Intrusion Tolerance and the MAFTIA project

Yves Deswarte
deswarte@laas.fr

David Powell
dpowell@laas.fr

LAAS-CNRS
Toulouse, France

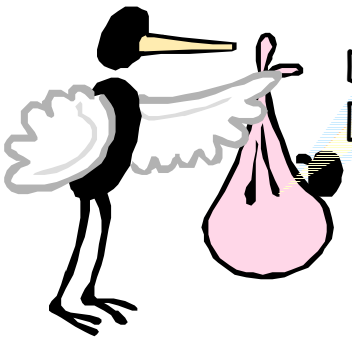
Intrusion-tolerant data processing
[Fabre, Deswarte & Randell 1994]

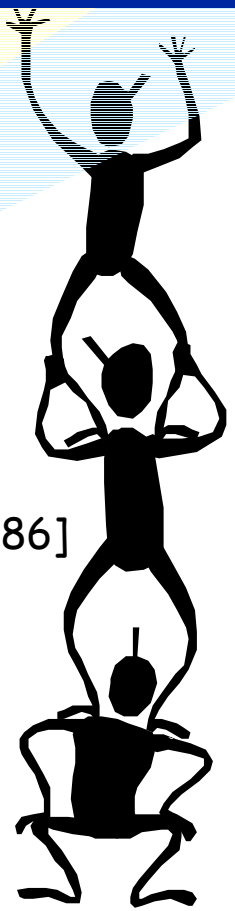
Intrusion-tolerant distributed systems
[Deswarte, Blain & Fabre 1991]

Secure systems from insecure components
[Dobson & Randell 1986]

Intrusion-tolerant file system
[Fraga & Powell 1985], [Fray, Deswarte, Powell 1986]

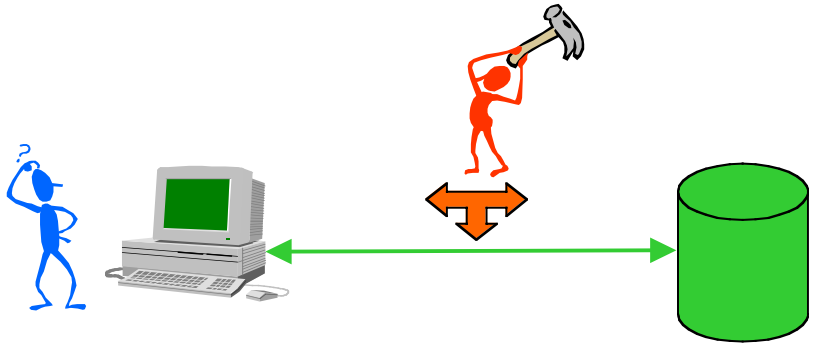
Dependability as a generic concept
[Laprie 1985]





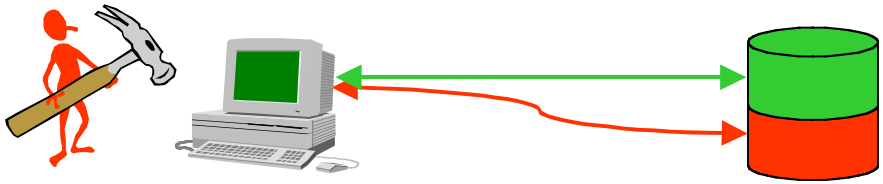
Who are the intruders?

1: Outsider



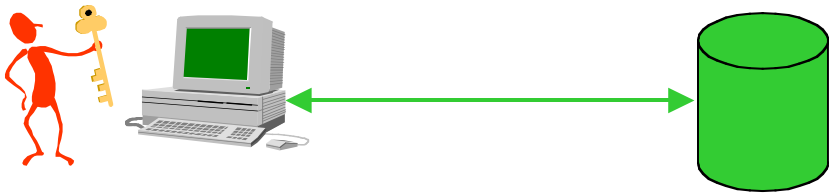
☺ Authentication
☺ Authorization

2: User



☹ Authentication
☺ Authorization

3: Privileged User



☹ Authentication
☹ Authorization

Insiders or Outsiders ?

