A Framework for Security Metrics Based on Operational System Attributes

Erland Jonsson

Laleh Pirzadeh

Chalmers University of Technology

Göteborg, Sweden

Basics: “Definitions” of Security and Dependability

Security:

- A system’s ability to withstand hostile interaction or attacks (***intentionality***)
- *Confidentiality, Integrity, Availability*

Dependability:

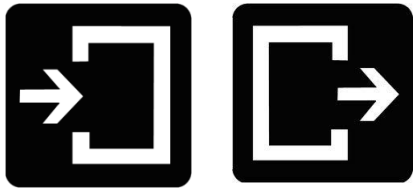
- *Availability, Reliability, Safety, Integrity Maintainability*
- Non-intentional, random faults (traditionally)
- Intentional faults (to some extent)

The Overall Message

- It is hard (or even impossible?) to find a comprehensive and mathematically well-defined metric of security
- We believe that (the combined concept of) **security and dependability** represent different aspects of the same generic system property
- We suggest that security (and dependability) metrication is best achieved by finding metrics for each security (and dependability) attributes

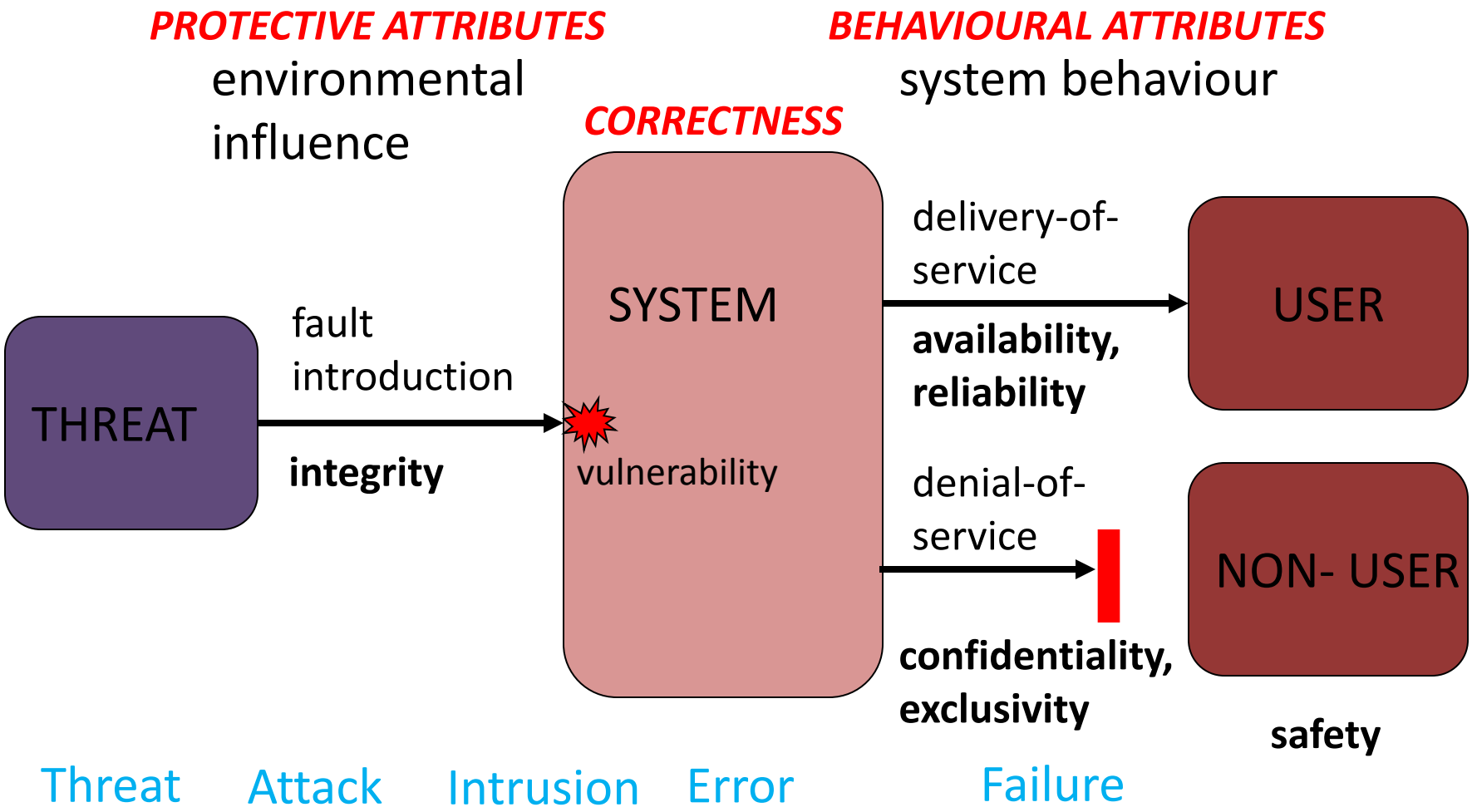
Black Box Approach

System interaction with the **environment** i.e.
Input and Output



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

A Conceptual System Model w.r.t Security and Dependability



Two different Types of Security Metrics

- **Protective metrics** (INPUT)
  - embodies the notion of protection
  - most important characteristics of security (i.e. integrity)
- **Behavioural metrics** (OUTPUT)
  - relates to system behaviour
  - dependent on protective security

