MAFTIA's Interpretation of the IFIP 10.4 Terminology

David Powell

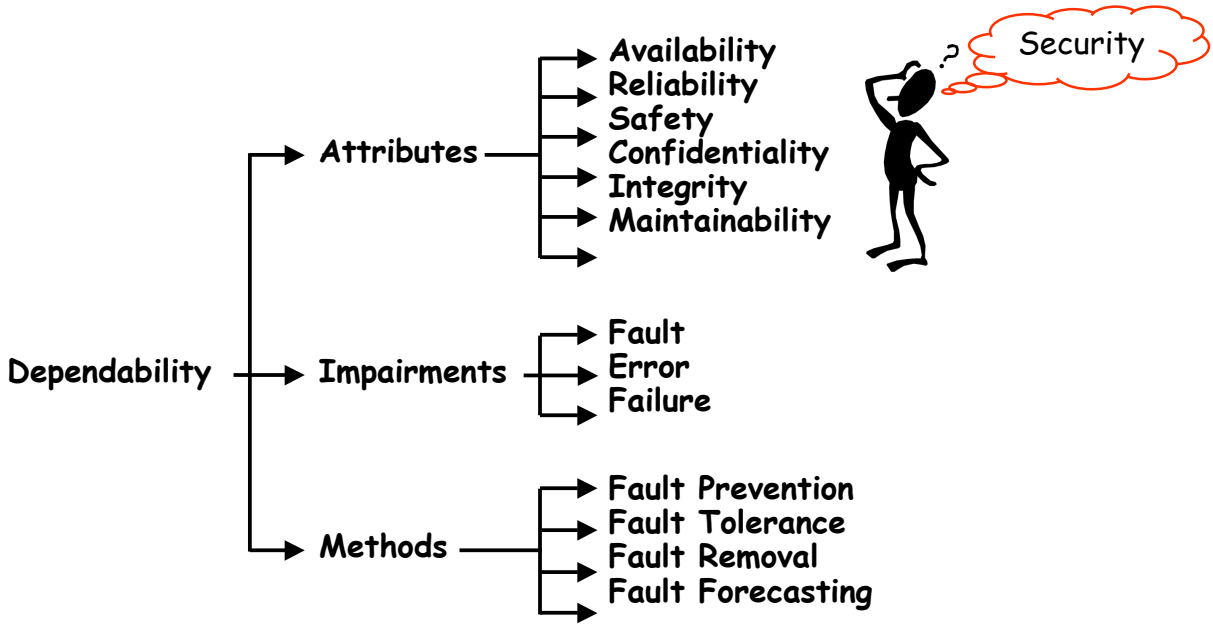
Yves Deswarte
LAAS-CNRS
Toulouse, France
deswarte@laas.fr

Dependability

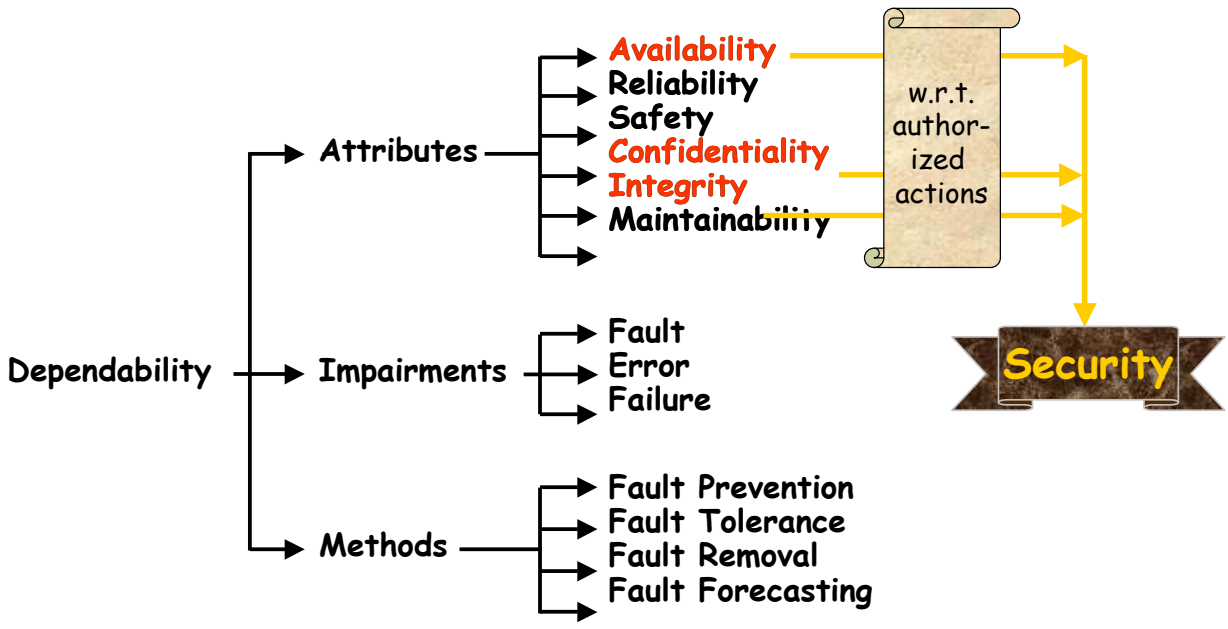
- Trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers

J.-C. Laprie *(Ed.)*, *Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese*, 265p., ISBN 3-211-82296-8, Springer-Verlag, 1992.

