On Dependability Concepts with respect to Deliberately Malicious Faults

David Powell & Yves Deswarte

IX Brazilian Symposium on Fault-Tolerant Computing (SCTF)
Florianópolis/SC , 5-7 March 2001

IST Dependability Initiative

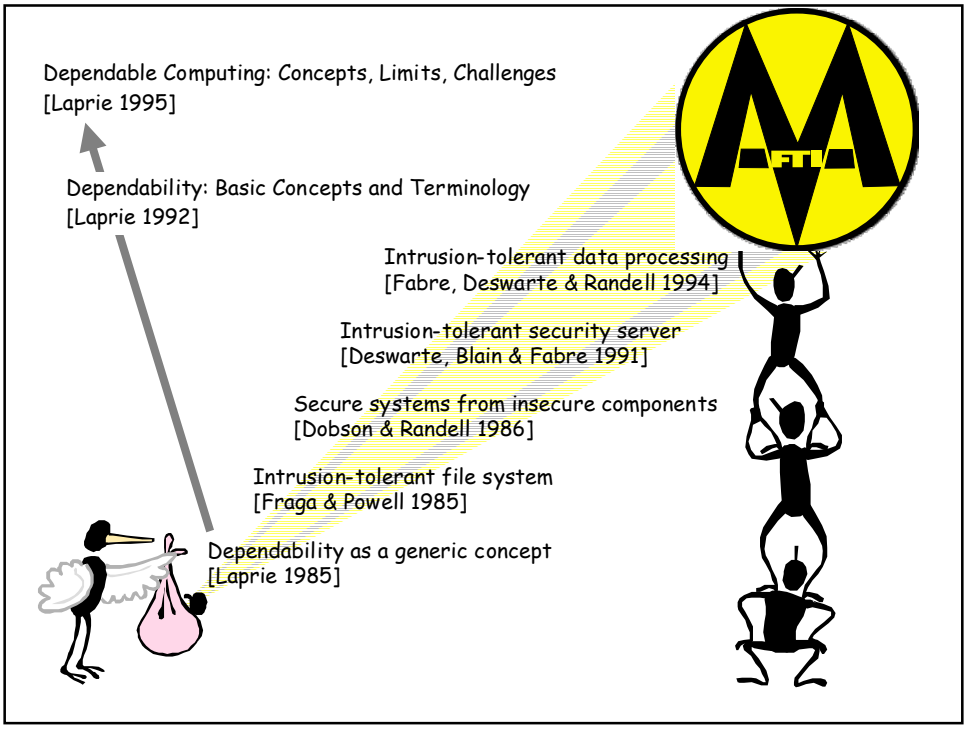
MAFTIA

Malicious- and Accidental-Fault Tolerance for Internet Applications

University of Newcastle (UK)
University of Lisbon (P)
DERA, Malvern (UK)
University of Saarland (D)
LAAS-CNRS, Toulouse (F)
IBM Research, Zurich (CH)

c. 45 man-years, c. 2.5M euro

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

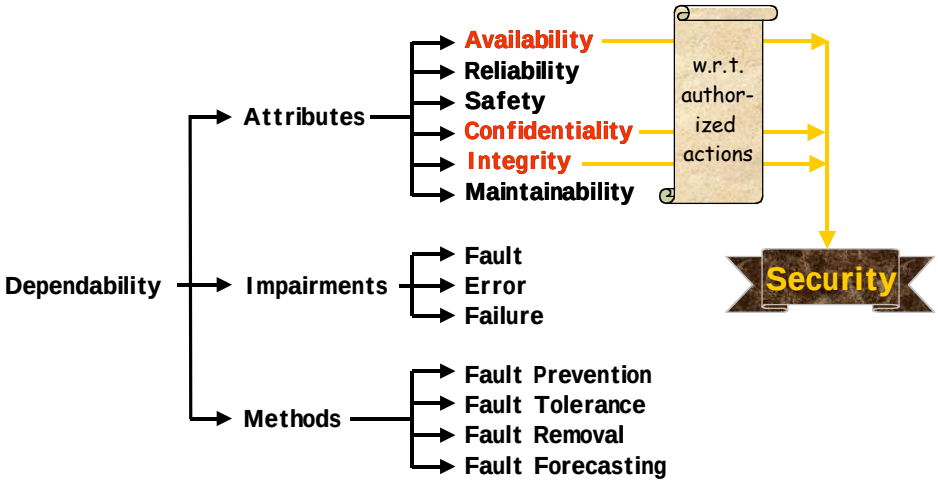


Dependability

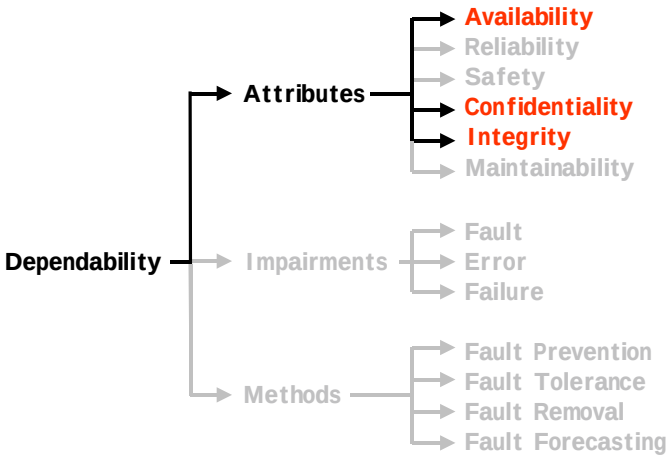
- Property of a computer system such that reliance can justifiably be placed on the service it delivers

