Security and dependability modelling

Erland Jonsson

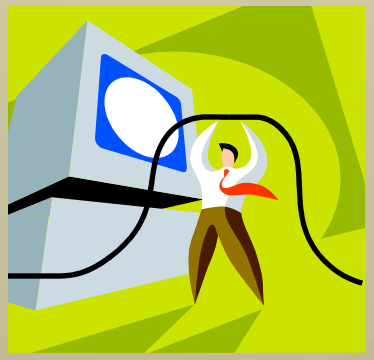
Department of
Computer Science and Engineering
Chalmers University of Technology

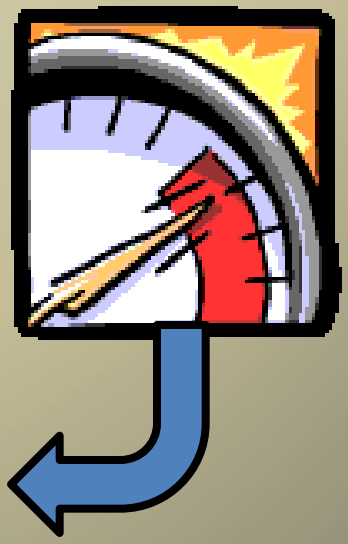
150215

OUTLINE OF LECTURE

- Goal and motivation
- A system model for security and dependability
- A biological analogy
- The time aspect
- A few observations
- Extensions/complications
- Conclusions

GOAL and MOTIVATION





GOAL OF LECTURE

The goal of this lecture is to:

- answer the question: “What ***is*** SECURITY?”
- present a conceptual model of dependability and security, including a suggested terminology. Thus, dependability and security represent different aspects of a common meta-concept.
- clarify that security is multi-faceted and can not be treated as a clear-cut atomic concept.
- the conceptual model is aimed to facilitate metrication of security/dependability
- All in all: **to give a better understanding of the security/dependability area**

Why modelling?

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

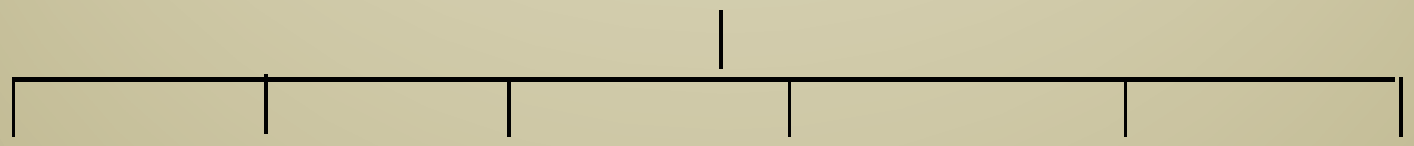
A SYSTEM MODEL for SECURITY and DEPENDABILITY

WHAT IS DEPENDABILITY?

DEPENDABILITY

- is a general, “umbrella” concept
- is not mathematically well-defined
- denotes the research area: Dependable Computing

DEPENDABILITY ATTRIBUTES



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

"CIA" = SECURITY

What is Security?

- SECURITY *("prevention of unauthorized access and/or handling")*
  - A system is considered Secure if it is can protect itself against intrusions
  - 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)
- There is no mathematical or formal definition of the security of a system.
- Security as a concept denotes the absence of something (normally vulnerabilities) rather than the presence of somehing. This raises some fundamental problems wrt verification and metrication.

Traditional security attributes (CIA)

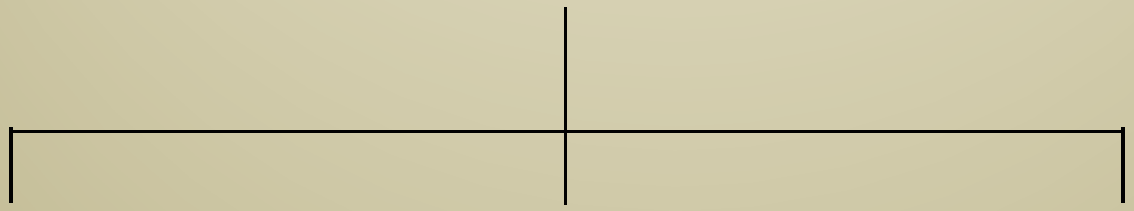
- Confidentiality
  - Prevention of the unauthorized disclosure of information
- Integrity
  - Prevention of the unauthorized modification of information
- Availability
  - Prevention of the unauthorized withholding of information or resources