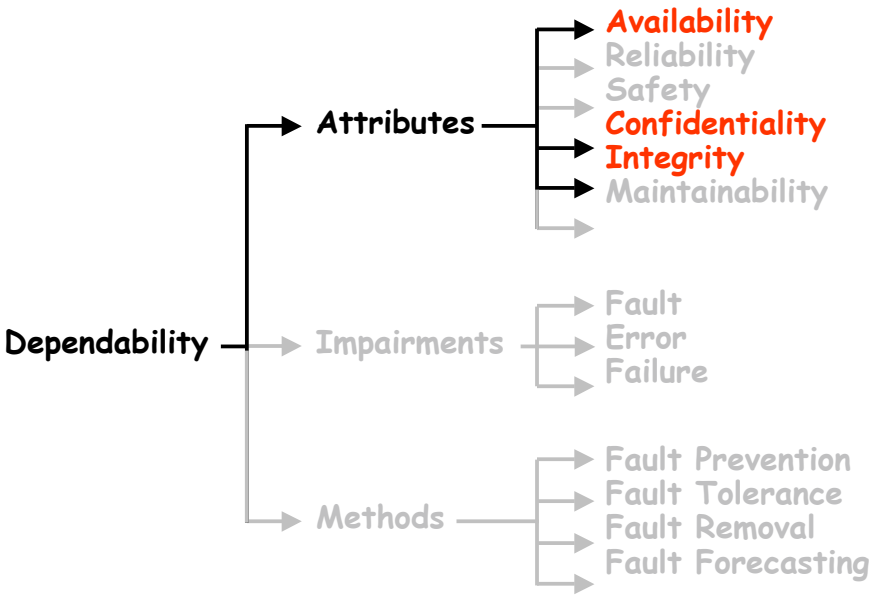
The Dependability Tree



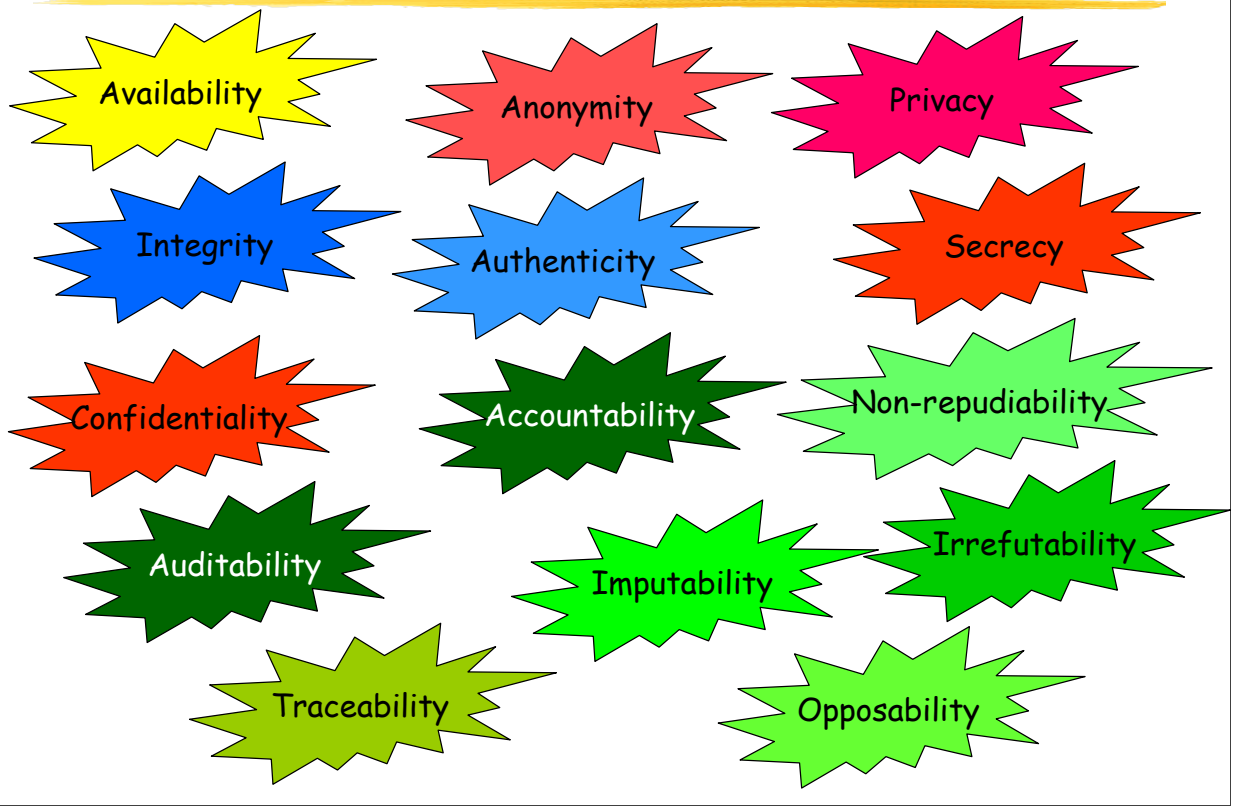