- 01 Informatique 1998
  - 1200 companies in 32 countries
  - 66% experienced fraud in last 12 months
    - 85% by company employees
- Information Week's security survey 1999

  http://www.informationweek.com/743/security.htm
  - 2700 security professionals in 49 countries
  - 76% had suffered a security breach
    - 41 % from authorised users (in 1998: 58 %)
    - 31 % from service providers (in 1998: 10 %)

Intrusion Tolerance

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

FRS: Fragmentation-Redundancy-Scattering

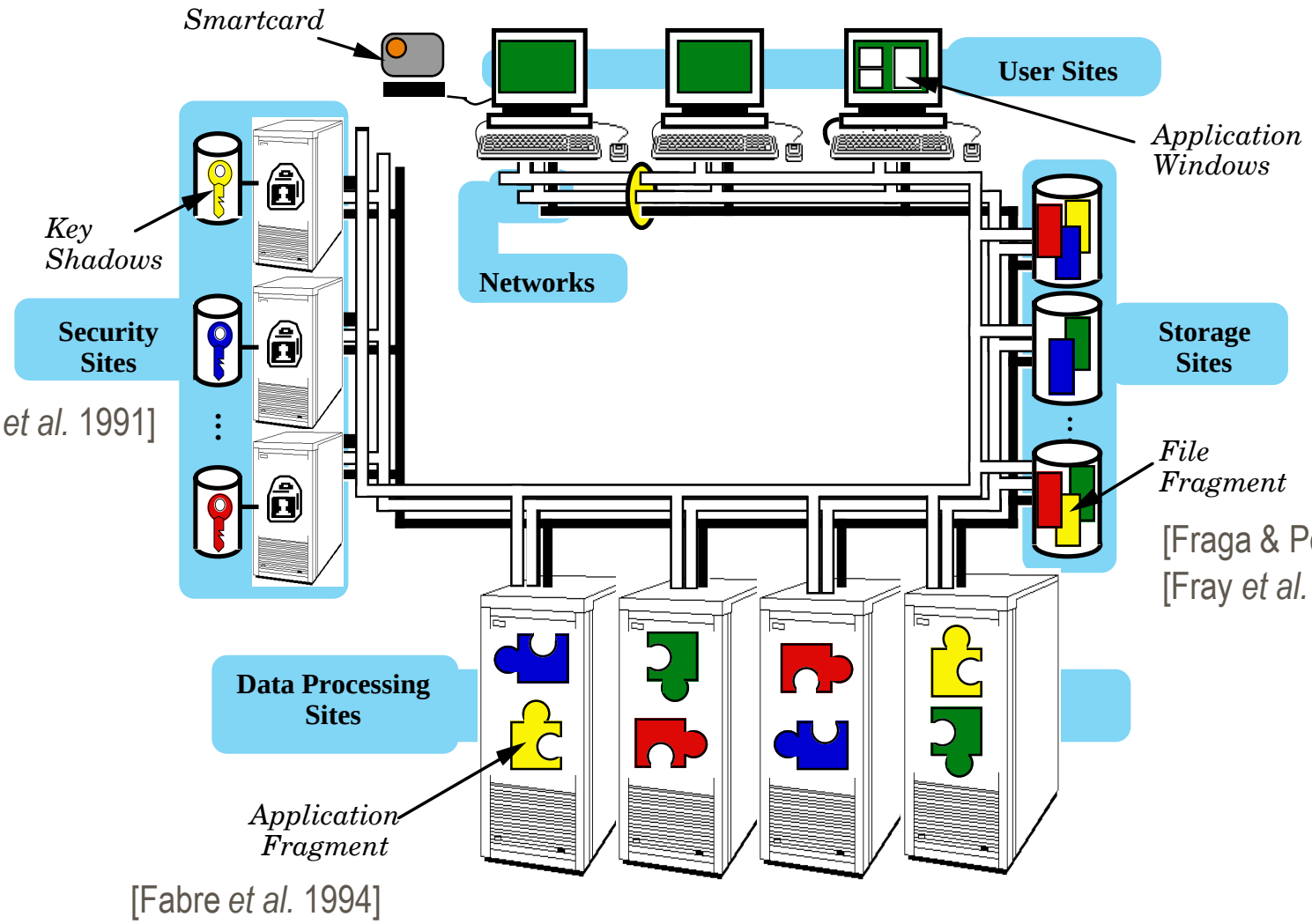
- Fragmentation: split the data into fragments so that isolated fragments contain no significant information: *confidentiality*
- Redundancy: add redundancy so that fragment modification or destruction would not impede legitimate access: *integrity + availability*
- Scattering: isolate individual fragments