Others include: authenticity, non-repudiation, survivability, accountability, freshness, etc

AN INTERPRETATION OF THE TRADITIONAL SECURITY ATTRIBUTES

Information security

Datasäkerhet



Confidentiality

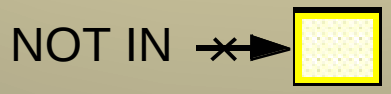
Sekretess

prevention of the ***unauthorized*** disclosure of information

Integrity

Integritet

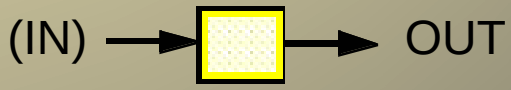
prevention of the ***unauthorized*** modification of information



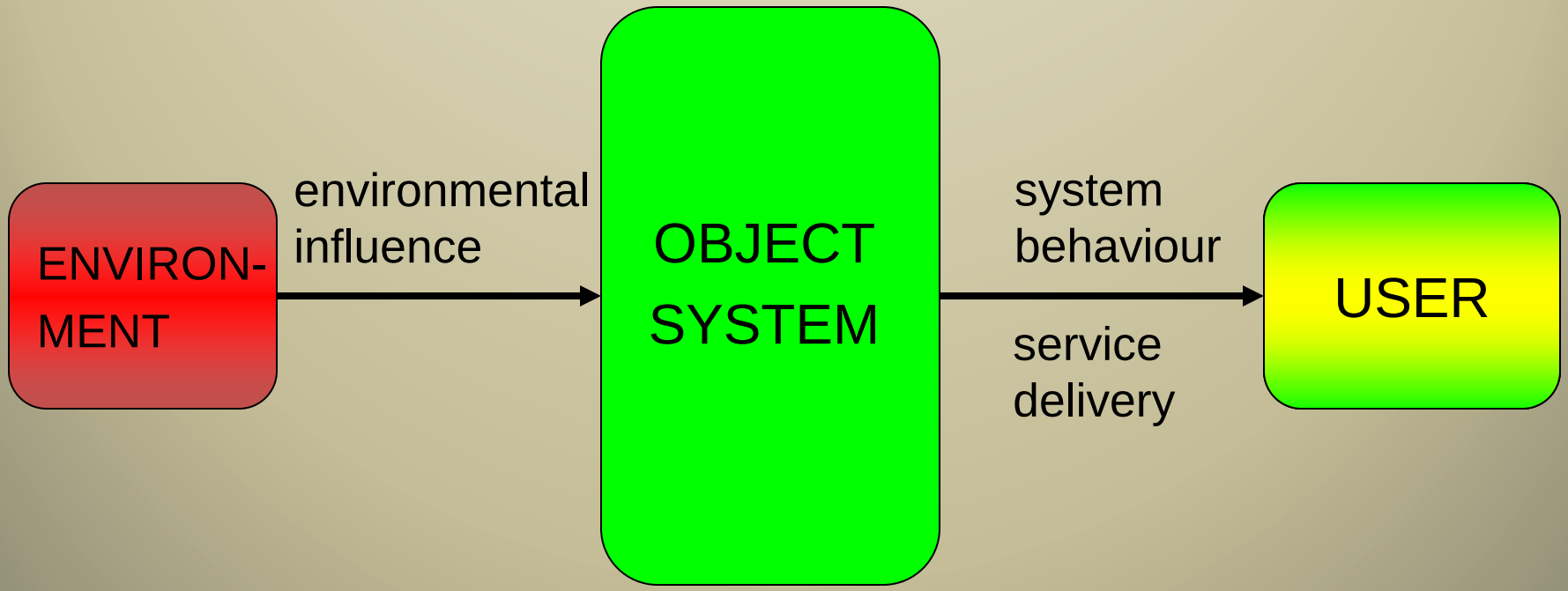
Availability ("CIA")