The Dependability Tree



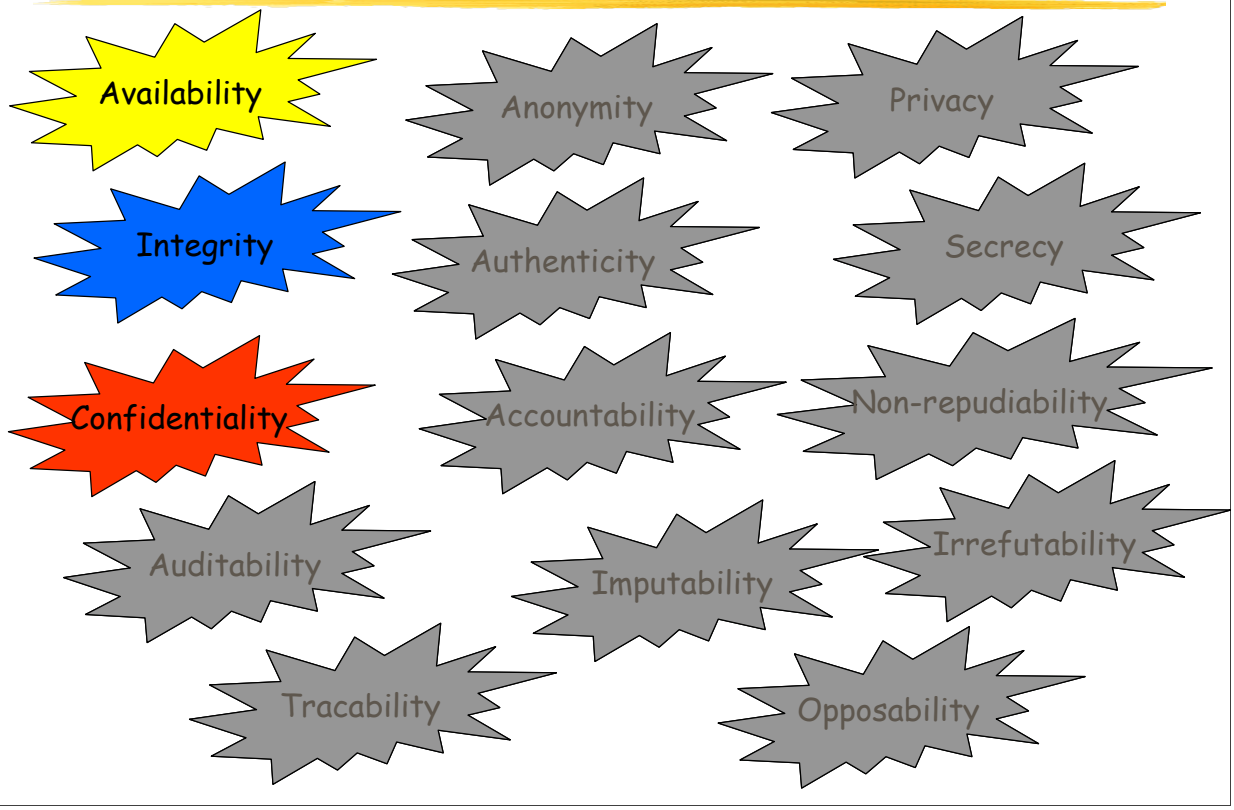
Are these attributes sufficient?



