MAFTIA concepts

Yves Deswarte

& David Powell
LAAS-CNRS, France

SRI International

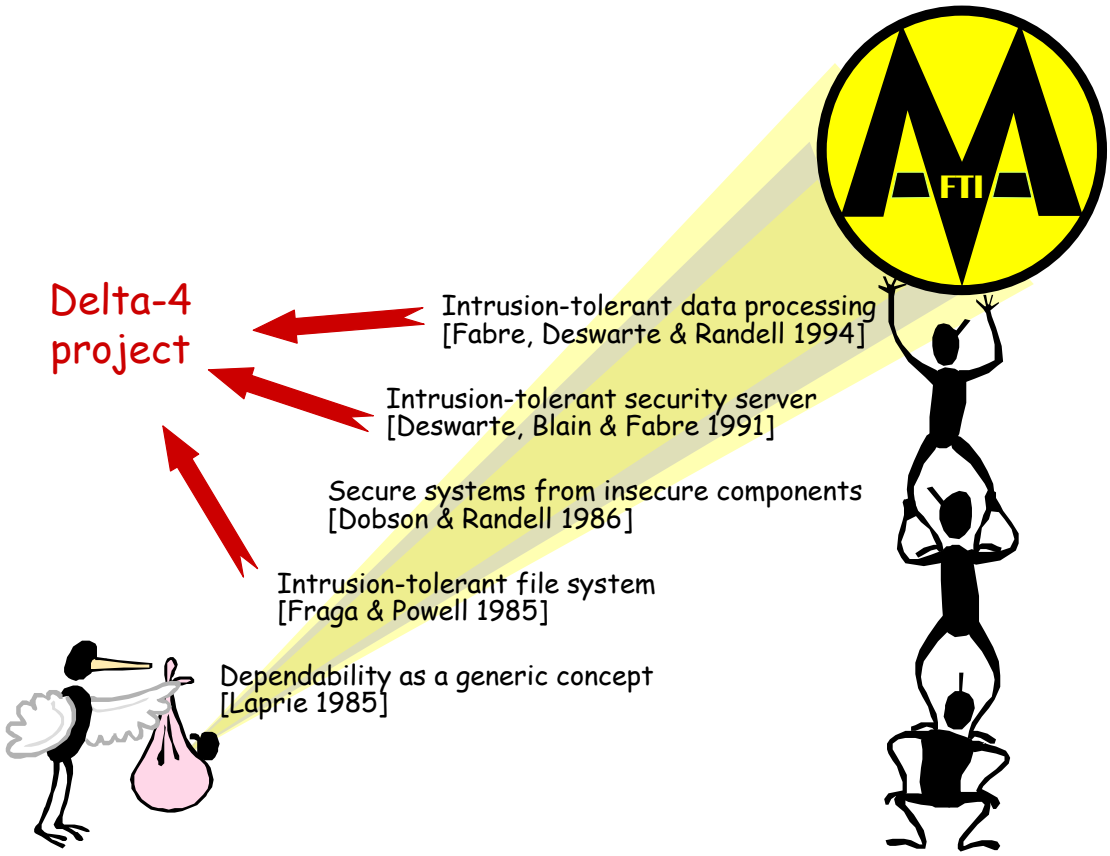
European IST Program
Dependability Initiative

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)

