# Scale of measurement



- Now if  $F$  is defined over some subset of real numbers, then:
  - measurement maps the key property of each object of the target set into a number
  - further, if the mapping is **homomorphic** then:
    1. the **measured data will be representative** of the key property of the corresponding object, and
    2. empirical **relations and operations** on the properties **will have correct representations** on the corresponding numbers

# Scale of measurement



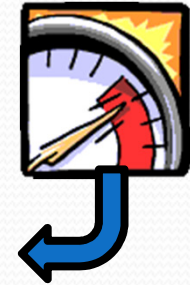
- The **homomorphism** assures that these formal conclusions, drawn in the number domain will have corresponding conclusions in the empirical domain and thus that the purpose of the measurement is fulfilled
- Or in more general terms:  
Our theoretical conclusions will be valid to the real world and let us draw corresponding conclusions for it
- A homomorphism is seldom unique, e.g cost can be expressed in EUROS or in SEK

# Measurement scales



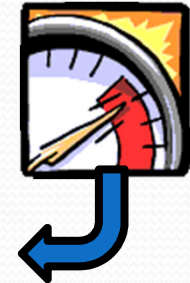
- Measurement theory distinguishes five types of **scale**:
  - **nominal** scale
  - **ordinal** scale
  - **interval** scale
  - **ratio** scale
  - **absolute** scale
- Here they are given in an ascending order of "strength", in the sense that each is permitting less freedom of choice and imposing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

# Nominal scale



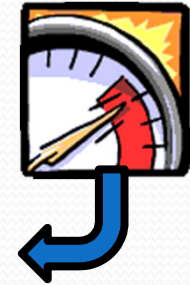
- The **nominal scale** can be used to denote membership of a class for purposes such as **labelling** or colour matching
- There are **no operations** between **E** and **F**
- The **only relation** is equivalence
- One-to-one mapping

# Ordinal scale



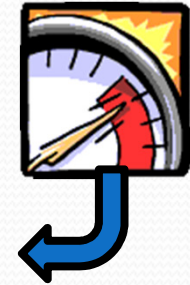
- The **ordinal scale** is used when measurement expresses **comparitive judgement**
- The scale is preserved under any montonic, transformation:  
$$x \geq y \Leftrightarrow \phi(x) \geq \phi(y),$$
where  $\phi$  is an admissible transformation
- Used for grading goods or rating candidates

# 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



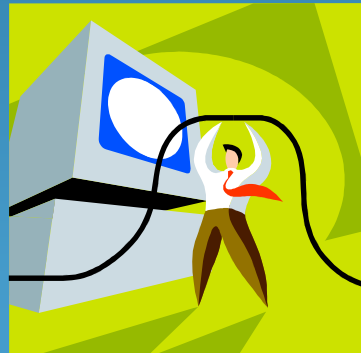
- The **absolute scale** is a ratio scale which includes a "standard" unit.
- The scale is only preserved under the identity transformation:  
$$\phi(x) = x,$$
which means that it is not transformable
- Used for **counting items** of a class

# Meaningfulness

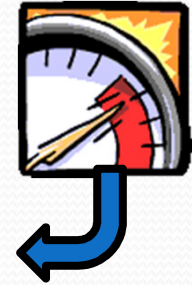


- **Meaningfulness** means that the scale measurement should be appropriate to the type of property measured, such that once measurement has been performed – and data expressed on some scale - **sensible conclusions can be drawn** from it
- Example 1: Point A is twice as far as point B (meaningless, 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)

# Security Metrics today



# 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? (I.e. **what kind of data** do I gather?)
- How do I **process these data**? If at all?
- Do which extent do the **gathered and processed data represent the metric of security** that I want to capture?

# Why is measuring security hard?



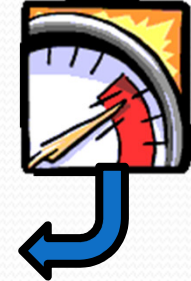
- In order to **measure** something we must define what we measure. i.e. define the **object system** and its characteristics
- Security is a **non-functional** attribute – others are dependability, reliability, safety, etc
- A **non-functional** attribute defines **to which extent a functional attribute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

# Methods for “measuring” security I



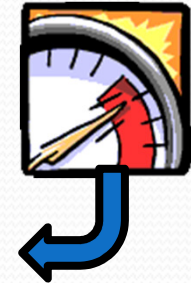
- **Evaluation/Certification** (according to some standard):
  - *classification* of the system in classes based on design characteristics and security mechanisms.  
*“The ‘better’ the design is, the more secure the system”*
- **Risk analysis:**
  - *estimation* of the probability for specific intrusions 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

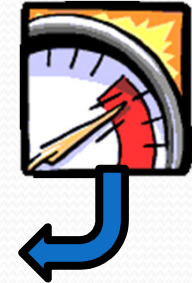
# Methods for “measuring” security III – special cases



- **Cryptographic strength:**
  - a statistical metric of the strength of a crypto system based on *the computational effort* for a successful cryptanalysis.  
*“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, ....**

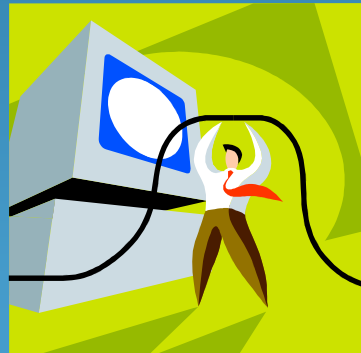


# Methods for “measuring” security IV - tools



- **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
- **ISO/IEC 27001** (An ISO standard – the old BS 7799-2):
  - is an infosec management standard. Includes risk assessment.