Security Properties



Security Properties



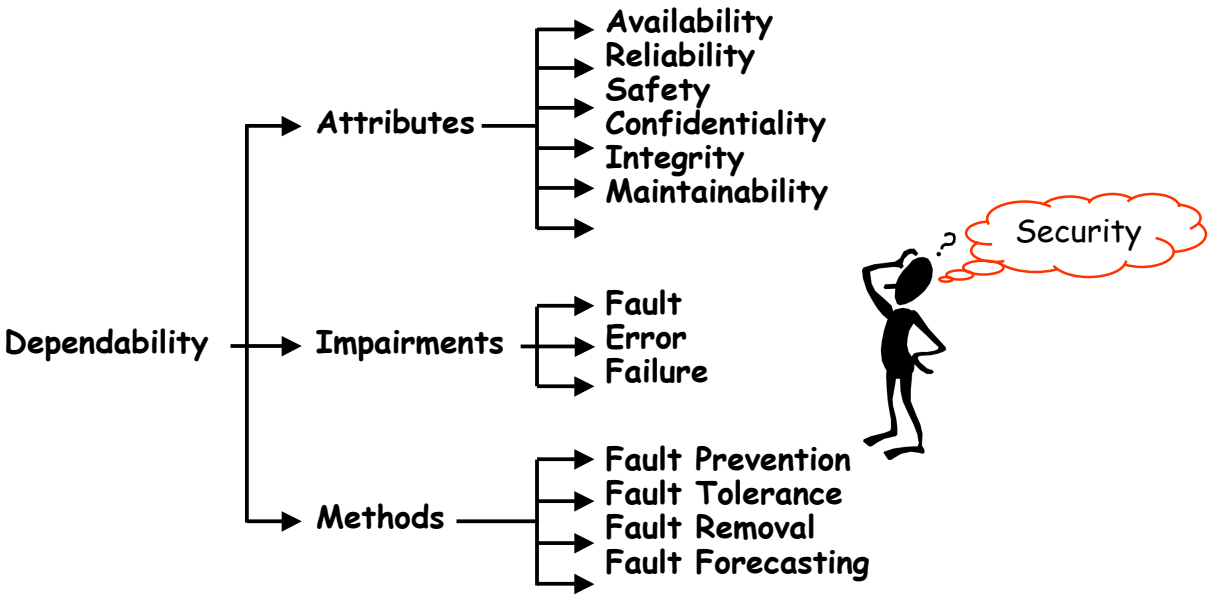
Security Properties

- Confidentiality
- Integrity
- Availability

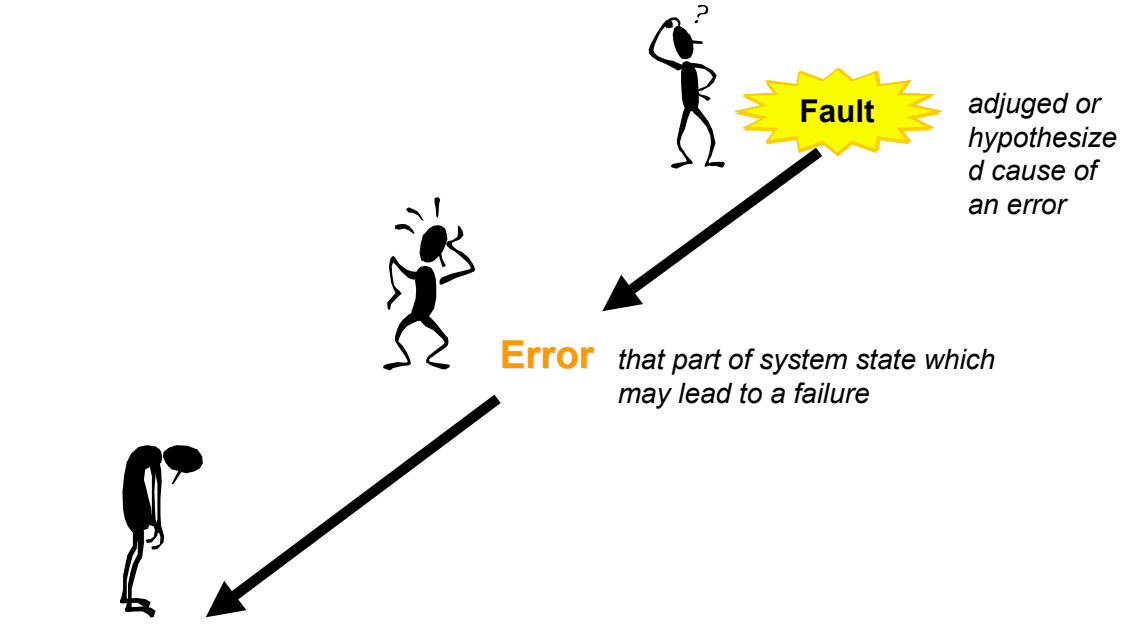
} of { Information, Meta-information

Accountability	*A+I*	• existence of operation • identity of person
Anonymity	*C*	• personal data
Privacy	*C*	• message content
Authenticity	*I*	• message origin
Non-repudiation	*A+I*	• sender, receiver identity