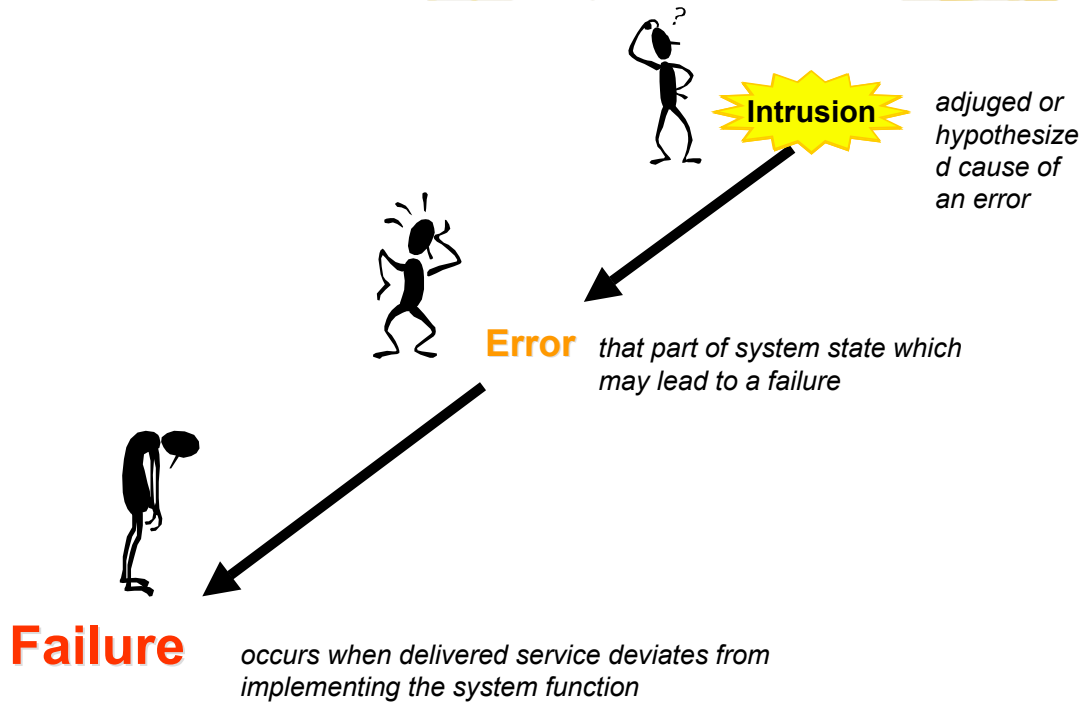
3 years (2000-2002), ~45 man-years, EU funding ~2.5M€



Workplan

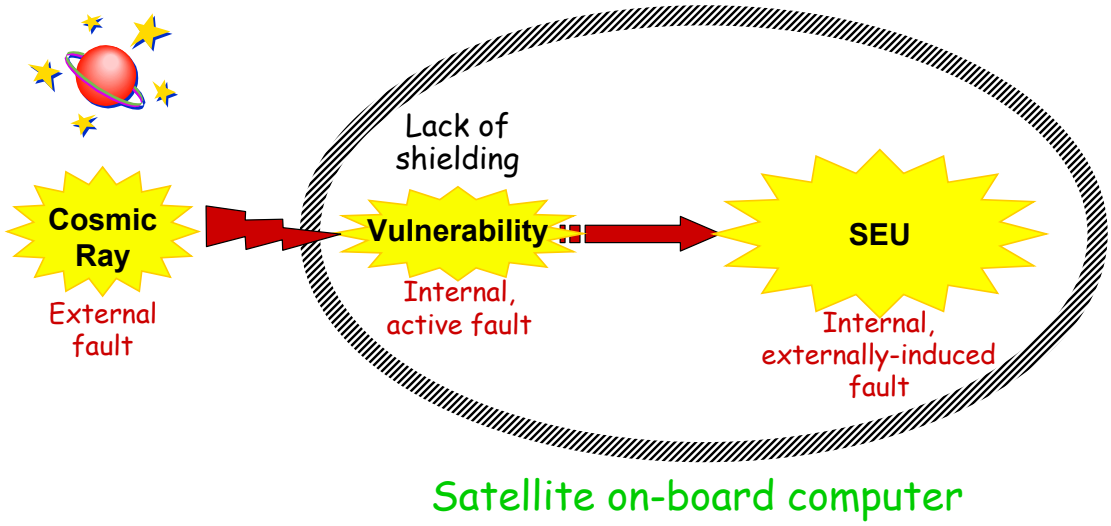
- WP1: Conceptual model and architecture
- WP2: Dependable middleware
- WP3: Intrusion detection
- WP4: Dependable trusted third parties
- WP5: Distributed authorization
- WP6: Assessment

