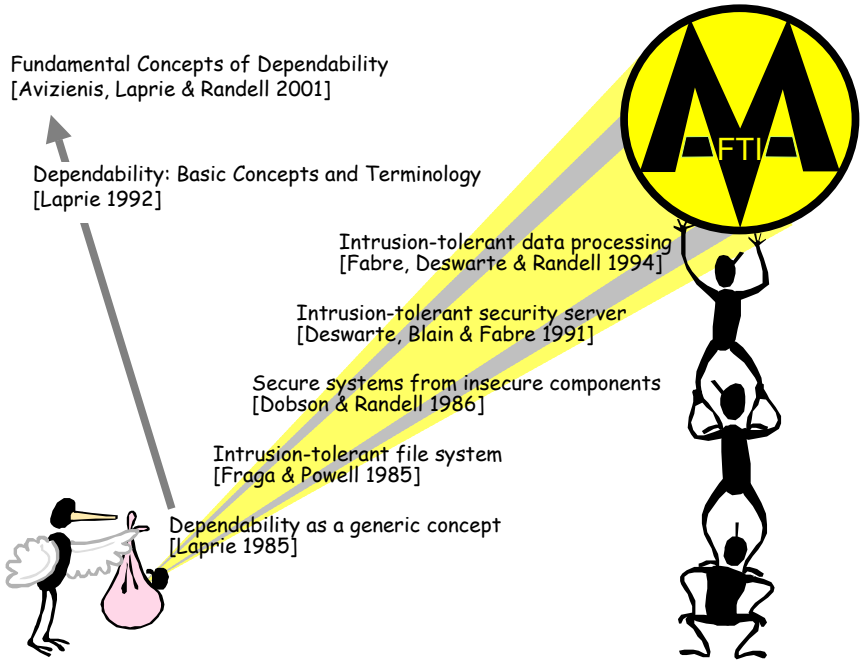
MAFTIA:
a European project for dependable Internet applications despite intrusions and accidental faults

David Powell

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



MAFTIA

IST Dependability Initiative
Cross Program Action 2
Dependability in services and technologies

- Malicious- and Accidental-Fault Tolerance for Internet Applications

University of Newcastle (UK)	Brian Randell, Robert Stroud
University of Lisbon (P)	Paulo Verissimo
DERA, Malvern (UK)	Tom McCutcheon, Colin O'Halloran
University of Saarland (D)	Birgit Pfitzmann
LAAS-CNRS, Toulouse (F)	Yves Deswarte, David Powell
IBM Research, Zurich (CH)	Marc Dacier, Michael Waidner

c. 55 man-years, EU funding c. 2.5M€
Jan. 2000 -> Dec. 2002

Industrial Advisory Board

- Andrew Izon (North Durham NHS Trust, GB)
- Jean-Claude Lebraud (Rockwell-Collins, F)
- Derek Long (CISA Ltd., GB)
- Joachim Posegga (SAP Systems, D)
- Carlos Quintas (Easyphone, P)
- Gilles Trouessin (Ernst & Young Audit, F)
- Gritta Wolf (Credit Suisse, CH)

Objectives

- Architectural framework and conceptual model (WP1)
- Mechanisms and protocols:
  - dependable middleware (WP2)
  - large scale intrusion detection systems (WP3)
  - dependable trusted third parties (WP4)
  - distributed authorization mechanisms (WP5)
- Validation and assessment techniques (WP6)

Authorisaton

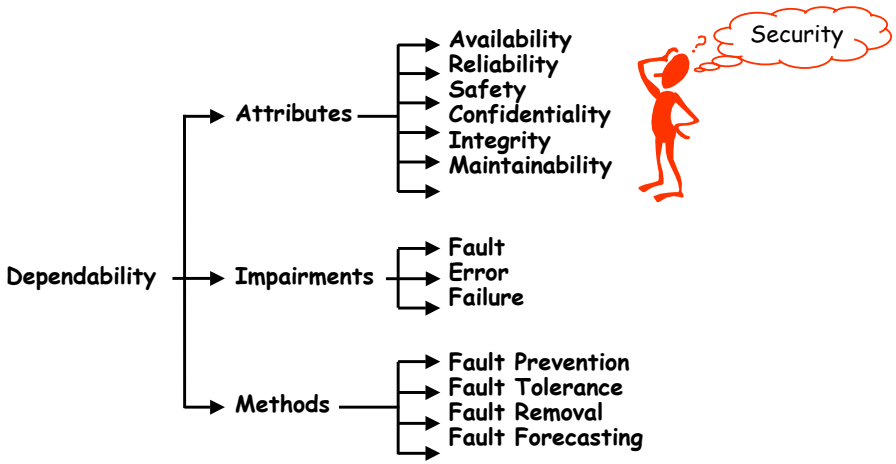
- Contributes to protection:
  - Error detection/confinement
  - Intrusion prevention/confinement
- For Internet applications:
  - More flexible than "client-server" paradigm
  - Contributes to privacy:
    personal information is disclosed only on a "need-to-know" basis