The Dependability Tree

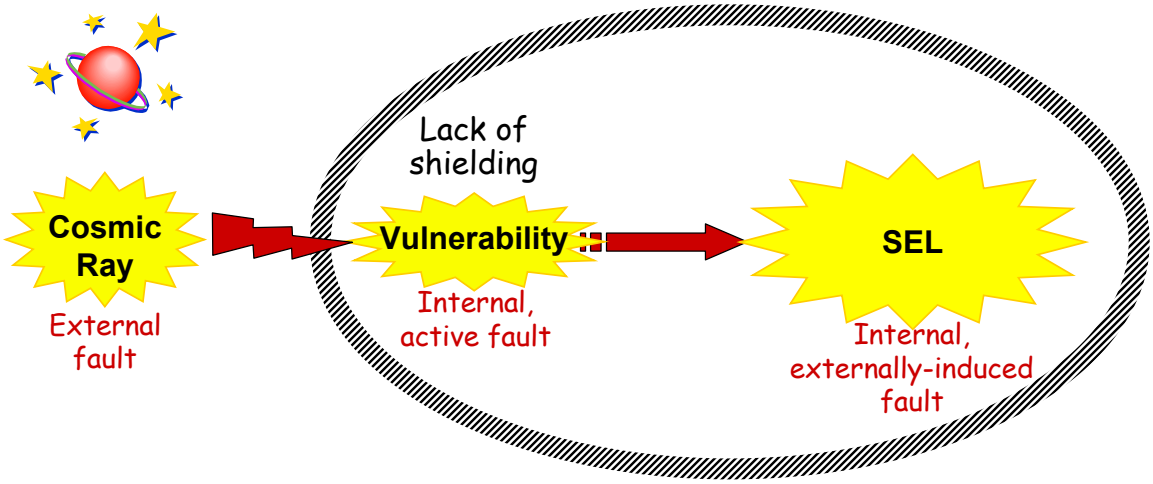


Fault, Error & Failure



Example: Single Event Latchup

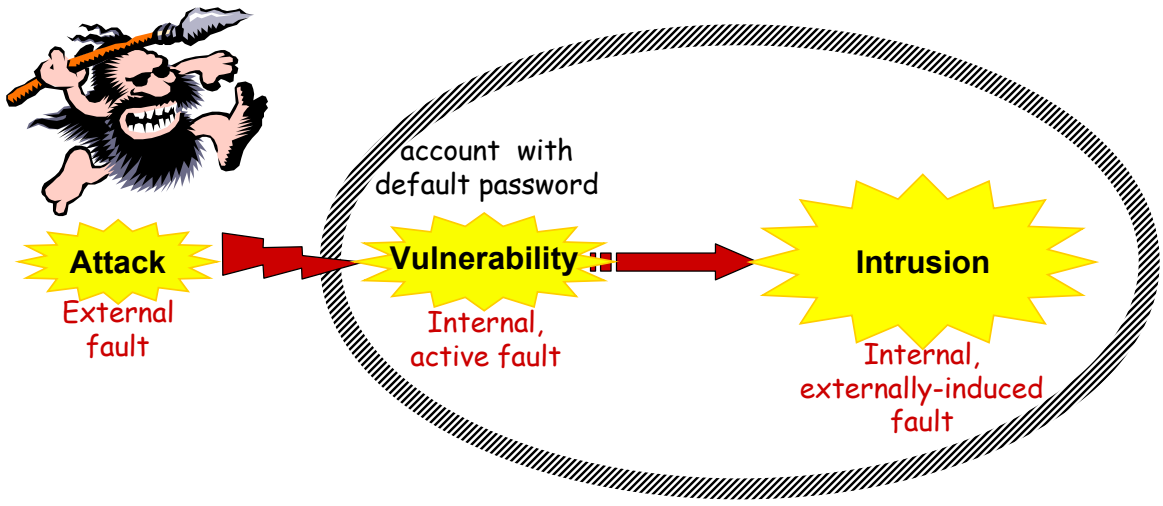
SELs (reversible stuck-at faults)
may occur because of radiation
(e.g., cosmic ray, high energy ions)



Satellite on-board computer

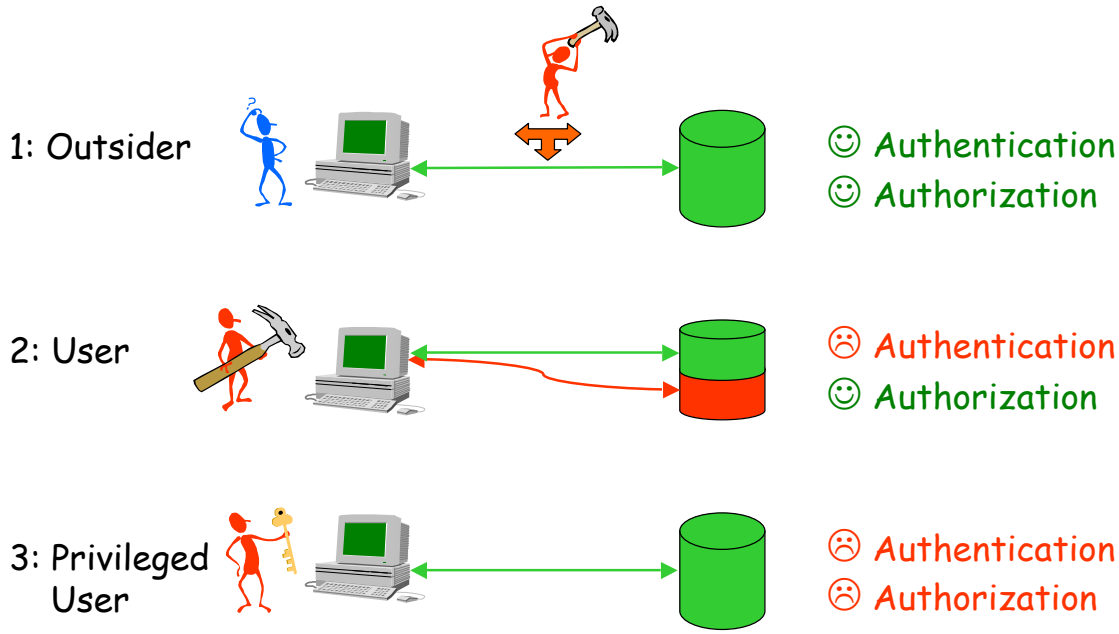
Intrusions

Intrusions result from
(at least partially) successful attacks:



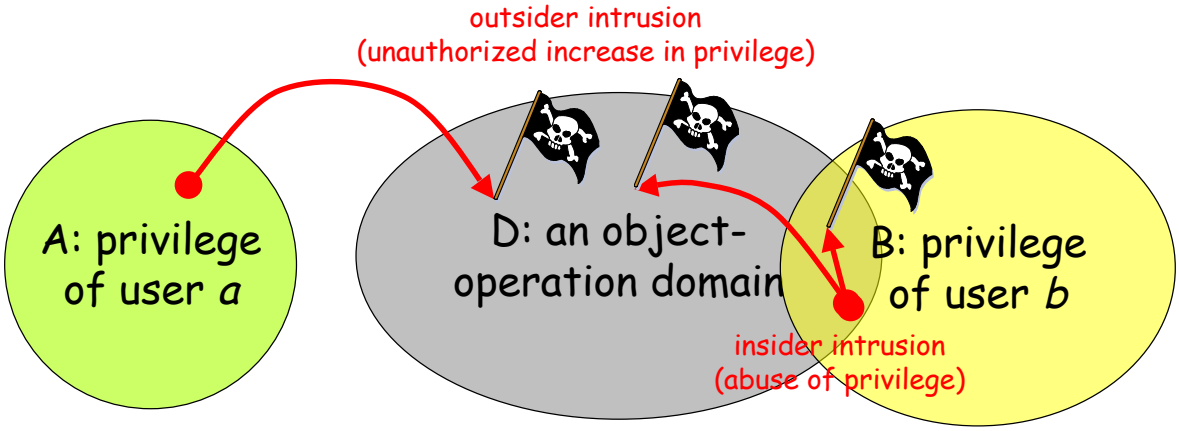
Computing System

Who are the intruders?