Tillgänglighet

information must be available to the ***authorized*** user

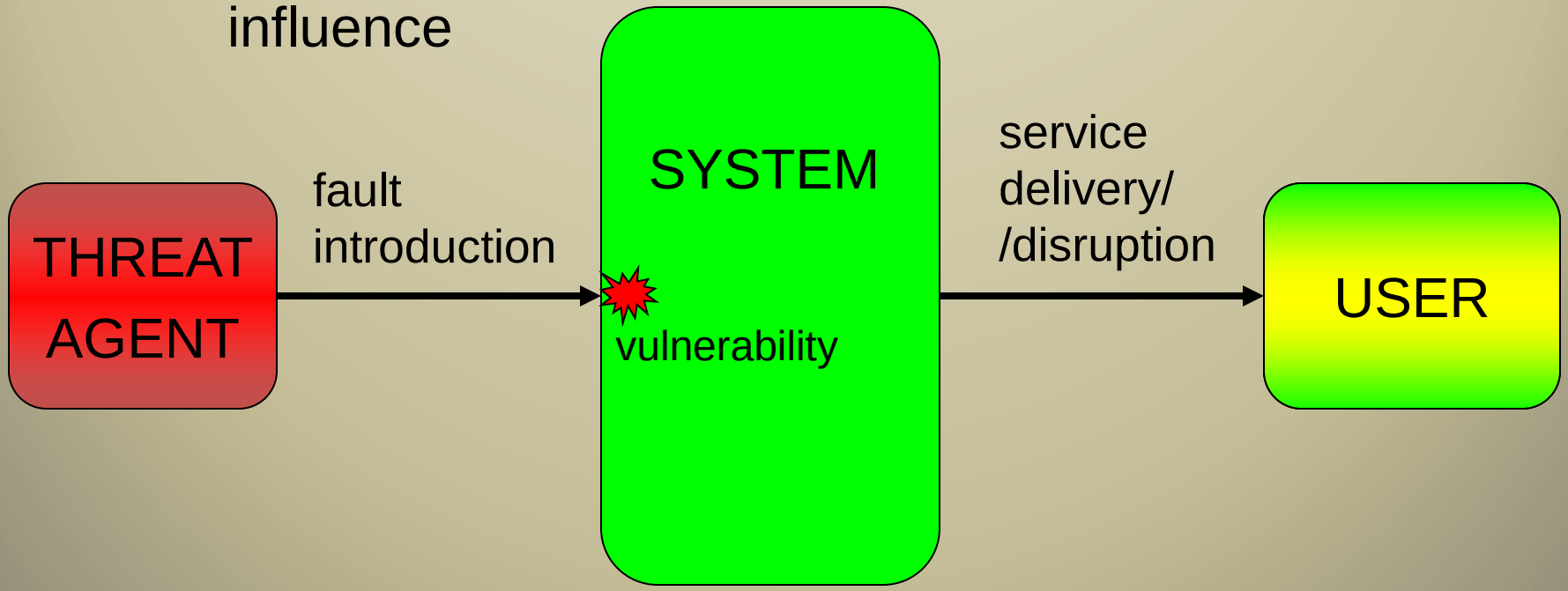