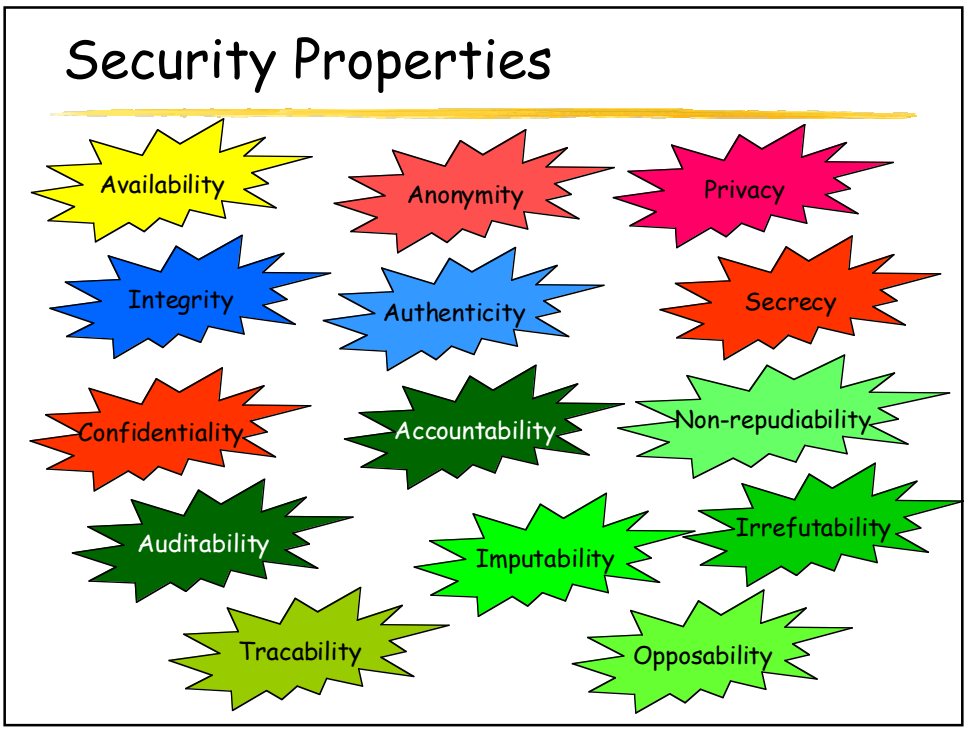
J.-C. Laprie *et al.*, *Guide de la sûreté de fonctionnement*, 324p., ISBN 2-85428-382-1, Cépaduès-Editions, Toulouse, 1995.

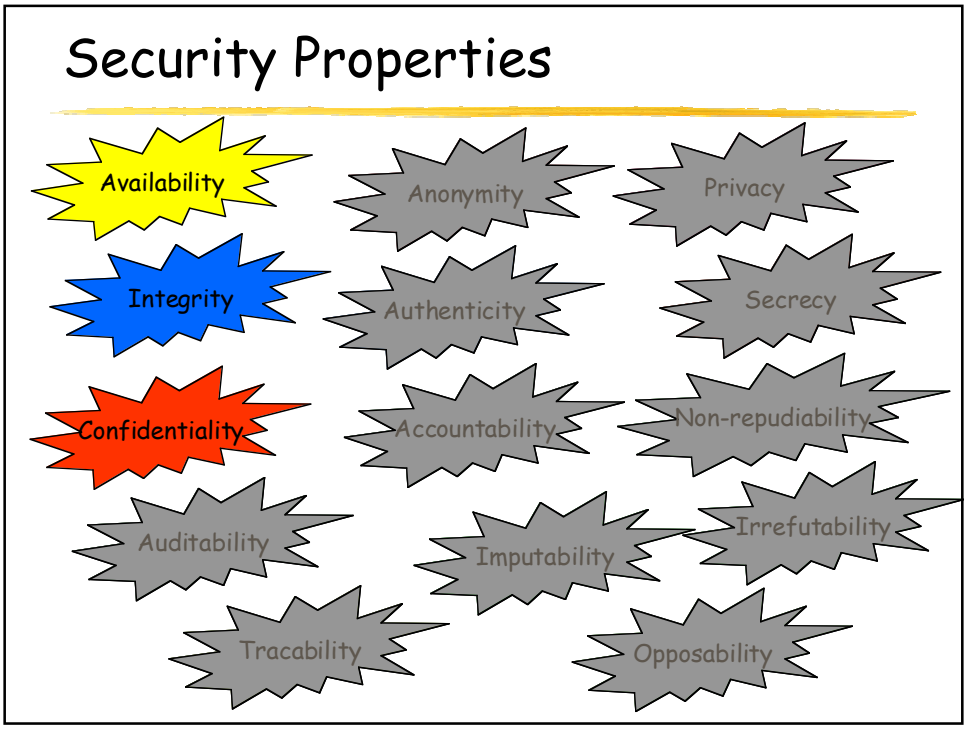
The Dependability Tree



Are these attributes sufficient?