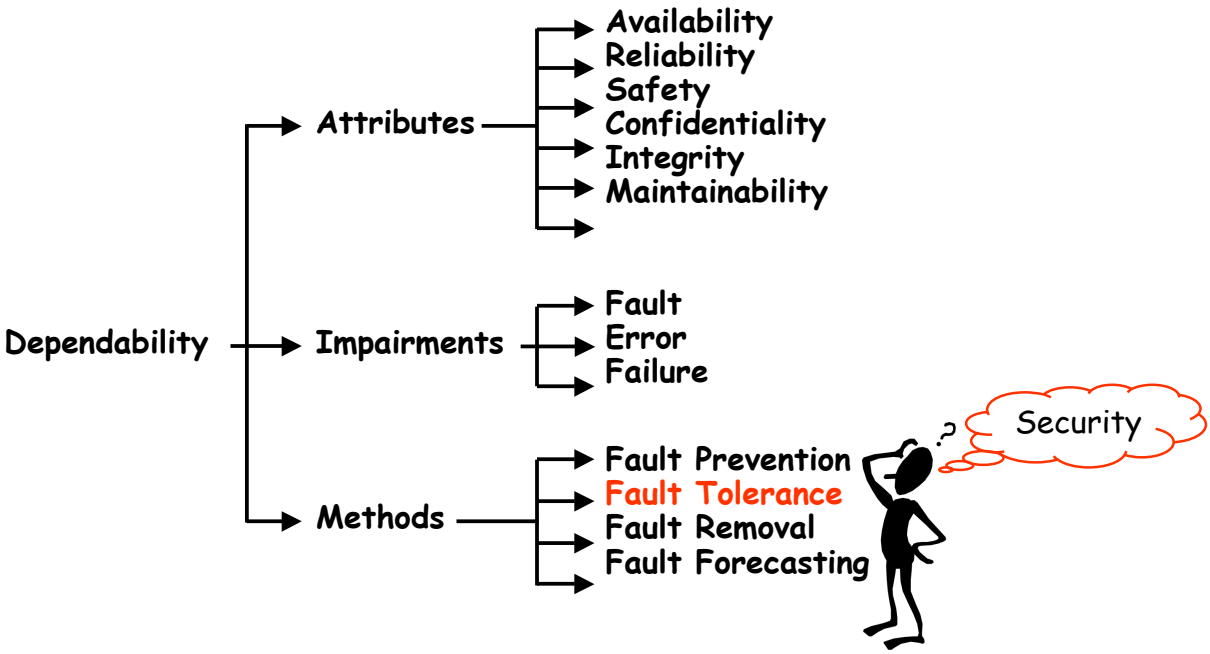


Outsiders vs Insiders

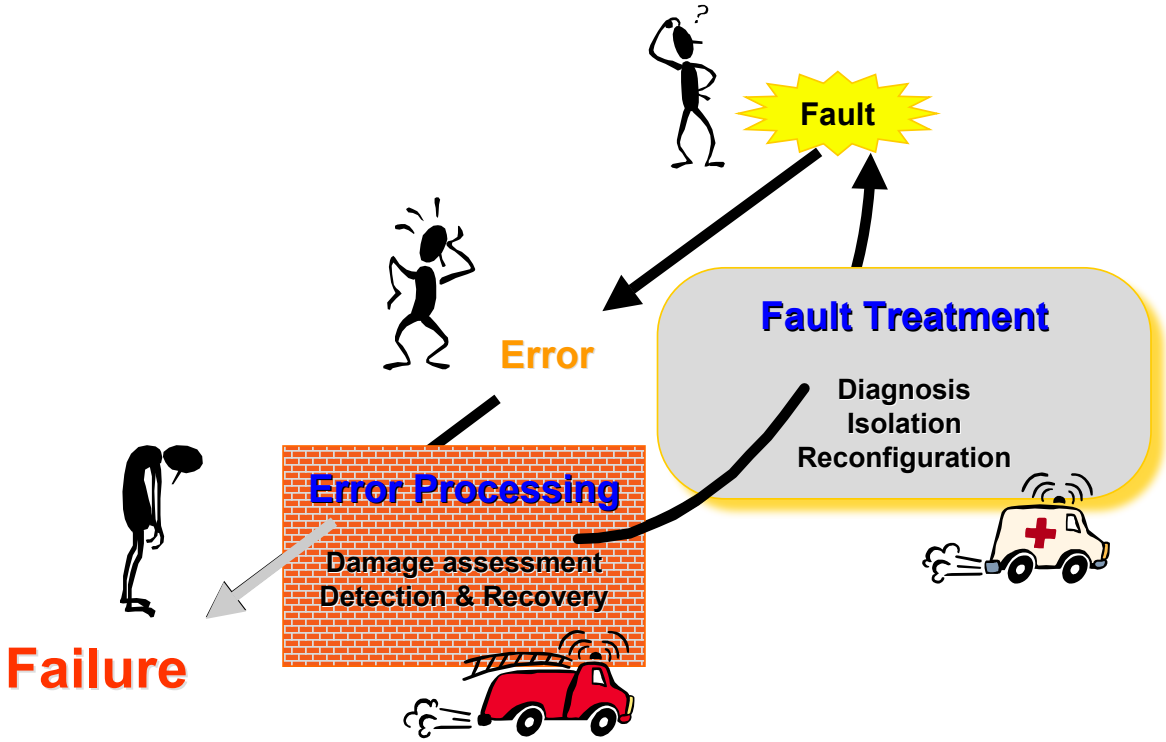
- Outsider: not authorized to perform any of specified object-operations
- Insider: authorized to perform some of specified object-operations