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]

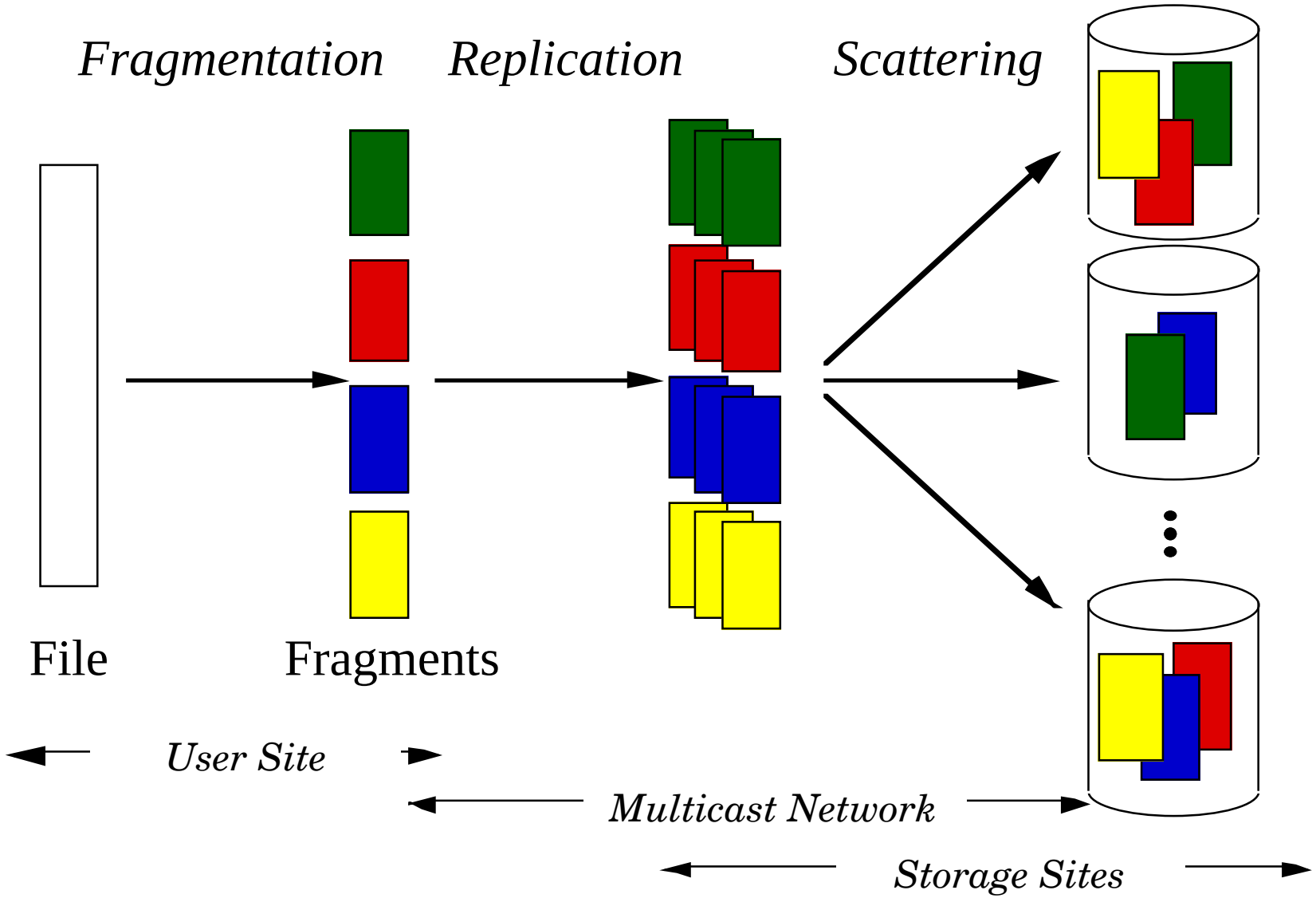