Security Properties
Availability
Anonymity
Privacy
Integrity
Authenticity
Secrecy
Confidentiality
Accountability
Non-repudiability
Auditability
Imputability
Irrefutability
Tracability
Opposability


Security Properties
Availability
Anonymity
Privacy
Integrity
Authenticity
Secrecy
Confidentiality
Accountability
Non-repudiability
Auditability
Imputability
Irrefutability
Tracability
Opposability

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
		• message origin
Non-repudiation	*A+I*	• sender, receiver identity

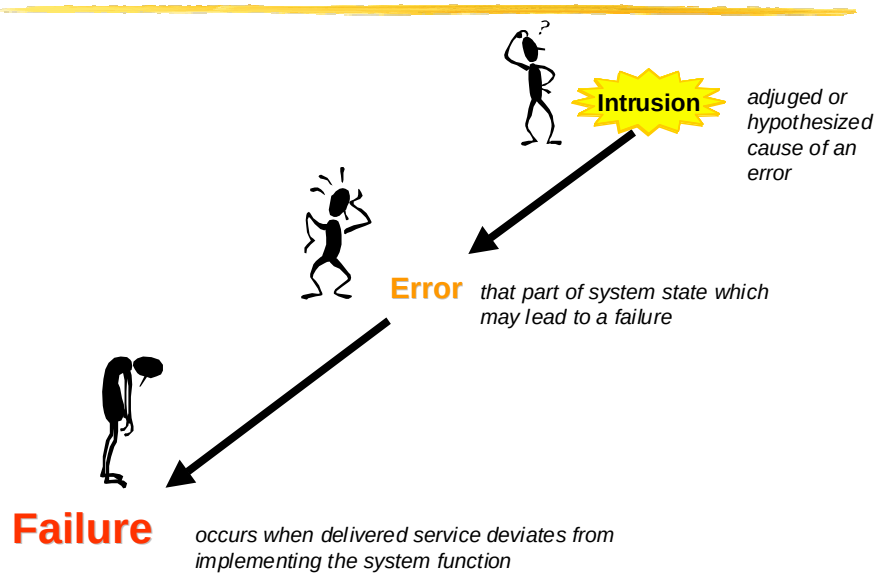
Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- Loss of Confidentiality
- Security Guarantees
- Intrusion Tolerance

Intrusion-Tolerance Concepts

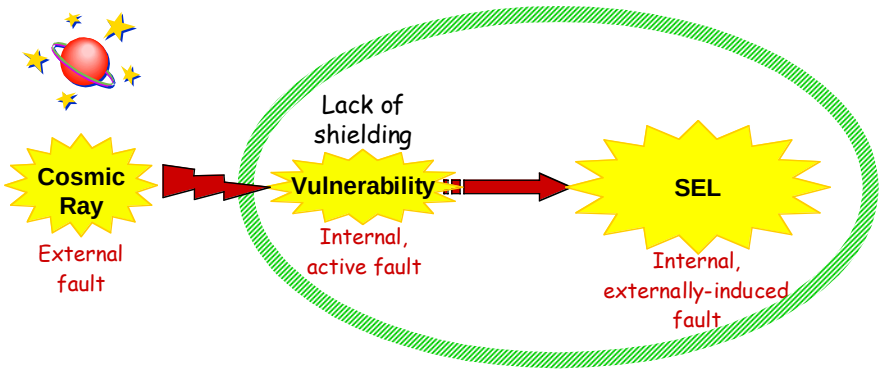
- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- Loss of Confidentiality
- Security Guarantees
- Intrusion Tolerance

Fault, Error & Failure



Example: Single Event Latchup

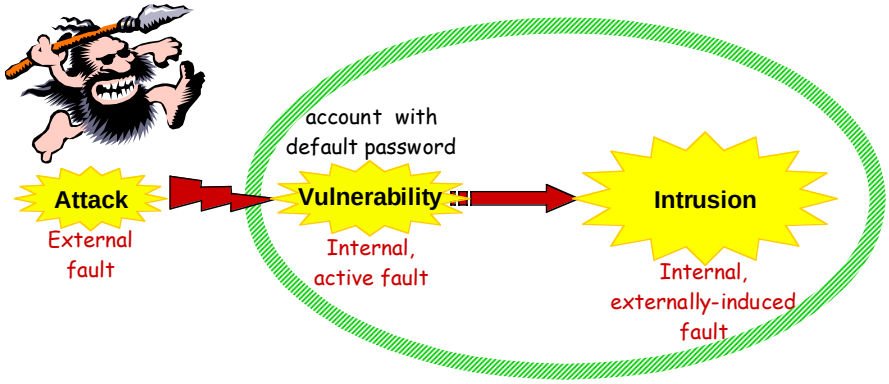
SELs (reversible stuck-at faults)
may occur because of radiation
(e.g., cosmic ray, high energy ions)