Protective Security Metrics

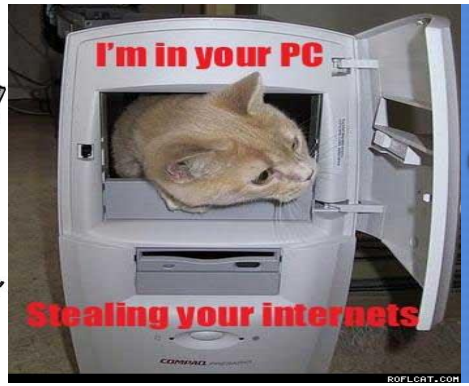
- Protective metrics should quantify:
  - the extent to which the system is able to protect itself against unwanted **external influence**
  - i.e. integrity
- *Two types of protective metrication (at least)*
  - *System-related metrics*
  - *Threat-related metrics*

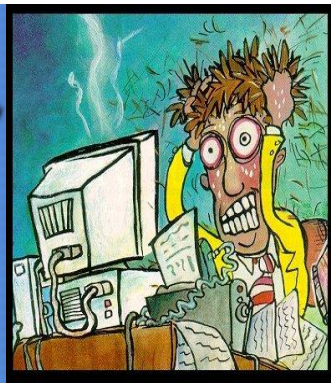
Protective Security Metrics (cont'd)

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

Causal Chain of Impairments

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





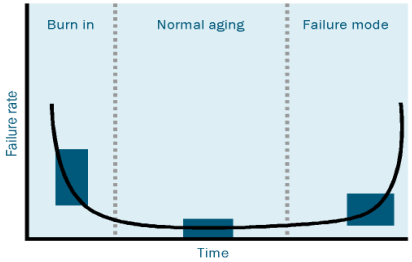
- Note that a **failure** may (or may not) **originate from an attack**.
- Or vice versa, there can be a **failure without an attack**
- There is an unknown **delay** (0 -> ∞) between the attack and the failure (**latent errors)**

- Thus: ***Insufficient integrity*** **MIGHT Lead To** ***degraded behaviour***

Behavioural Security Metrics

Behavioural metrics:

Quantify system behaviour



Such measures already exist, e.g.:

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

But less so for:

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

Conclusion

- We have suggested that **security** (and dependability) is best measured by measuring its **operational** system attributes
  - ***Protective metrics***
    - ***System-related metrics***
    - ***Threat-related metrics (effort-based)***
  - ***Behavioural metrics***
- **Protective security** is closest to the essence of **traditional security**