A very simple system model



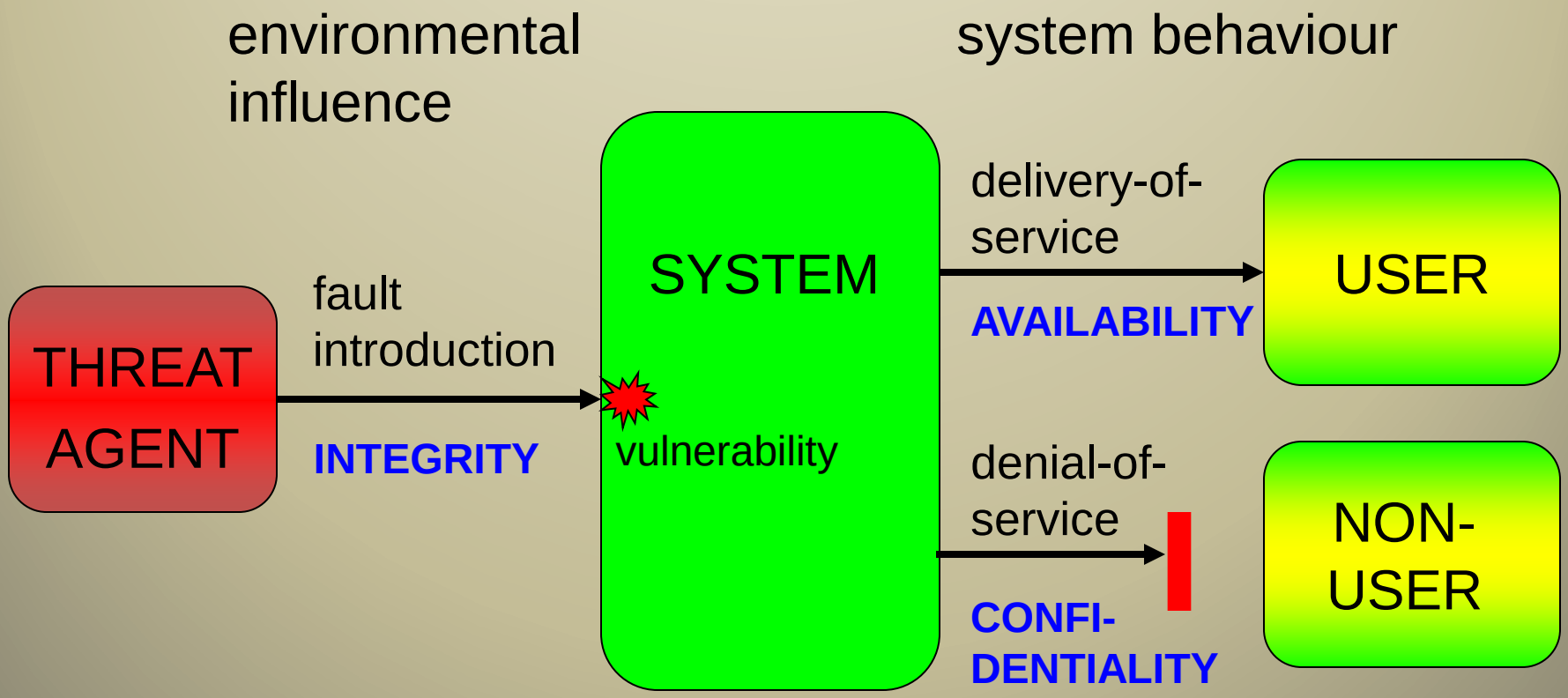
Embedded parameters (design)