Satellite on-board computer

Intrusions

Intrusions result from
(at least partially) successful attacks:



Computing System

Intrusion-Tolerance Concepts

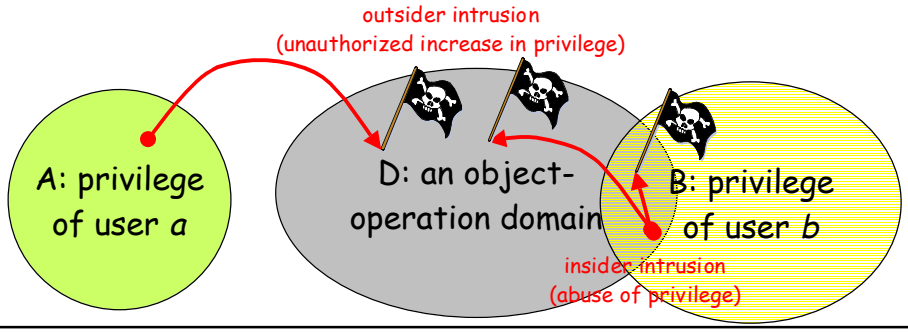
- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- Loss of Confidentiality
- Security Guarantees
- Intrusion Tolerance

Outsiders vs Insiders

- Outsider ⇔ Privilege = Ø?
  - Privilege: set of rights
  - Right: authorization(operation x object)
- Quid "open" systems?
- Need different definition
  - types of possible attack
  - sub-set (domain) of universe of object-operation pairs

Outsiders vs Insiders

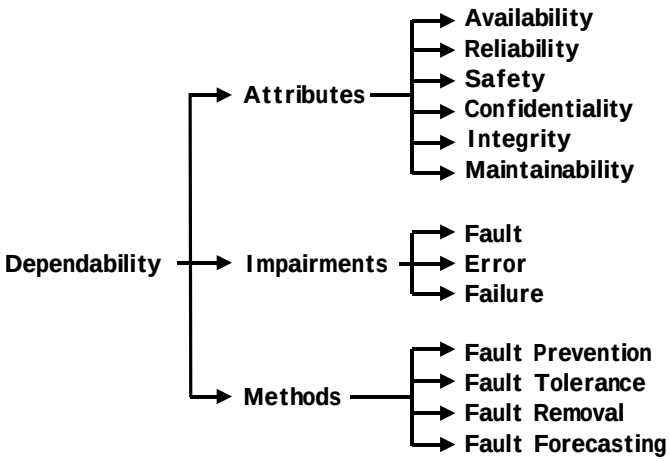
- Outsider: not authorized to perform any of specified object-operations
- Insider: authorized to perform some of specified object-operations



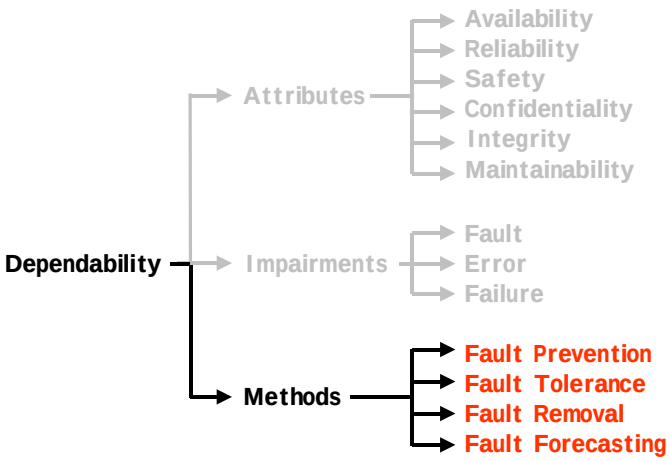
Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- **Security Methods**
- Intrusion Detection
- Loss of Confidentiality
- Security Guarantees
- Intrusion Tolerance

The Dependability Tree



The Dependability Tree



Dependability Methods:

Fault prevention	how to prevent the occurrence or introduction of faults
Fault tolerance	how to provide a service capable of or implementing the system function despite faults
Fault removal	how to reduce the presence (number, severity) of faults
Fault forecasting	how to estimate the presence, creation and consequences of faults