Dependability

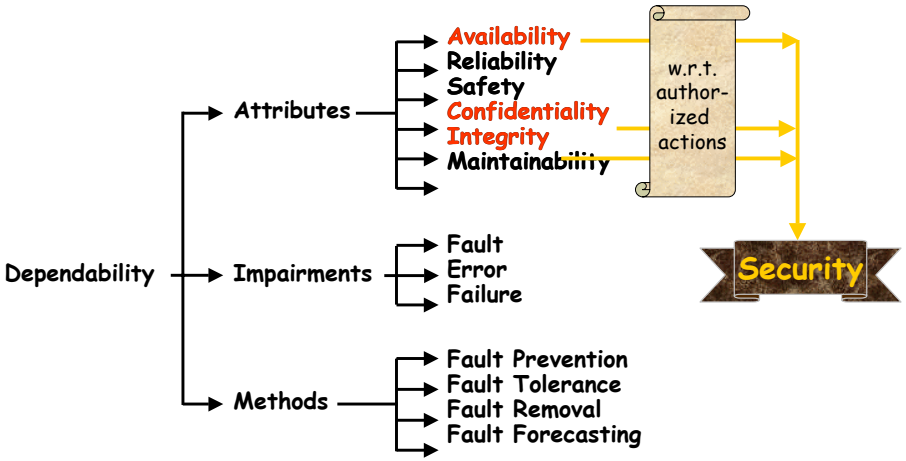
- Trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers

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.

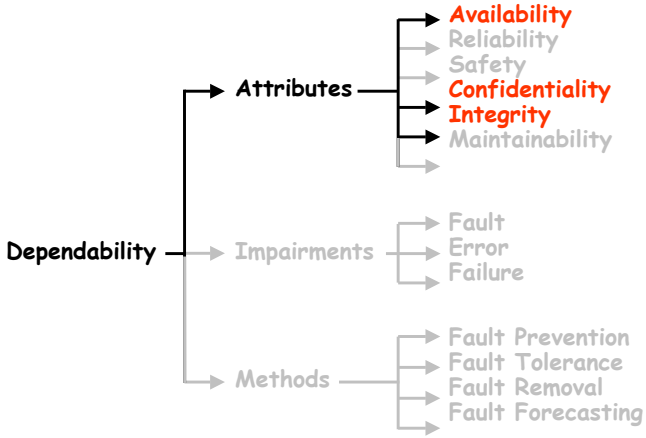
The Dependability Tree



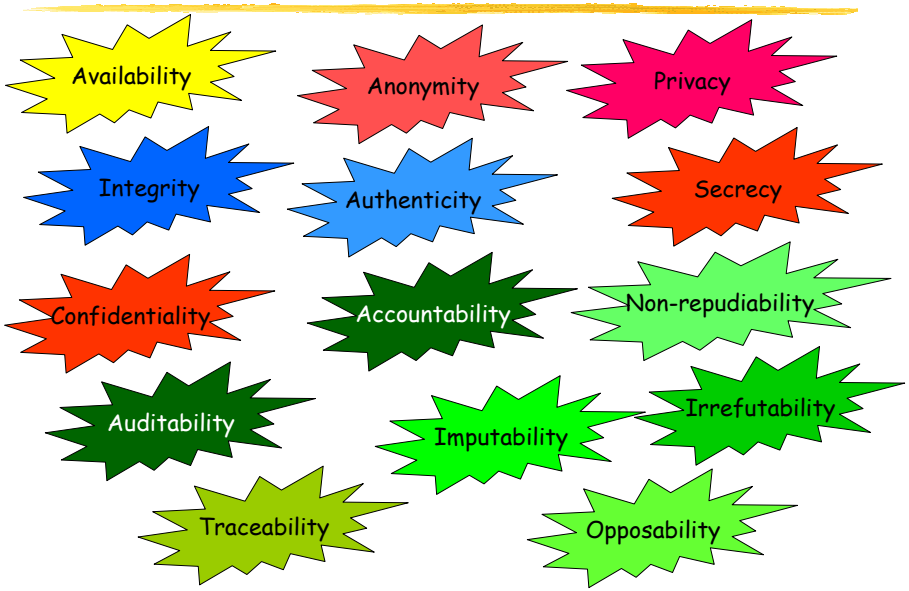
The Dependability Tree



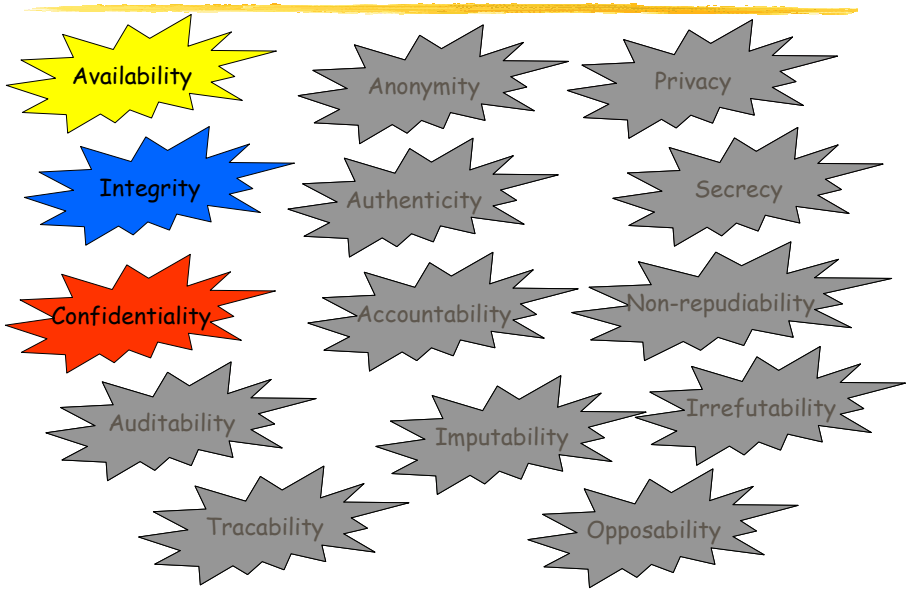
Are these attributes sufficient?