[Deswarte *et al.* 1991]

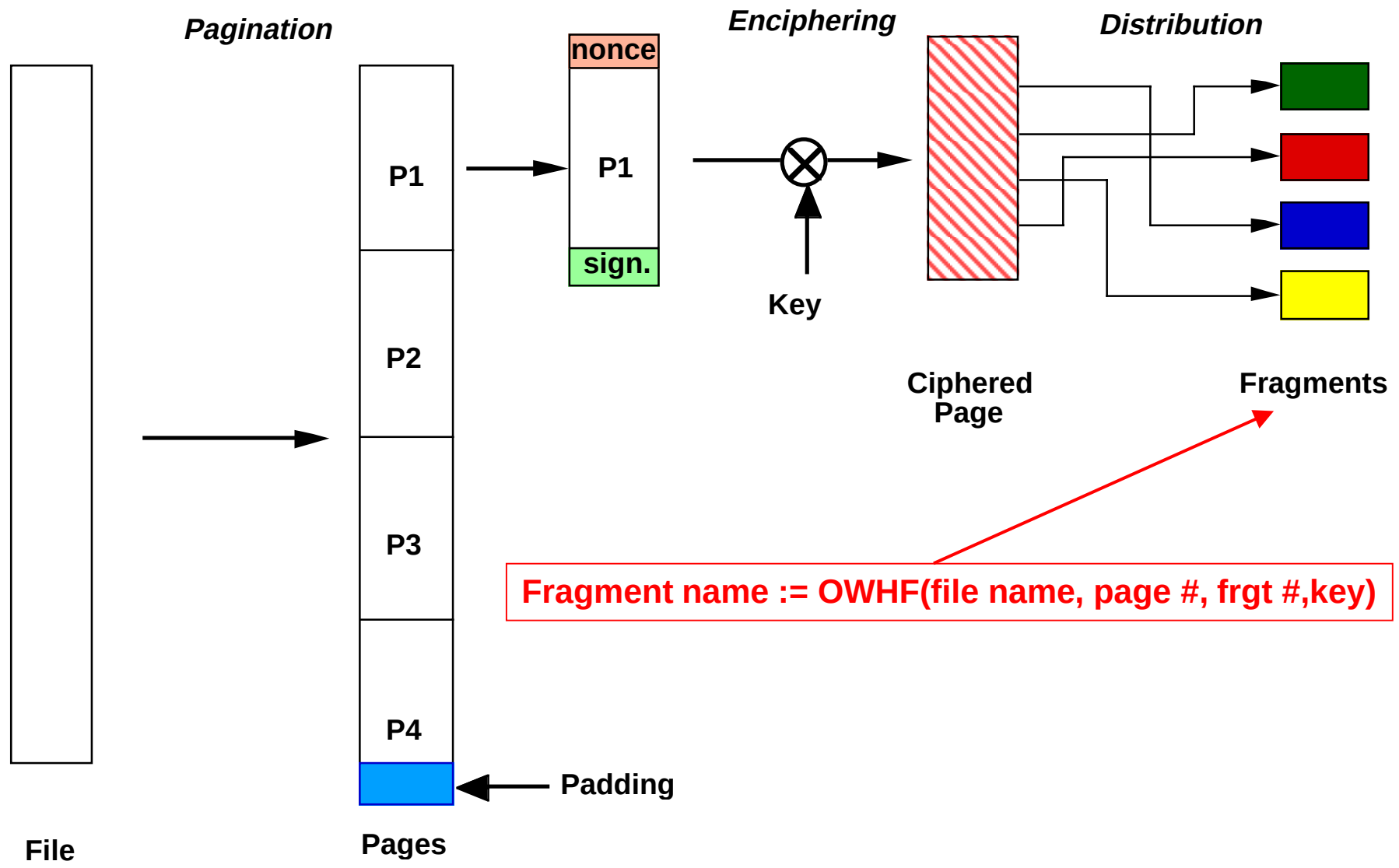
[Fraga & Powell 1985]
[Fray *et al.* 1986]