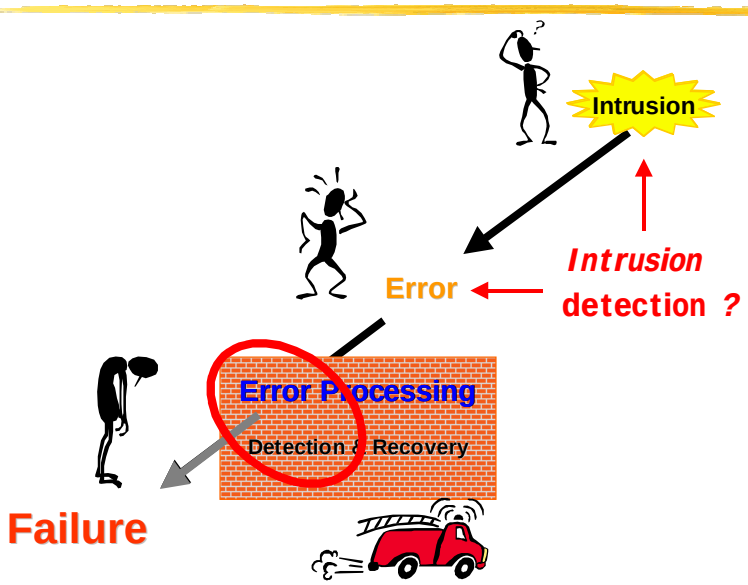
Security Methods:

Vulnerability prevention	how to prevent the occurrence or introduction of vulnerabilities
Intrusion prevention	how to prevent the occurrence of intrusions (vulnerability + attack prevention)
Vulnerability tolerance	synonym for intrusion tolerance
Intrusion tolerance	how to provide a service capable of or implementing the system function despite intrusions
Vulnerability removal	how to reduce the presence (number, severity) of vulnerabilities
Intrusion removal	not meaningful
Vulnerability forecasting	how to estimate the presence, creation and consequences of vulnerabilities
Intrusion forecasting	how to estimate the creation and consequences of intrusions (vulnerability + attack forecasting)

Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- **Intrusion Detection**
- Loss of Confidentiality
- Security Guarantees
- Intrusion Tolerance

Error Detection



What is Intrusion Detection?

- When?
  - after the fact
    - post-mortem analysis

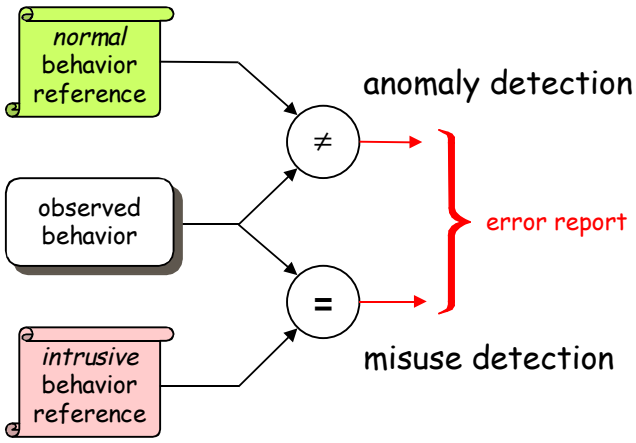
    off-line diagnosis
    part of curative maintenance
  - near real-time
    - for SSO intervention

    error detection + on-line diagnosis
    for operator-assisted fault treatment
  - real-time
    - support of automated countermeasures

    error detection
    for automatic error recovery

What is Intrusion Detection?

- How?



Intrusion Detection System

- Facility aimed at discovering the presence of intrusions
  - set of sensors or error detectors (including anomaly and misuse detectors), and
  - intrusion diagnosis mechanism that collates sensor outputs to decide whether the detected errors are symptomatic of intrusion

Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- **Loss of Confidentiality**
- Security Guarantees
- Intrusion Tolerance

Loss of Confidentiality

- No equivalent in traditional fault-tolerance
- Implies that information is in some place it should not be
  - this is an error!
- Detection? — "undetachable" labels?
- Recovery? — substitute new secret?

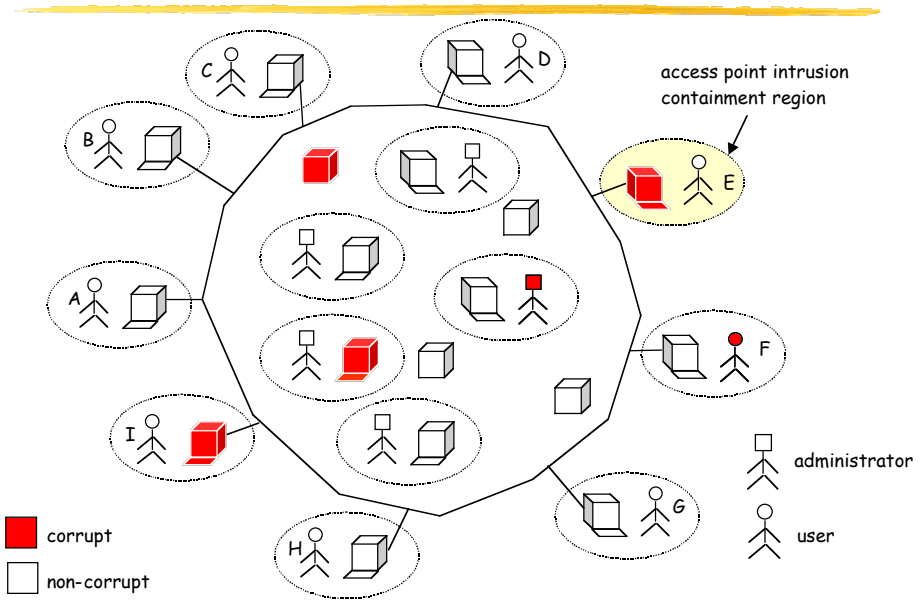
Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- Loss of Confidentiality
- **Security Guarantees**
- Intrusion Tolerance