Security Properties



Security Properties



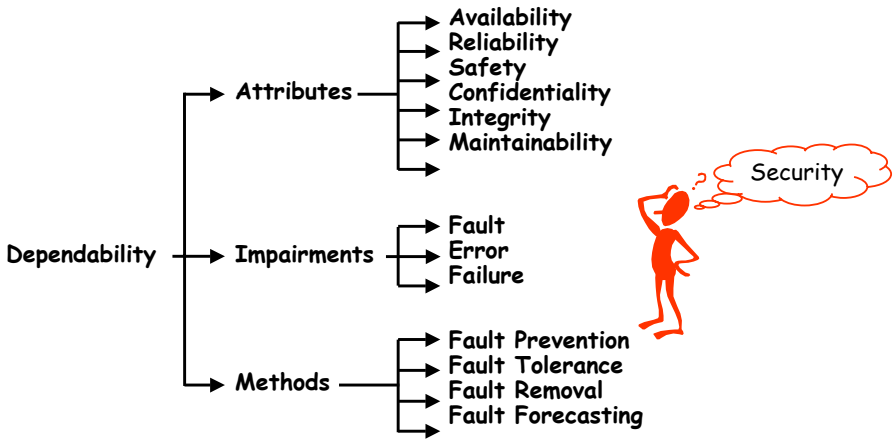
Security Properties

- Confidentiality
- Integrity
- Availability

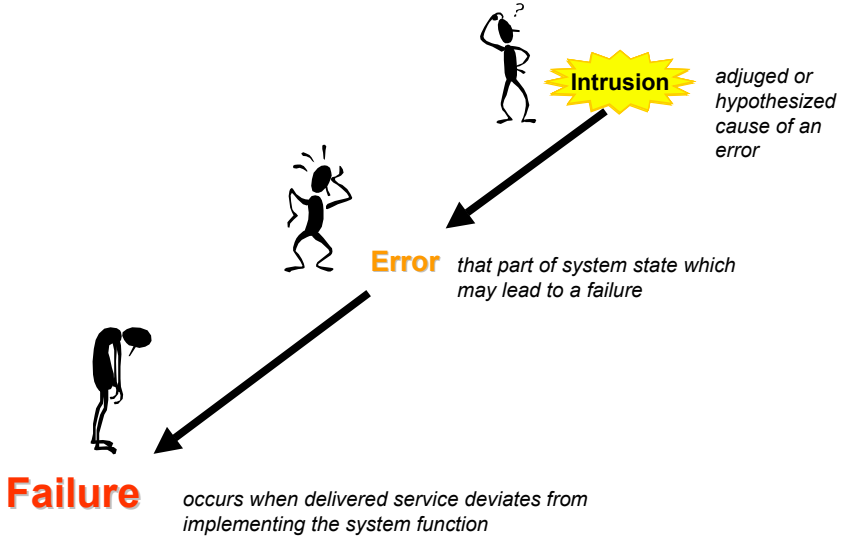
} of { Information, Meta-information

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

The Dependability Tree

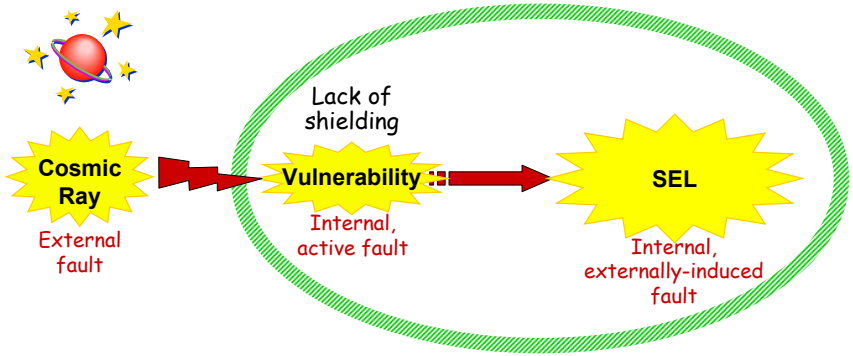


Fault, Error & Failure



Example: Single Event Latchup

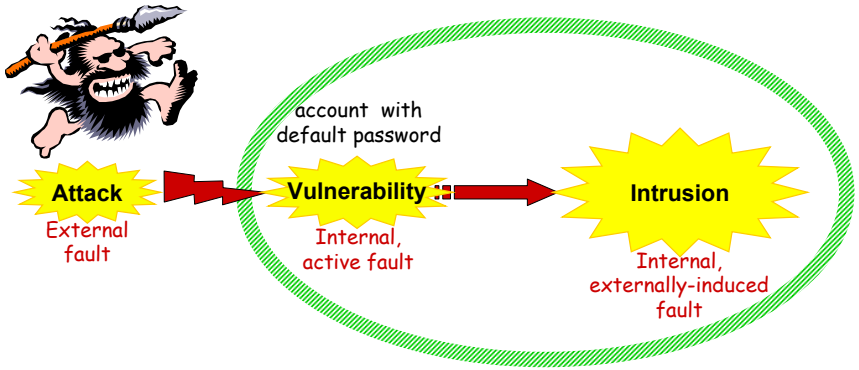
SELs (reversible stuck-at faults) may occur because of radiation (e.g., cosmic ray, high energy ions)