# Suggested Security Metrics Research



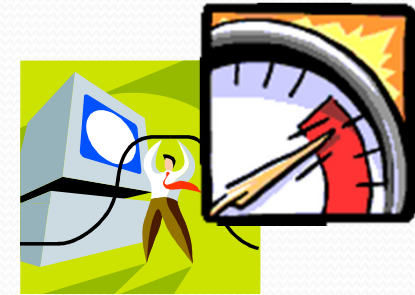
# Security metrics research

- 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”)

# Summary



- An overall security metric is **highly desirable** by many actors
- As of today there are **no scientifically solid metrics** for security
- We have given a brief and heuristic overview of a few **concepts from measurement theory**
- I have given a brief overview over the **state of research** and available methods
- I have listed a number of different security **definitions and approaches**





The Seventh International Conference  
on Emerging Security Information,  
Systems and Technologies



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

---

**Experts Panel**

**Topic: How Much Security is Enough: A Fair Cost Assessment?**  
Tuesday, July 20, 17:30 – 19:30h

**SECUWARE 2013**  
**August, 27<sup>th</sup>. 2013 – Barcelona, Spain**

---



---

---

---

---

---


---

---


---

---

---



The Seventh International Conference  
on Emerging Security Information,  
Systems and Technologies



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

---

**Behavior Risk: the Indefinite Aspect at the  
Stuxnet Attack?**

**SECUWARE 2013**  
**August, 27<sup>th</sup>. 2013 – Barcelona, Spain**

Wolfgang BÖHMER, TU-Darmstadt,  
Hochschulstr. 10, D-64289 Darmstadt,  
Dpt. of Computer Science, Security Engineering Group  
Email: wboehmer@cdc.informatik.tu-darmstadt.de

---



---

---

---

---

---


---

---

---

---

---



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

---

**Outline**

- (1) Introduction / Motivation
  - 6-tuple I/O automaton and static/dynamic policies
  - Control theory and the feedback component
- (2) Bi-simulation between a standard automaton and the Deming cycle
  - Describing the PDCA-Cycle by a standard automation
  - Observed behavior between the Deming quintupel  $\mathcal{D}$  and a standard Automaton  $\mathcal{A}$
- (3) Control loops and Standards for Management Systems
  - Control circuit for ISO 27001 (ISMS)
  - Control circuit for BS 25999 (BCMS)
  - Control circuit for ISO20000 (ITSM)
- (4) The Coupling function  $\xi$  and Management Systems
  - "coupling" is generally a linkage between different systems
  - Weak and strong coupling between different Management System
  - Discussion of the coupling results between the management systems
- (5) Conclusion and further work

---

August 25-31, SECUWARE 2013 | Barcelona, Spain | W. Boehmer | experts panel discussion, Tuesday, 27 | page 3

---

---

---

---

---

---

---

---

---

---

### My statement to the panel (I)



1. We have to distinct between it-security and information security. This are two different pair of faces of security. IT-security is strongly technical orientated and information security not. It's about a flow of information in network, which has to be protect.
2. The internet has growing up from scientific network to global communication platform. Nicolas Carr has pointed out in his book, the big switch, a couple of years ago, that the internet is now a common infrastructure component like, electricity, water, energy.
3. The infrastructure of the internet has been changed from a strictly wired oriented network to a global network with intensive use of mobile connections. The internet is now ubiquity.
4. For this background some new challenges rise up, especially for trust and privacy in the internet.
5. There is a big difference between trust, privacy and security. Security has (nearly) nothing to do with trust and privacy.

August 25-31, SECLWARE 2013 | Barcelona, Spain | W. Boehmer | experts panel discussion, Tuesday, 27 | page 4

---

---

---

---

---

---

---

---

---

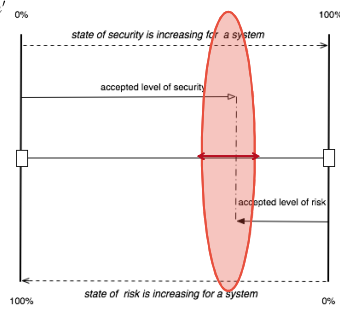
---

### Relationship between risk and security the cost/ benefit calculation



$$sec = 1 - risk [R^-] \mapsto 'value chain'$$

- Increasing your safeguarding leads automatically to an increasing to the cost for the measurements
- Decreasing your safeguarding leads automatically to an increasing of a possible damage
- It must be established a balance between the effectiveness and the economic efficiency of the measurements



August 25-31, SECLWARE 2013 | Barcelona, Spain | W. Boehmer | experts panel discussion, Tuesday, 27 | page 5

---

---

---

---

---

---

---

---

---

---

### My statement to the panel (II)



6. Privacy has a binary behavior, if some information is on the internet, this information will be never deleted, because the internet has not the potential to forget anything.
7. Trust is a bit different to privacy, because trust is level oriented and you can get some experience with trust.
8. You can have some different levels of trust to the same person or same connection on the internet.
9. Trust and security have the same control objective – confidentiality. But security has in general the additional control objective of integrity and availability.
10. The pitfall of the current internet technology is, that we have no trust metrics and no privacy metrics, so we can't measure both of this control objectives. We have only different policies and different requirements from different countries.

August 25-31, SECLWARE 2013 | Barcelona, Spain | W. Boehmer | experts panel discussion, Tuesday, 27 | page 6

---

---

---

---

---

---

---

---

---

---