Fault-tolerance guarantees

- Cannot place restriction on what an *arbitrarily* faulty component can do
- So guarantees are restricted to *fault-free* components
- An atomic component (from the viewpoint of fault-tolerance) has been called a "fault containment region"

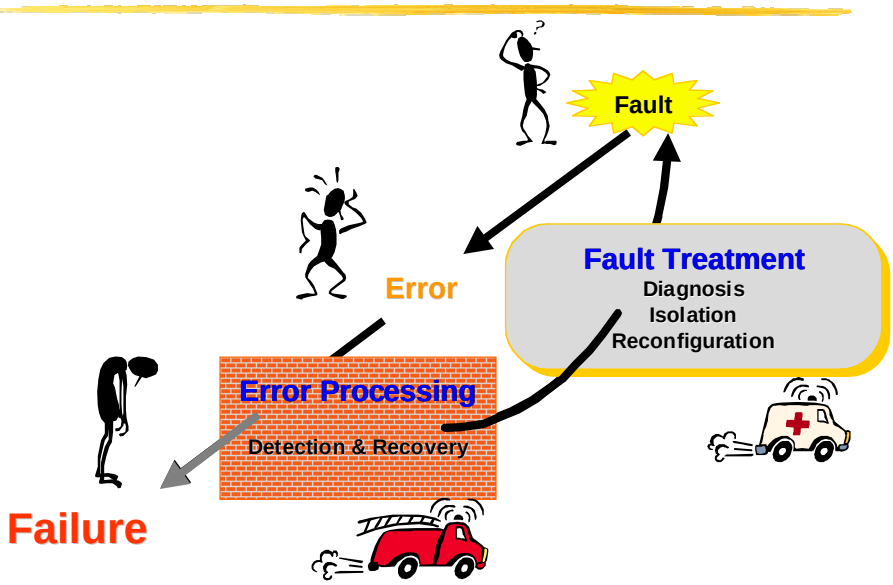
Intrusion-Containment Regions



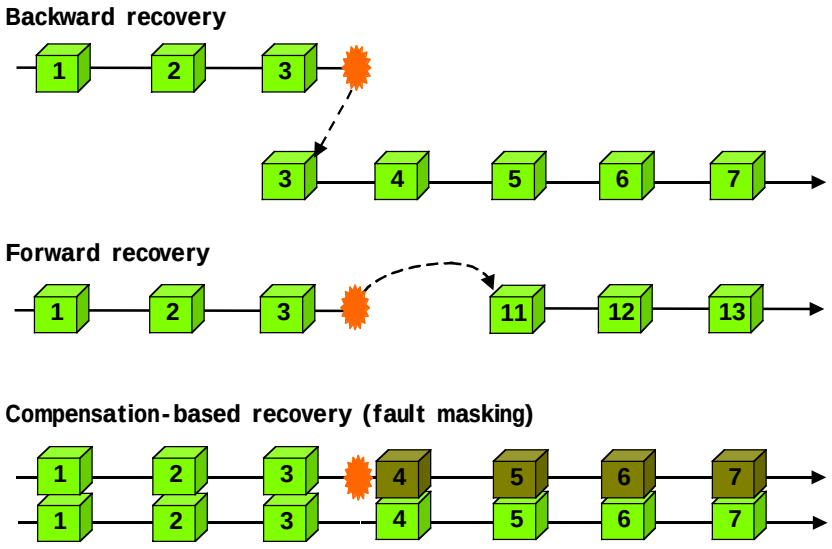
Intrusion-Tolerance Concepts

- Intrusion vs Attack
- Outsiders vs Insiders
- Security Methods
- Intrusion Detection
- Loss of Confidentiality
- Security Guarantees
- **Intrusion Tolerance**