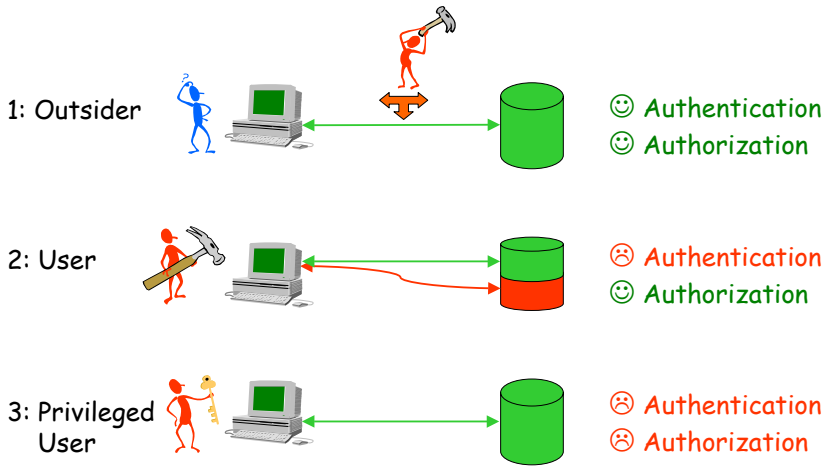
Satellite on-board computer

Intrusions

Intrusions result from
(at least partially) successful attacks:



Who are the intruders?

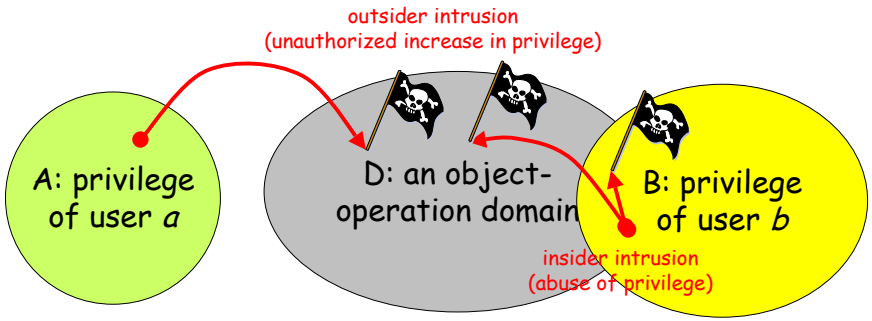


Insiders or Outsiders ?

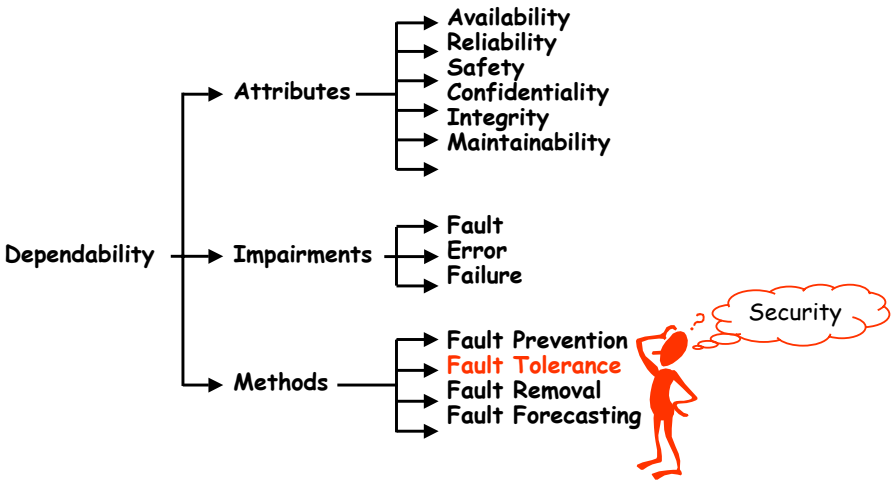
- 01 Informatique 1998
  - 1200 companies in 32 countries
  - 66% experienced fraud in last 12 months
    - 85% by company employees
- Computer Crime and Security Survey 2001
  (Computer Security Institute and the FBI)
  http://www.gocsi.com/prelea_000321.htm
  - 91% of respondent reported employee abuse of Internet (79% in 2000)
  - but decreasing proportion of disgruntled employees: 76% (82% in 2000)
  - 70% cite Internet as a frequent point of attack (59%)