[Fabre *et al.* 1994]

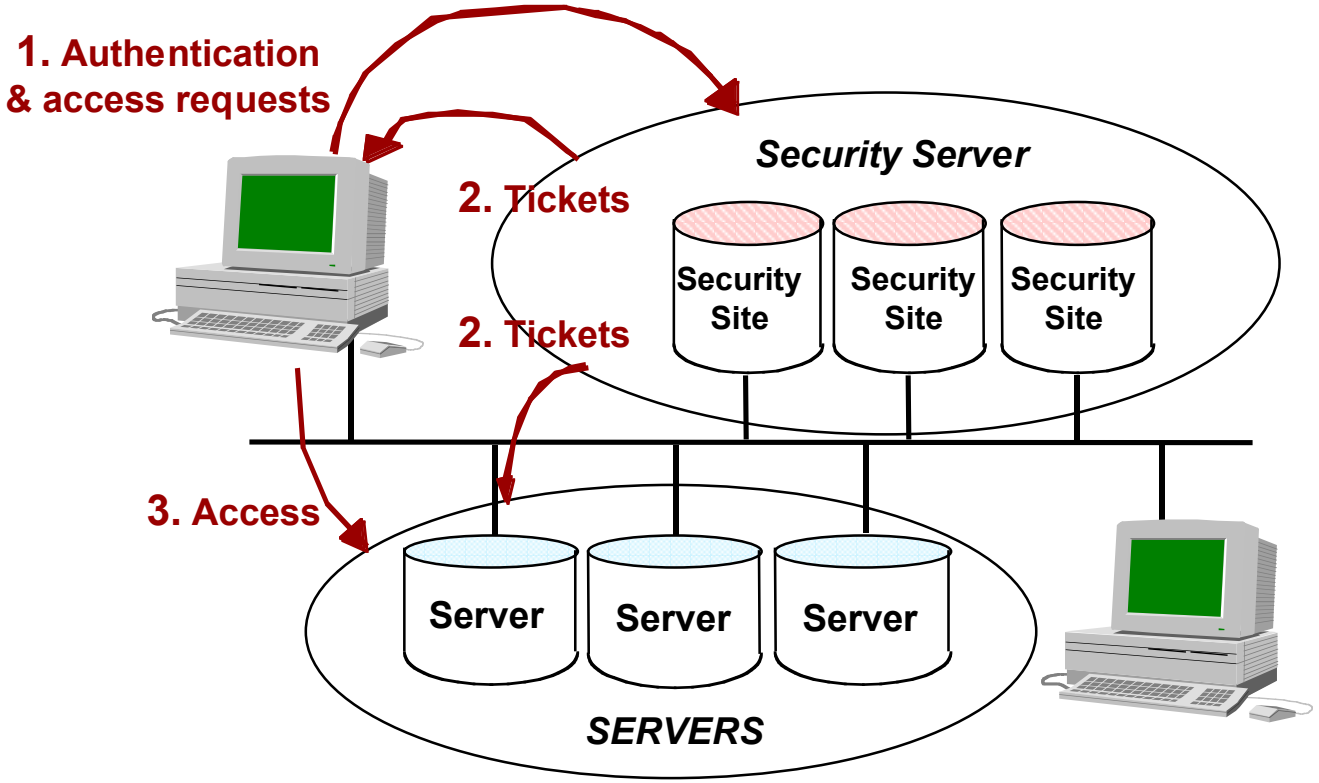
FRSed File Server



File Fragmentation