Fault Tolerance



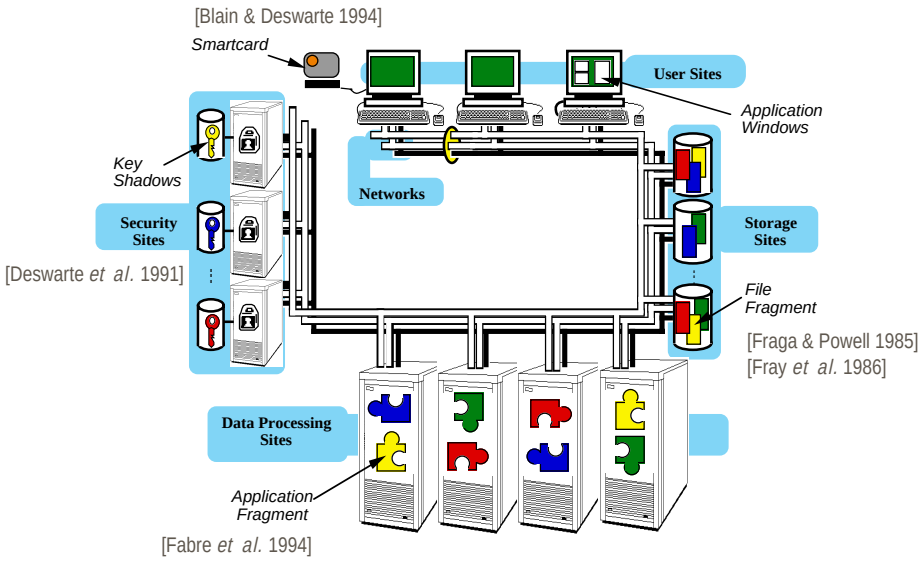
Error Processing

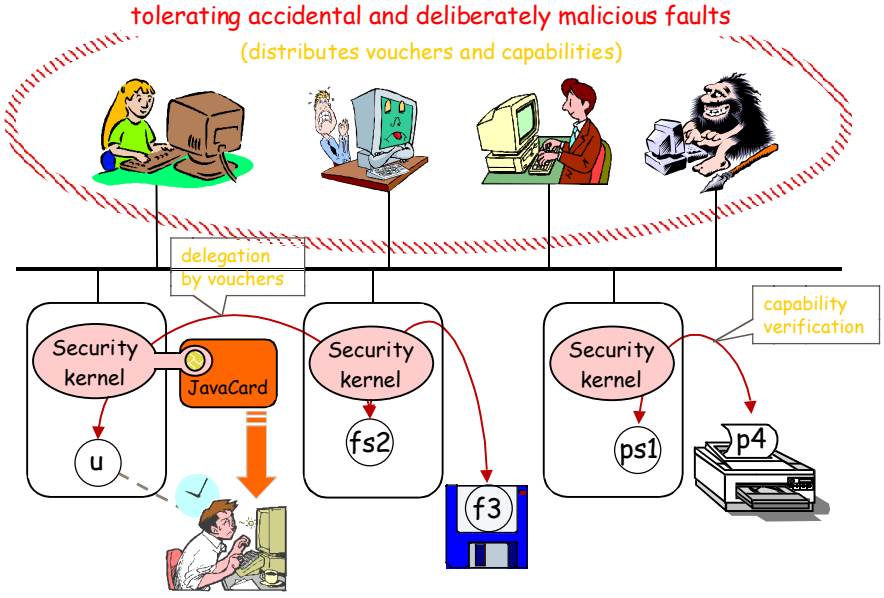


Error Processing (wrt intrusions)

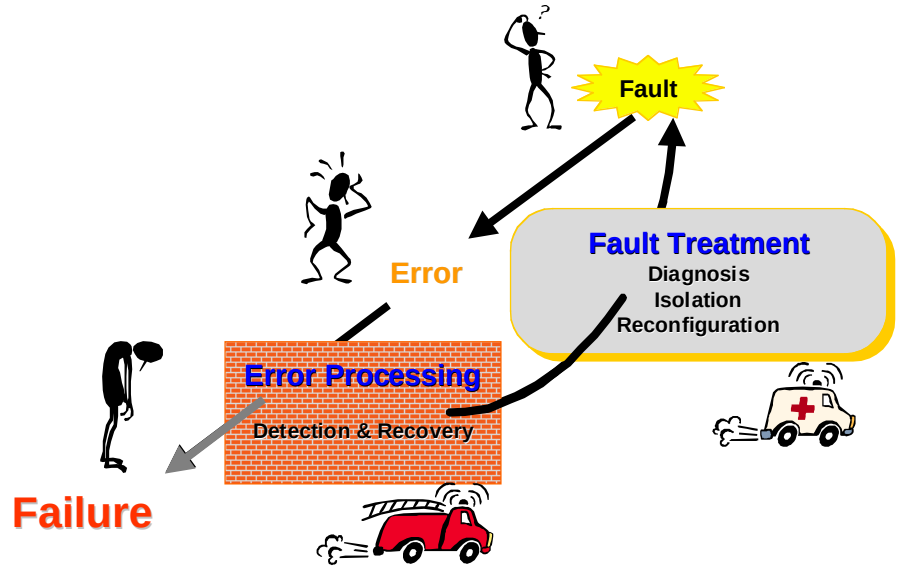
- Error (intrusion-symptom) detection
  - + Backward recovery (availability, integrity)
  - + Forward recovery (availability, confidentiality)
- Intrusion masking
  - o Fragmentation (confidentiality)
  - o Redundancy (availability, integrity)
  - o Scattering