Outsiders vs Insiders

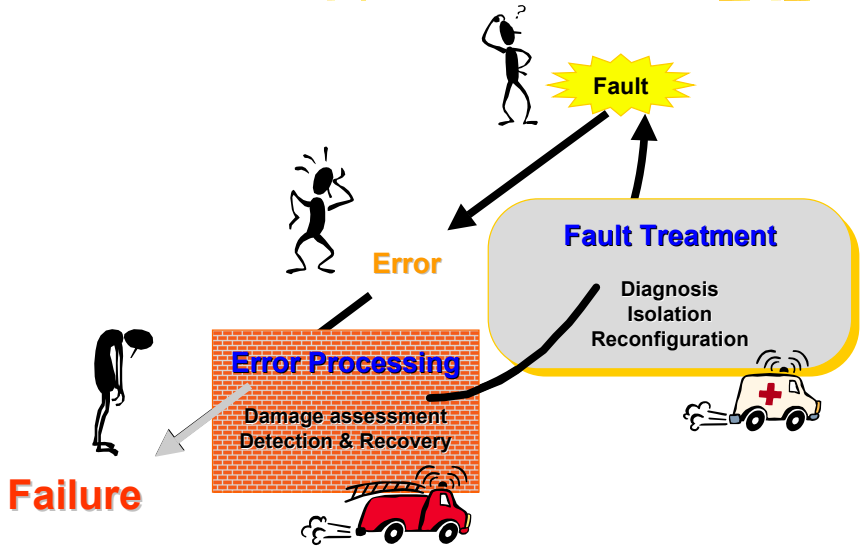
- Outsider: not authorized to perform any of specified object-operations
- Insider: authorized to perform some of specified object-operations



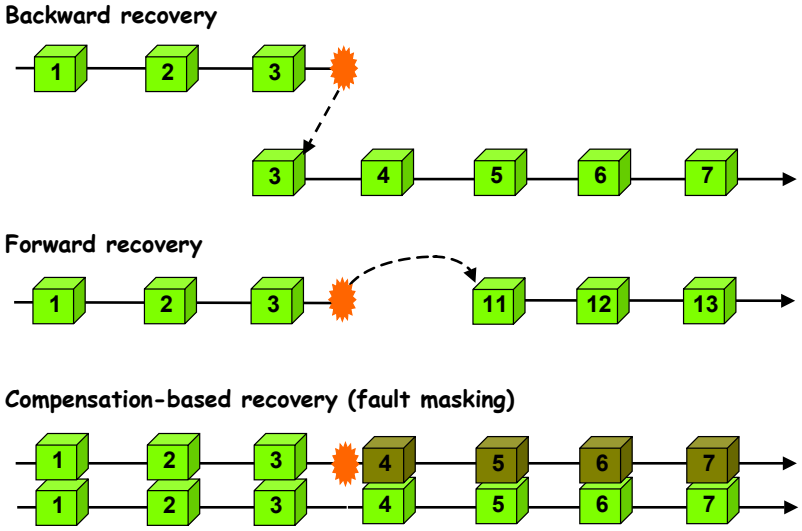
The Dependability Tree



Fault Tolerance



Error Processing



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

Intrusion Masking

Intrusion into a part of the system should give access only to non-significant information

FRS: Fragmentation-Redundancy-Scattering

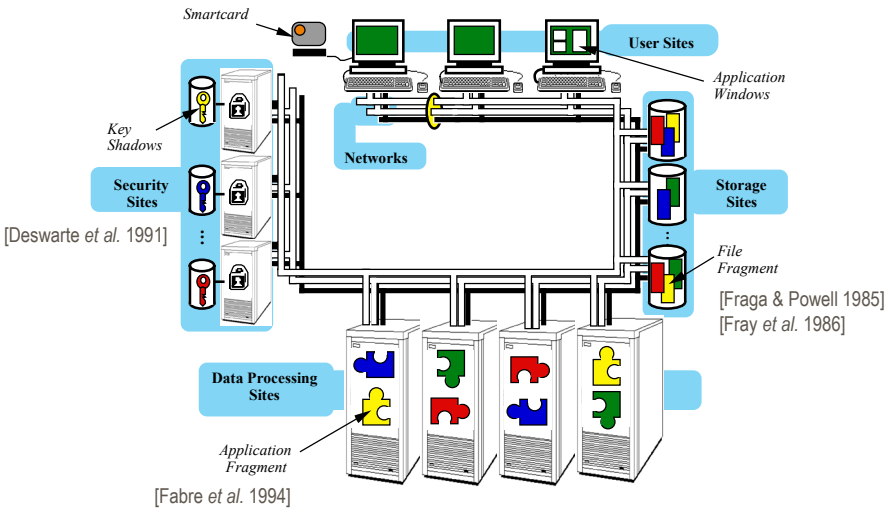
- Fragmentation: split the data into fragments so that isolated fragments contain no significant information: *confidentiality*
- Redundancy: add redundancy so that fragment modification or destruction would not impede legitimate access: *integrity + availability*
- Scattering: isolate individual fragments

Different kinds of scattering

- Space: use different transmission links and different storage sites
- Time: mix fragments (from the same source, from different sources, with jamming)
- Frequency: use different carrier frequencies (spread-spectrum)
- Privilege: require the co-operation of differently privileged entities to realise an operation (separation of duty, secret sharing)