A very simple system model - threat related



threat attack intrusion error failure

A system model wrt security



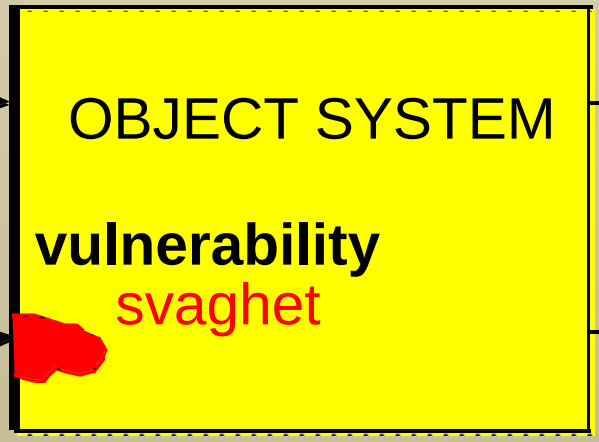
threat attack intrusion error failure

SECURITY ATTRIBUTES in the SYSTEM MODEL

PROTECTIVE ATTRIBUTES

CORRECTNESS

BEHAVIOURAL ATTRIBUTES



ACCESSABILITY
w.r.t ***the user***

INTEGRITY
w.r.t. the
unauthorized user

AVAILABILITY
towards ***the user***

CONFIDENTIALITY
towards the
unauthorized user

threat **attack** **intrusion** **erroneous state** **failure**

environmental **influence** system **function** **service** delivery

SECURITY/DEPENDABILITY ATTRIBUTES in the SYSTEM MODEL

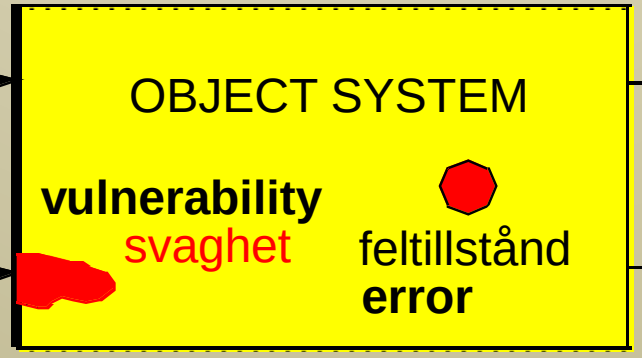
PROTECTIVE ATTRIBUTES

CORRECTNESS

BEHAVIOURAL ATTRIBUTES

ACCESSABILITY
w.r.t ***the user***

INTEGRITY
w.rt to the
unauthorized user



RELIABILITY
AVAILABILITY
towards the ***user***

CONFIDENTIALITY
towards the
unauthorized user

threat **attack** **intrusion** **erroneous state** **failure**

SAFETY

environmental **influence**

system **function**

service delivery

A FUNDAMENTAL SYSTEM MODEL FOR DEPENDABILITY/SECURITY

<----------INTRUSION DETECTION ---------->

THREAT REDUCTION **BOUNDARY PROTECTION** **RECOVERY**

PROTECTIVE ATTRIBUTES

CORRECTNESS

BEHAVIOURAL ATTRIBUTES

ACCESSABILITY
w.r.t ***the user***

INTEGRITY
w.rt to the
unauthorized user

OBJECT SYSTEM

vulnerability
svaghet

feltillstånd
error

RELIABILITY
AVAILABILITY
towards ***the user***

CONFIDENTIALITY
towards the
unauthorized user

threat **attack** **intrusion** **erroneous state** **failure** **SAFETY**

environmental **influence** system **function** **service** delivery

EXEMPLES of PROTECTION MECHANISMS - IN PRINCIPLE

- ***preventive protection - threat reduction:***
  - legal protection
  - reducing threats (e.g. “security check-ups”)
  - **education / information / propaganda!**
- ***boundary protection:***
  - shield cables
  - encryption
  - physical protection (e.g. locks)
  - access control
- ***internal protection - recovery:***
  - (anti-)virusprograms
  - supervision mechanisms (with recovery capabilities)
  - encryption of stored data

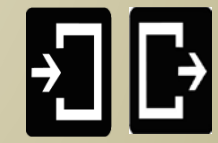
A BIOLOGICAL ANALOGY

AN ANALOGY TO HUMAN BEINGS

THREAT REDUCTION

BOUNDARY PROTECTION

RECOVERY



PROTECTION *HEALTH* *BEHAVIOUR*

system **function**

germs wound fever being ill/death

threat **attack** **intrusion** **erroneous state** **failure**

SOME OBSERVATIONS FROM THE BIOLOGICAL ANALOGY

- **THREATS:**
  Threats are there all the time.
  Threats change and evolve.
- **PROTECTION MECHANISMS:**
  Protection takes place at different levels.
  Protection mechanisms are active continuously.
  Protection mechanisms must also change and evolve according to the threats.
  Even anticipatory protection exists. (inoculation)
- **Hypothesis:**
  Modern IT systems are so complicated so that a biological paradigm must be adapted. Thus, security protection must be a continuous process, taking place simultaneously on all protection levels. Security protection must be adaptive.