Past Work on FRS





Fault Tolerance

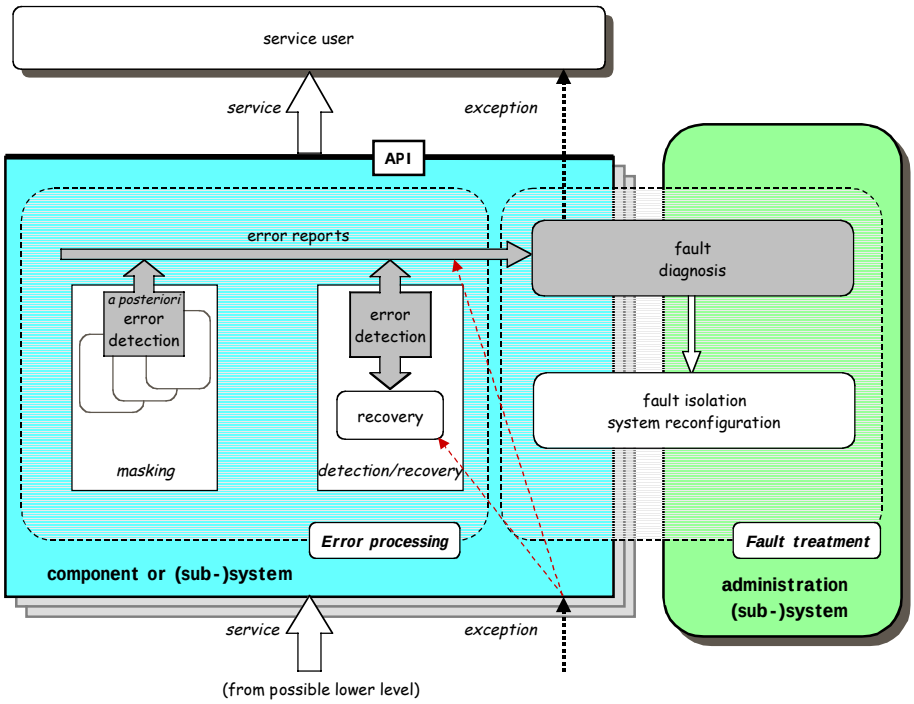


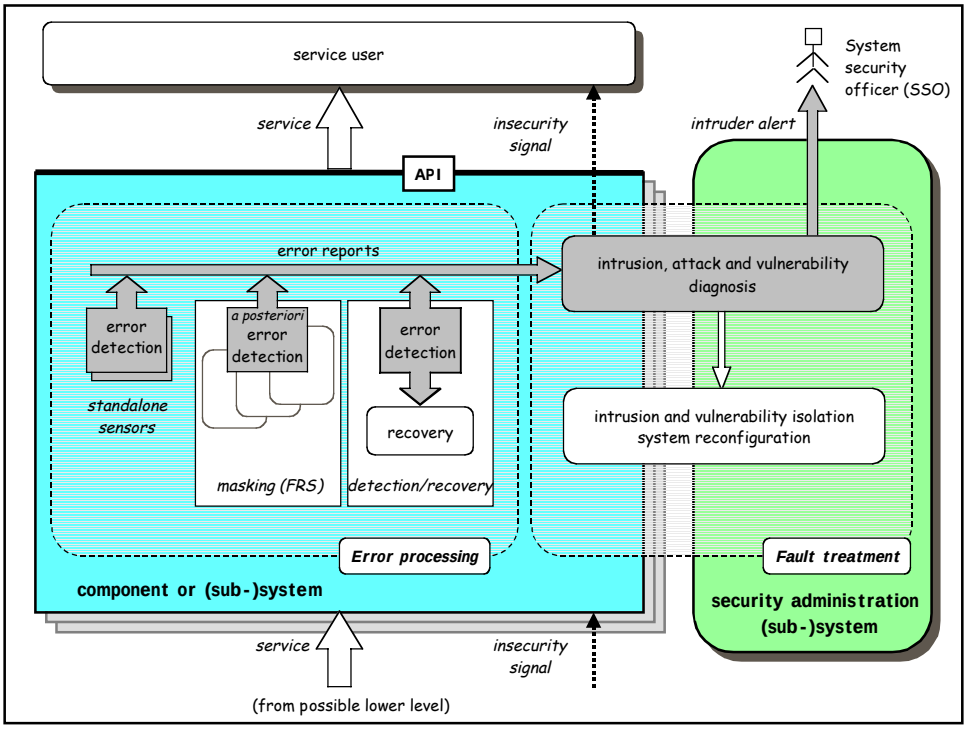
Fault Treatment

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





References

- 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 *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,* 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 *Conf. 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,* (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 *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, pp.2-11.
- Laprie, J.-C. (Ed.), (1992). *Dependability: Basic Concepts and Terminology,* Dependable Computing and Fault-Tolerance, 5, 265p., Springer-Verlag, Vienna, Austria.
- Laprie, J.-C. (1995). Dependable Computing: Concepts, Limits, Challenges, in *Special Issue, 25th IEEE Int. Symp. on Fault-Tolerant Computing (FTCS-25),* Pasadena, CA, USA, pp.42-54, IEEE Computer Society Press.

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