Prototype

[Blain & Deswarte 1994]

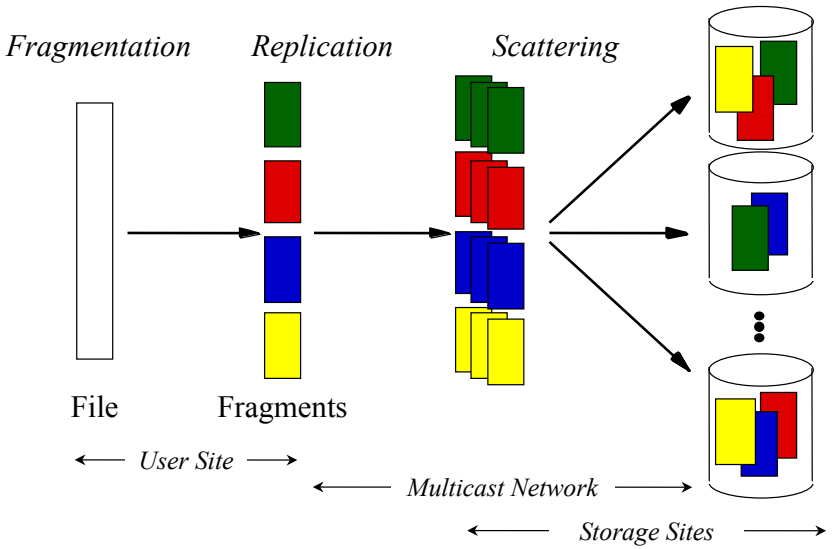


[Deswarte *et al.* 1991]

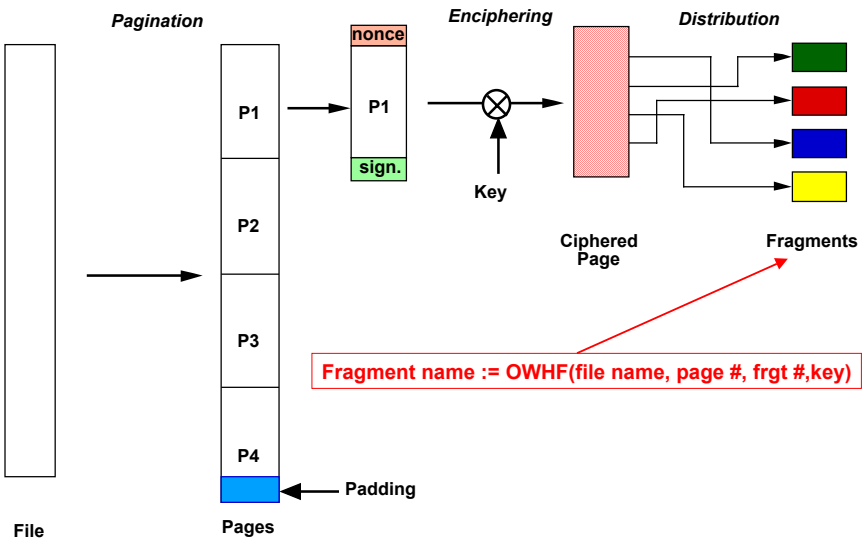
[Fraga & Powell 1985]
[Fray *et al.* 1986]

[Fabre *et al.* 1994]