THE TIME ASPECT

Causal Chain of Impairments

Threat → **Attack →** **Intrusion →** **Error** → **Failure**

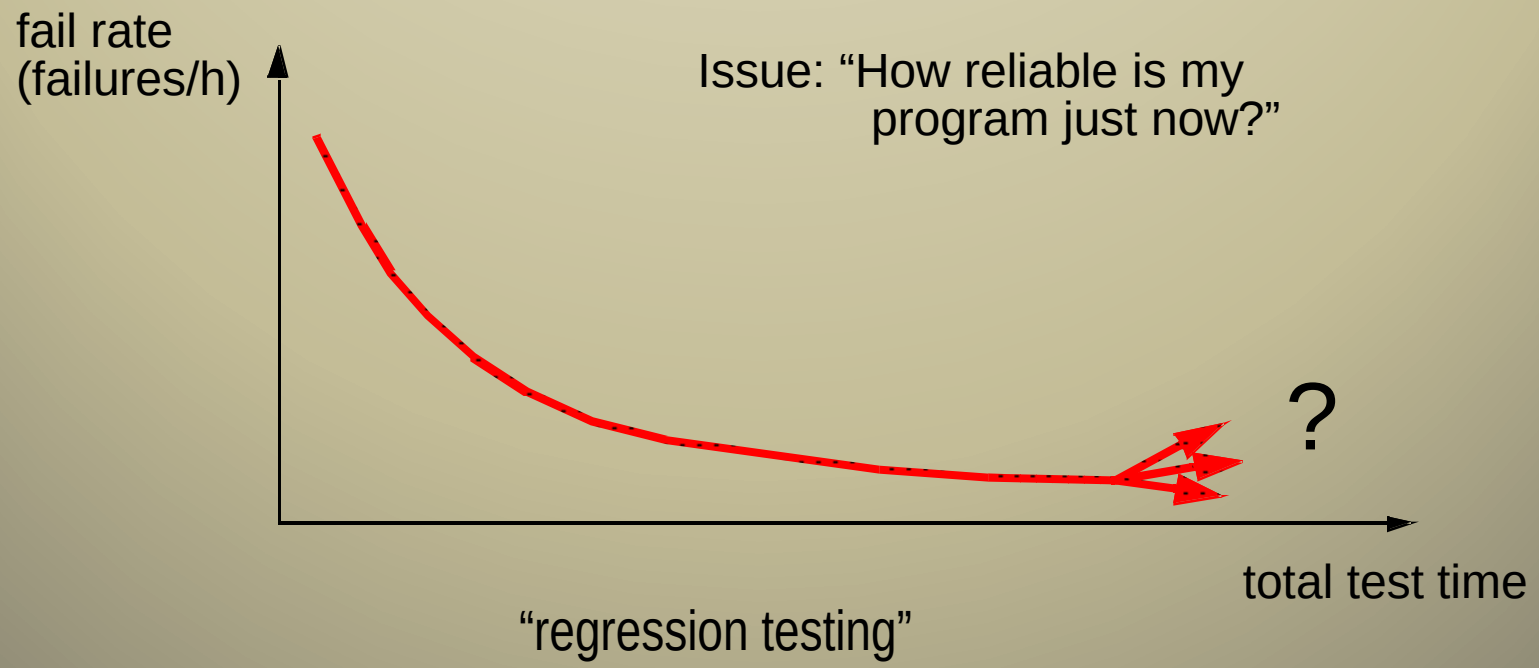
- Note that a **failure** may (or may not) **originate from an attack**.
- Or vice versa, there can be a **failure without an attack**
- There is an unknown **delay** (0 -> ∞) between the attack and the failure (**latent errors**)
- Thus: ***Insufficient integrity*** → **may lead to** → ***degraded behaviour***

THE TIME ASPECT – SOME OBSERVATIONS

- the time aspect is very often neglected in security analysis. It must be noted that:
- introduction of a fault into the system does not mean that the system fails immediately. It may never fail due to this fault. This is the latency aspect - latent errors.
- system latency affects system behaviour (e.g. reliability, availability, etc) and metrics. There might be a substantial time between the original fault occurrence and the resulting (deficient) system behaviour.
- faults can be introduced into a system throughout its lifetime. Many faults are introduced during the design phase.
- some security mechanisms do not protect the system as it stands. But it will give information for improving subsequent generations of it (e.g. intrusion detection)

THE TIME ASPECT – DEBUGGING
(A software analogy)

"the law of diminishing results"
(regarding debugging of software):
It will be increasingly hard to find the remaining faults



THE TIME ASPECT - LATENCY
(Another software analogy)

- A program can have many errors with very long MTTF.
- An investigation of an IBM-program showed that more than 30% of the errors had an **MTTF > 5000 years!!** This means that if we test the system continuously, after 5000 years some 30 % of the errors remain latent!

  (Ref: E. N. Adams: "Optimizing preventive service of software products", *IBM Journal of Research and Development*, vol. 28, No. 1, pp. 2-14, 1984.)

- The same problem applies to *security vulnerabilities*

A FEW OBSERVATIONS

- Make a distinction between non-functional and functional attributes
- The end-user perspective: the user does not care why there is a failure, only that there must be none
- The desirable behaviour of a system depends on the intended user (e.g. authorized or not)
- a security problem is not the same as a reliability problem but they are related (in a complicated way)
- Safety is a subset of other behavioural attributes
- 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

EXTENSIONS/COMPLICATIONS to the system model

Why is this just part of the truth?

There are a number of issues that are not addressed and extensions to be made to make things more realistic:

- add feedback
- non-binary output (degraded performance)
- non-binary input ("gradual attack")
- multiple causes for an attack

Some extensions that must be considered

- cascading of systems
- hierarchical systems ("systems-of-systems")

CONCLUSIONS

- Dependability and security reflect two different approaches to the same fundamental research area
- We have suggested a fundamental ***system model*** for dependability and security, describing the system in terms of **protective** and **behavioural characteristics** (and also ***correctness***)
- Dependability and security metrics could be defined in accordance
- Protection methods and mechanisms have been related to the system model