Fault, Error & Failure



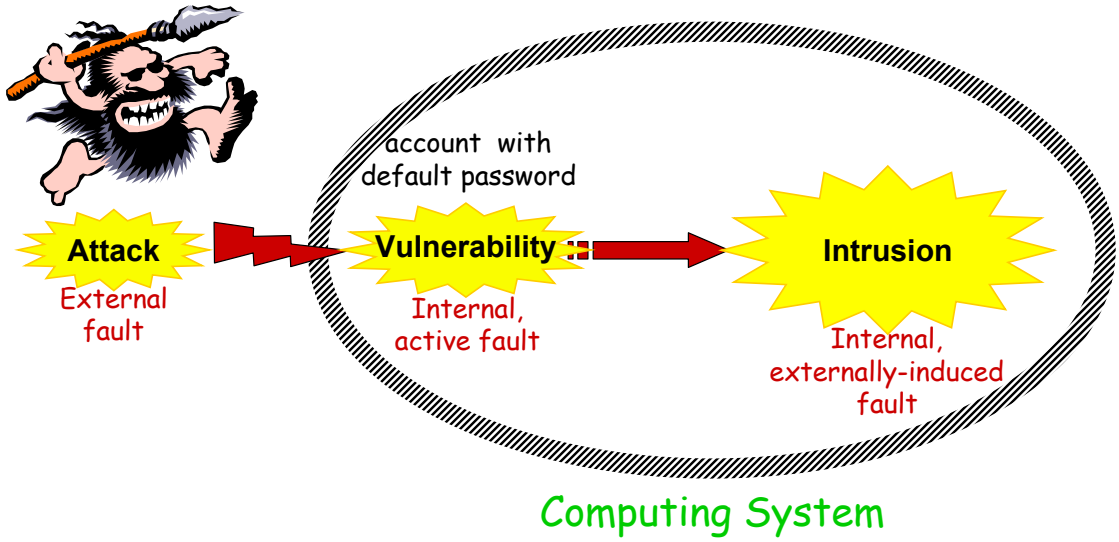
Example: Single Event Upset

SEUs (bit-flips, stuck-at faults, cell destructions)
can result from radiation
(e.g., cosmic ray, high energy ions)



Intrusions

Intrusions are resulting from
(at least partially) successful attacks:



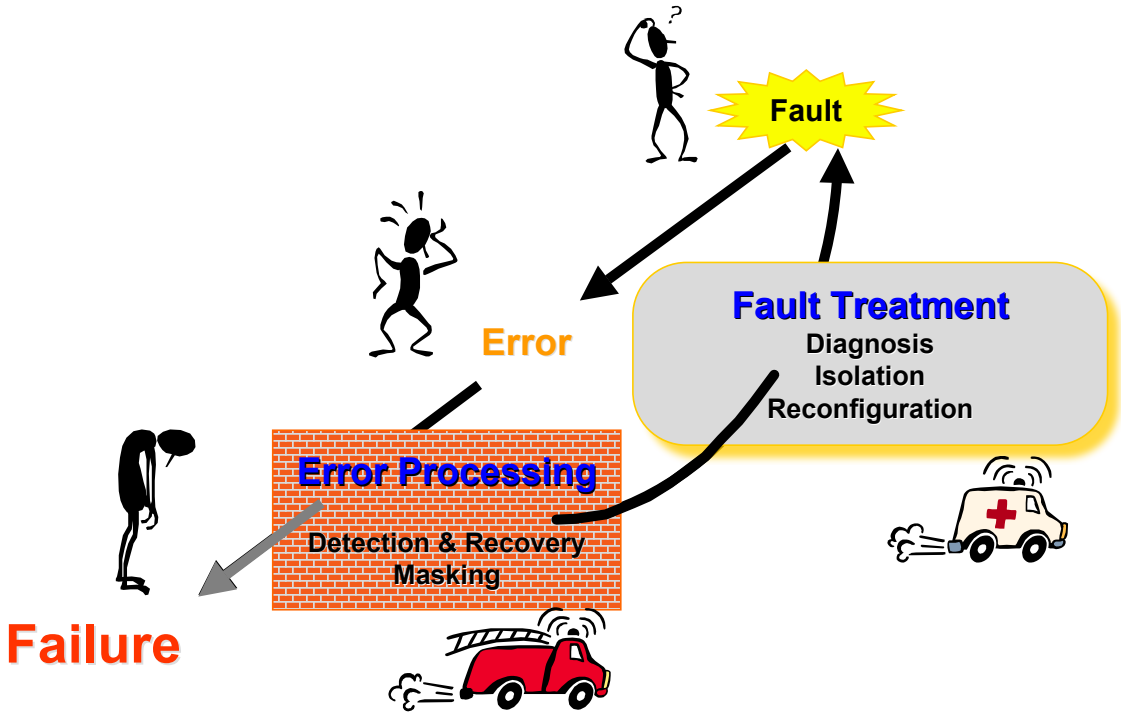
Dependability obtained through:

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

For intrusions:

Vulnerability prevention	how to prevent the occurrence or introduction of vulnerabilities
Intrusion prevention	how to prevent the occurrence of intrusions (vulnerability prevention + attack deterrence)
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)

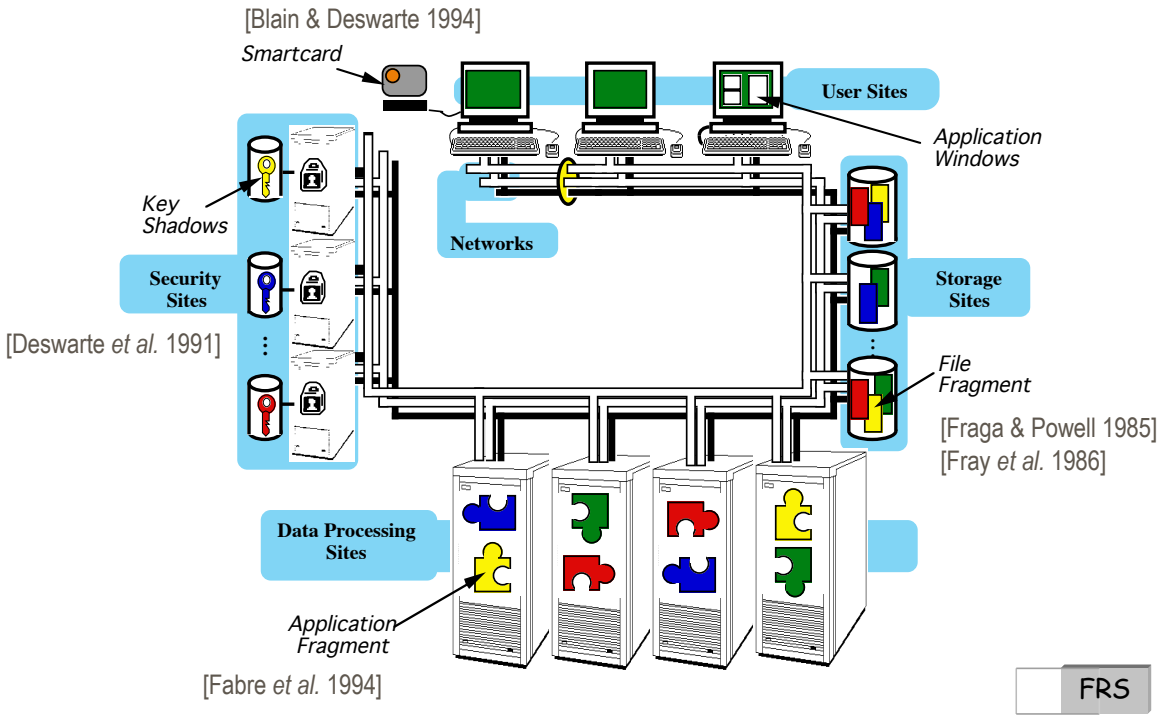
Fault Tolerance

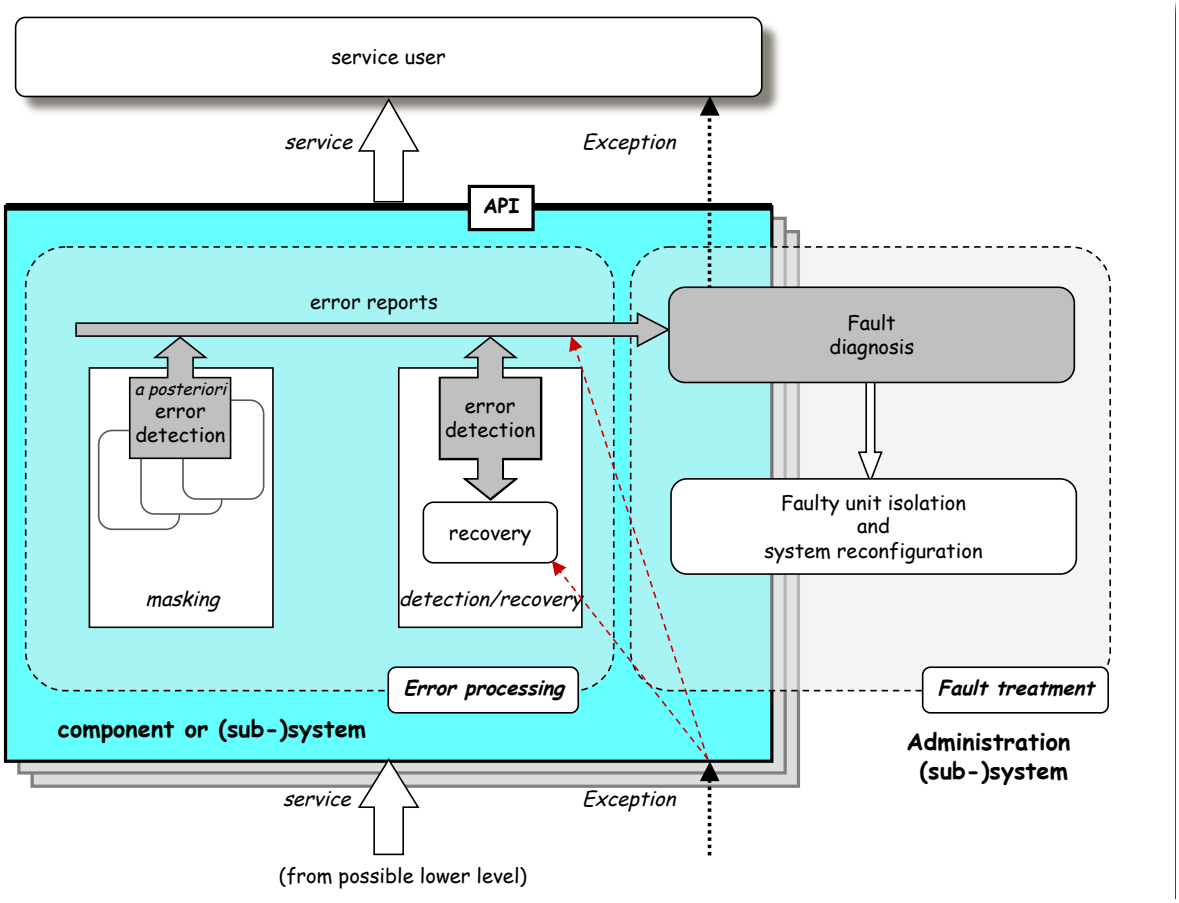


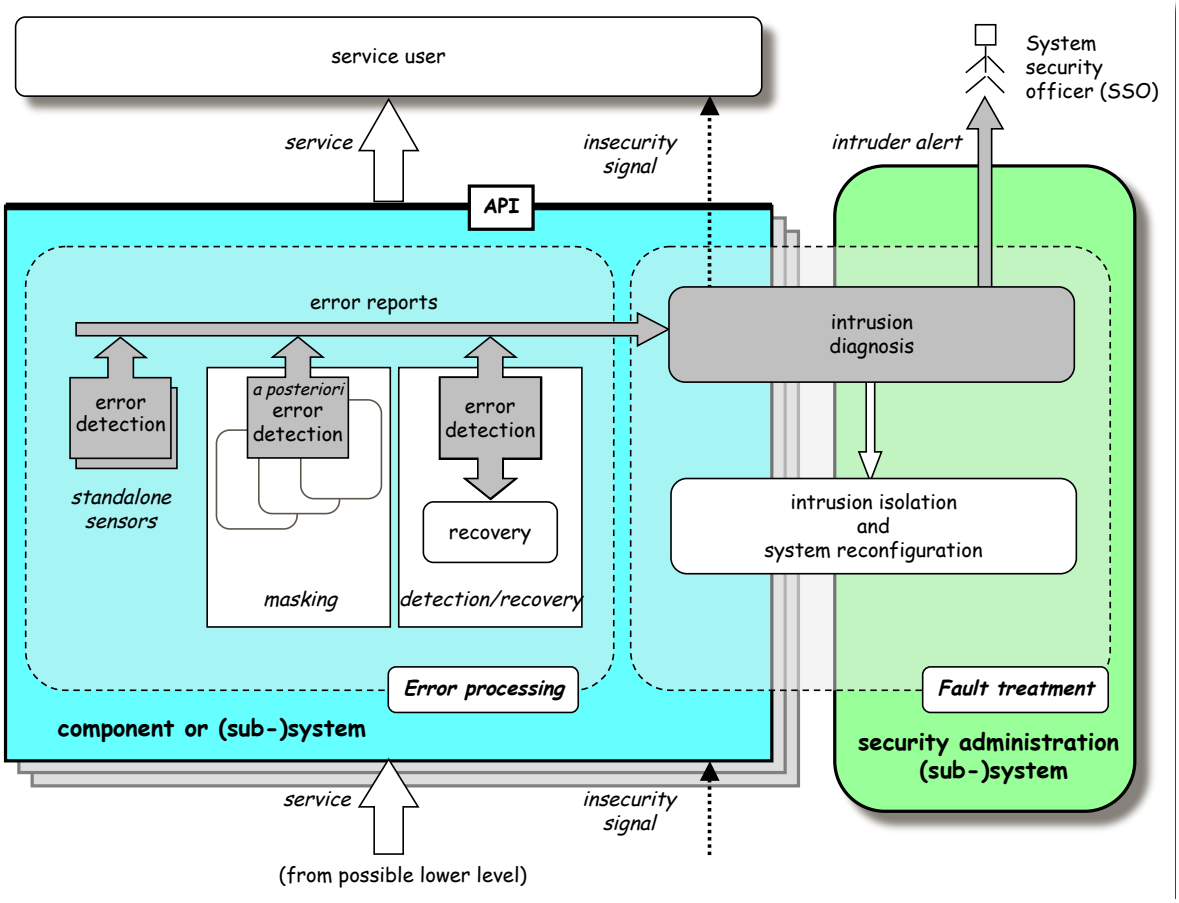
Intrusion tolerance

- Error processing:
  - Intrusion-symptom detection + recovery
  - Intrusion masking
- Fault treatment
  - Intrusion diagnosis (+ retaliation?)
  - Vulnerability removal

Intrusion Masking: Delta-4 (86-96)




service user
service
Exception
API
error reports
Fault
diagnosis
a posteriori
error
detection
error
detection
recovery
Faulty unit isolation
and
system reconfiguration
masking
detection/recovery
Error processing
Fault treatment
component or (sub-)system
Administration
(sub-)system
service
Exception
(from possible lower level)


service user
System
security
officer (SSO)
service
insecurity
signal
intruder alert
API
error reports
intrusion
diagnosis
error
detection
a posteriori
error
detection
error
detection
recovery
intrusion isolation
and
system reconfiguration
standalone
sensors
masking
detection/recovery
Error processing
Fault treatment
component or (sub-)system
security administration
(sub-)system
service
insecurity
signal
(from possible lower level)

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.
- 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.

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