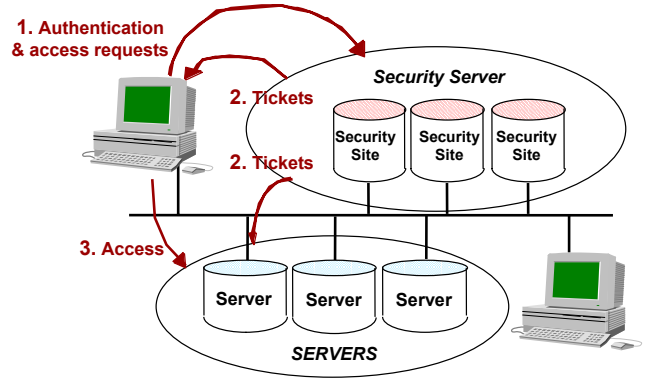
FRSed File Server



File Fragmentation

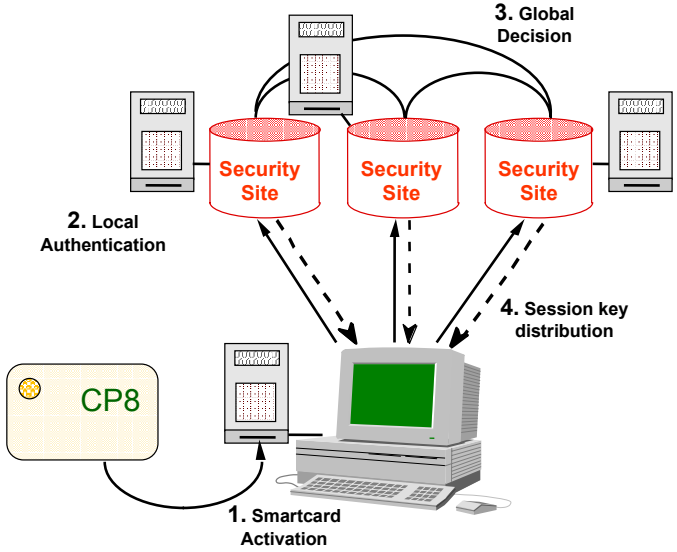


FRSed Security Management

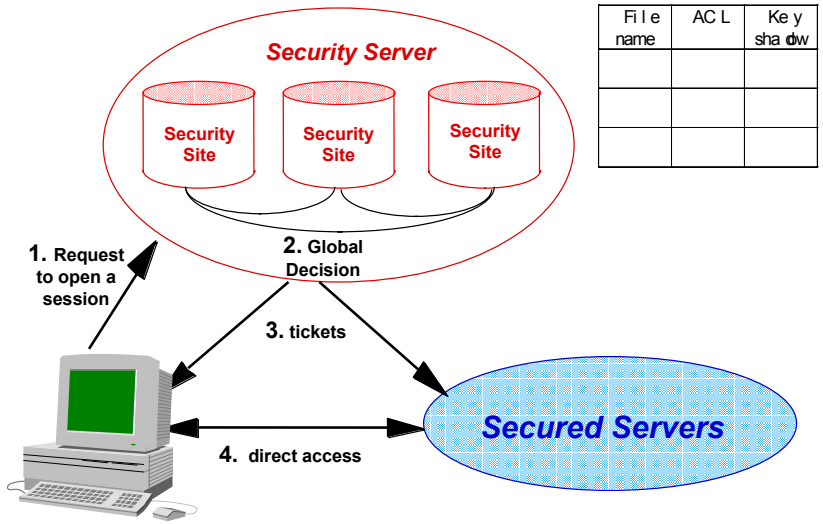


- No single trusted site or administrator
- Global trust in a majority of security sites (and administrators)