The Dependability Tree

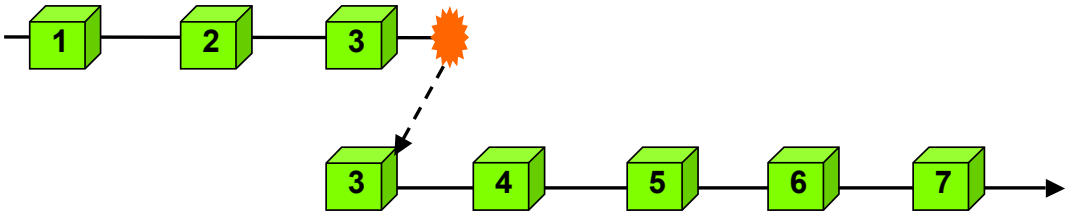


Fault Tolerance



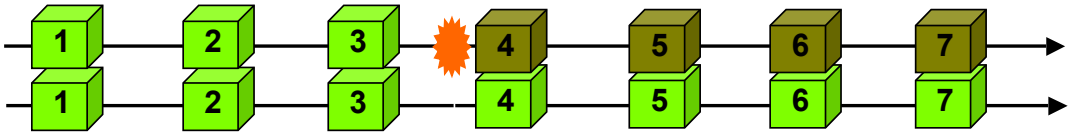
Error Processing

Backward recovery



Forward recovery

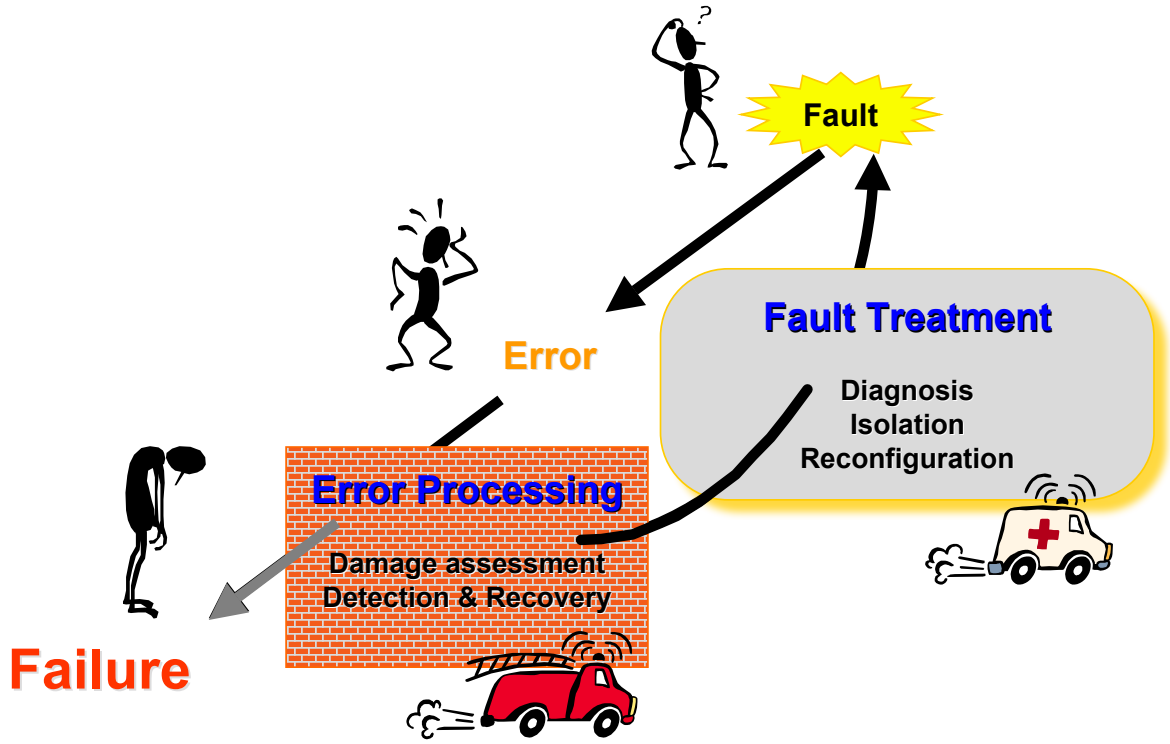
Compensation-based recovery (fault masking)



Error Processing (wrt intrusions)

- Error (security policy violation) detection
  - + Backward recovery (availability, integrity)
  - + Forward recovery (availability, confidentiality)
- Intrusion masking
  - Fragmentation (confidentiality)
  - Redundancy (availability, integrity)
  - Scattering

Fault Tolerance



Fault Treatment

- Diagnosis
  - determine cause of error, i.e., the fault(s)
    - localization
    - nature
- Isolation
  - prevent new activation
- Reconfiguration
  - so that fault-free components can provide an adequate, although degraded, service

Fault Treatment (wrt intrusions)

- Diagnosis
  - Non-malicious or malicious (intrusion)
  - Attack (to allow retaliation)
  - Vulnerability (to allow removal)
- Isolation
  - Intrusion (to prevent further penetration)
  - Vulnerability (to prevent further intrusion)
- Reconfiguration
  - Contingency plan to degrade/restore service
    - inc. attack retaliation, vulnerability removal

http://www.research.ec.org/maftia/

References

- Avizienis, A., Laprie, J.-C., Randell, B. (2001). Fundamental Concepts of Dependability, LAAS Report N°01145, April 2001, 19 p.
- Deswarte, Y., Blain, L. and Fabre, J.-C. (1991). Intrusion Tolerance in Distributed Systems, in *IEEE Symp. on Research in Security and Privacy,* Oakland, CA, USA, pp.110-121.
- Dobson, J. E. and Randell, B. (1986). Building Reliable Secure Systems out of Unreliable Insecure Components, in *IEEE Symp. on Security and Privacy,* Oakland, CA, USA, pp.187-193.
- Laprie, J.-C. (1985). Dependable Computing and Fault Tolerance: Concepts and Terminology, in *15th Int. Symp. on Fault Tolerant Computing (FTCS-15),* Ann Arbor, MI, USA, IEEE, pp.2-11.
- J.-C. Laprie (Ed.), Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese, 265p., ISBN 3-211-82296-8, Springer-Verlag, 1992.
- D. Powell, A. Adelsbasch, C. Cachin, S. Creese, M. Dacier, Y. Deswarte, T. McCutcheon, N. Neves, B. Pfitzmann, B. Randell, R. Stroud, P. Veríssimo, M. Waidner. MAFTIA (Malicious- and Accidental-Fault Tolerance for Internet Applications), *Sup. of the 2001 International Conference on Dependable Systems and Networks (DSN2001)*, Göteborg (Suède), 1-4 juillet 2001, IEEE, pp. D-32-D-35.