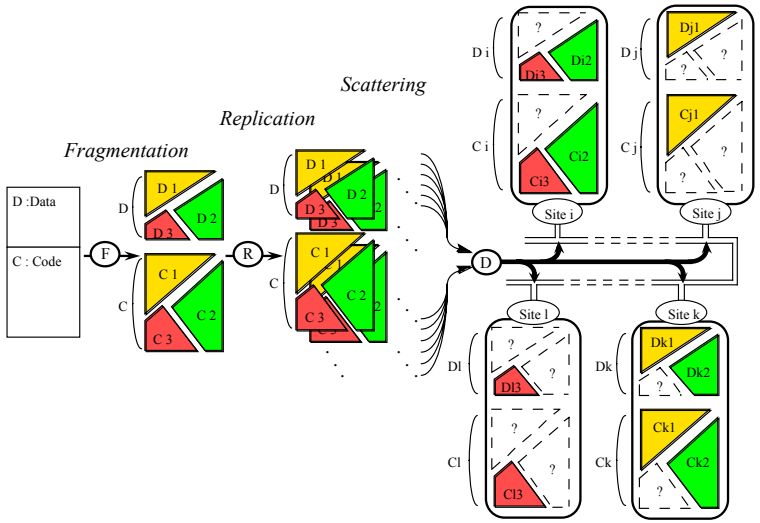
Authentication



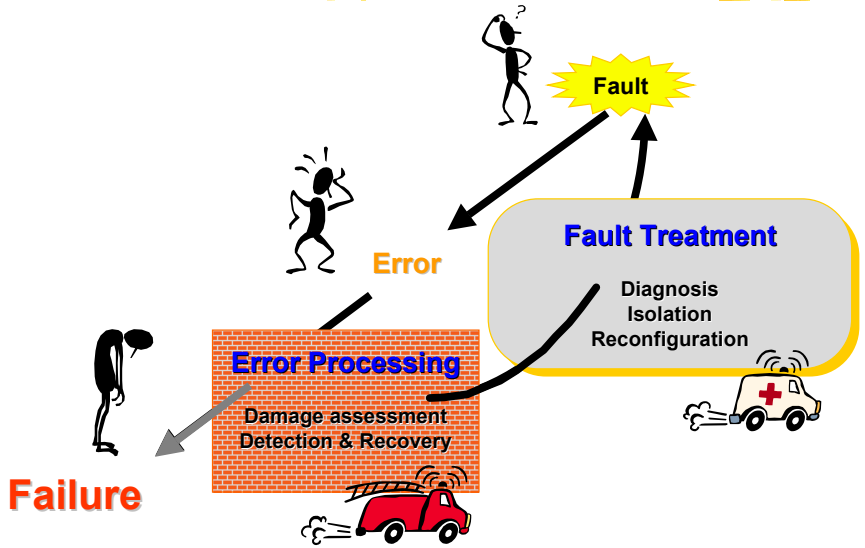
Authorization



Fragemented Data Processing



Fault Tolerance

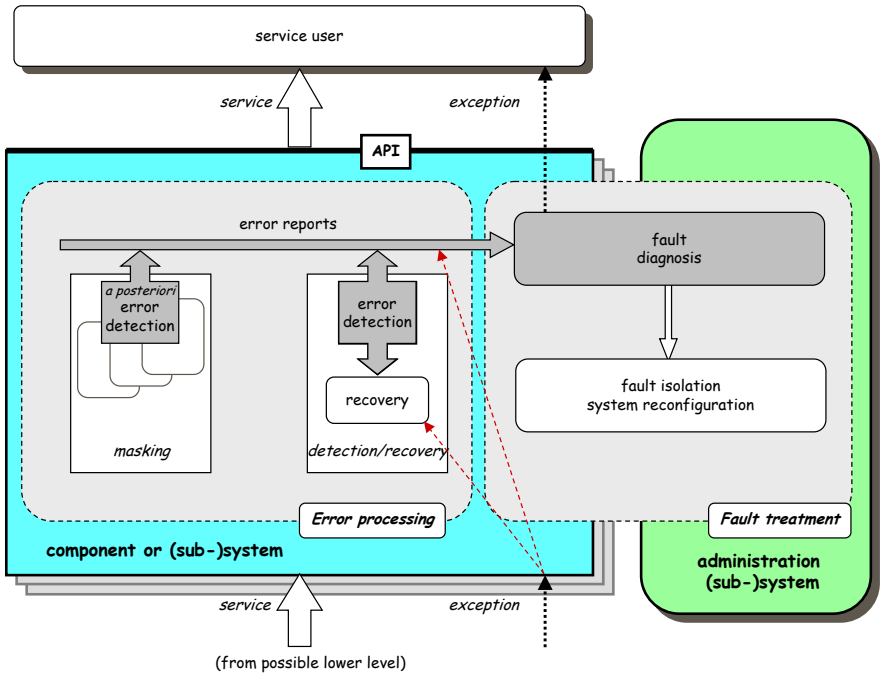


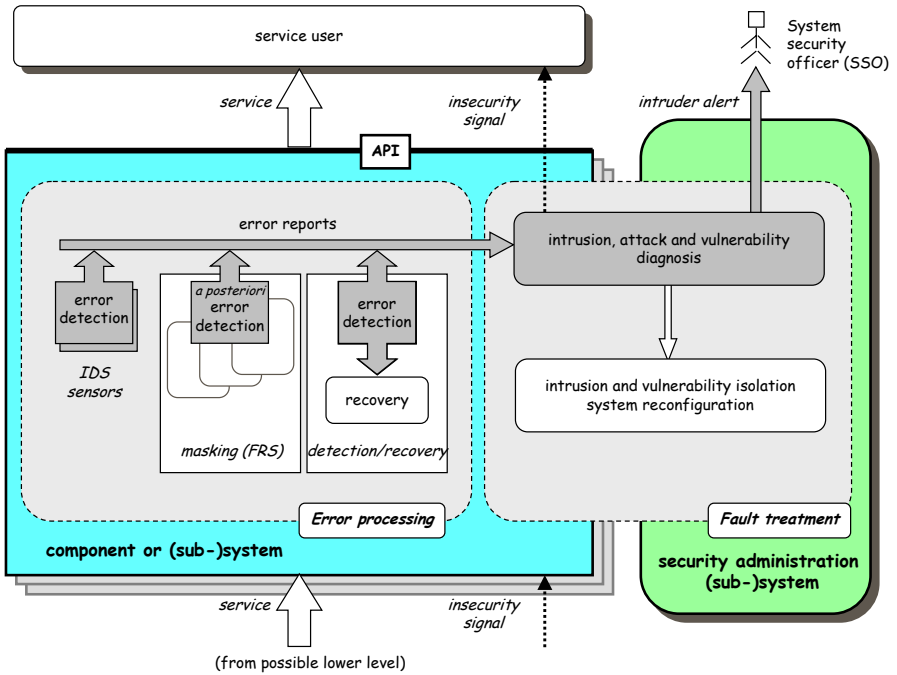
Fault Treatment

- 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/

Authorisation

References

- Avizienis, A., Laprie, J.-C., Randell, B. (2001). Fundamental Concepts of Dependability, LAAS Report N°01145, April 2001, 19 p.
- Blain, L. and Deswarte, Y. (1994). A Smartcard Fault-Tolerant Authentication Server, in *1st Smart Card Research and Advanced Application Conference (CARDIS'94),* Lille, France, pp.149-165.
- 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.
- Deswarte, Y., Fabre, J.-C., Laprie, J.-C. and Powell, D. (1986). A Saturation Network to Tolerate Faults and Intrusions, in *5th Symp. on Reliability of Distributed Software and Database Systems (SRDS-5),* Los Angeles, CA, USA, pp.74-81, IEEE Computer Society Press.
- 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.
- Fabre, J.-C., Deswarte, Y. and Randell, B. (1994). Designing Secure and Reliable Applications using FRS: an Object-Oriented Approach, in *1st European Dependable Computing Conference (EDCC-1),* Berlin, Germany LNCS 852, pp.21-38.
- Fraga, J. and Powell, D. (1985). A Fault and Intrusion-Tolerant File System, in *IFIP 3rd Int. Conf. on Computer Security (IFIP/Sec'85),* (J. B. Grimson and H.-J. Kugler, Eds.), Dublin, Ireland, Computer Security, pp.203-218.
- Fray, J.-M., Deswarte, Y. and Powell, D. (1986). Intrusion-Tolerance using Fine-Grain Fragmentation-Scattering, in *IEEE Symp. on Security and Privacy,* Oakland, CA, USA, pp.194-201.
- 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.