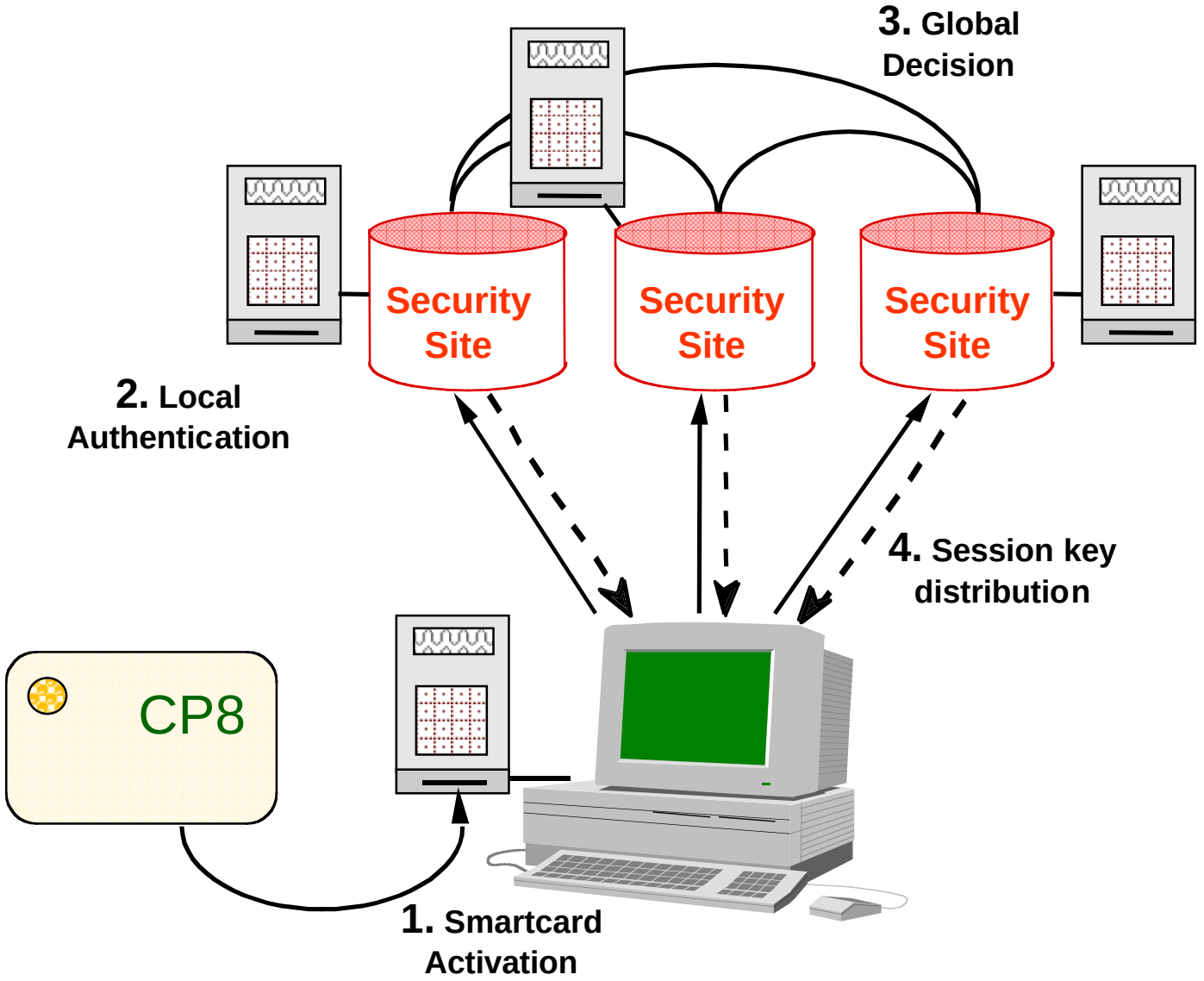


FRSed Security Management

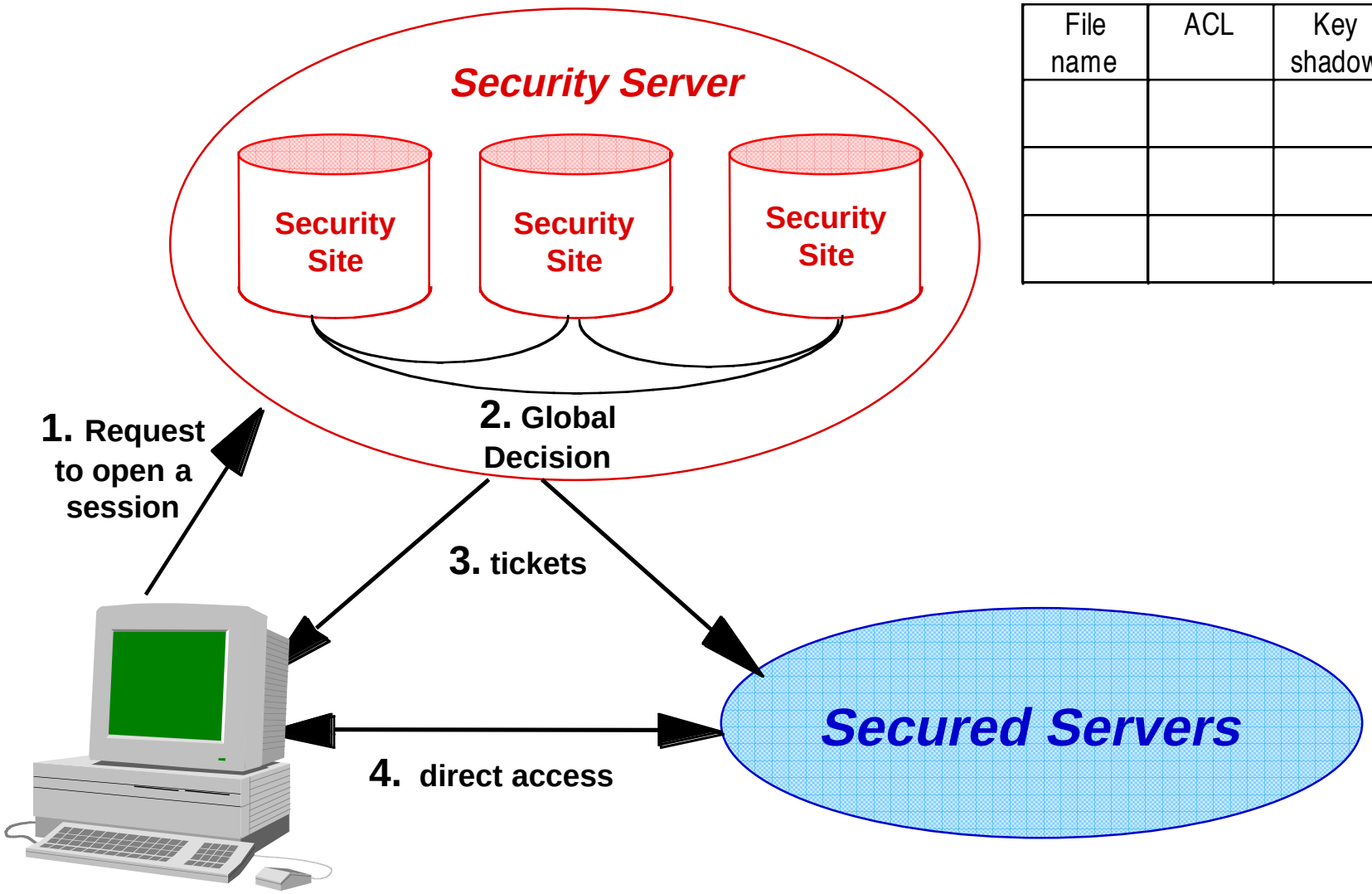


- No single trusted site or administrator
- Global trust in a majority of security sites (and administrators)

Authentication

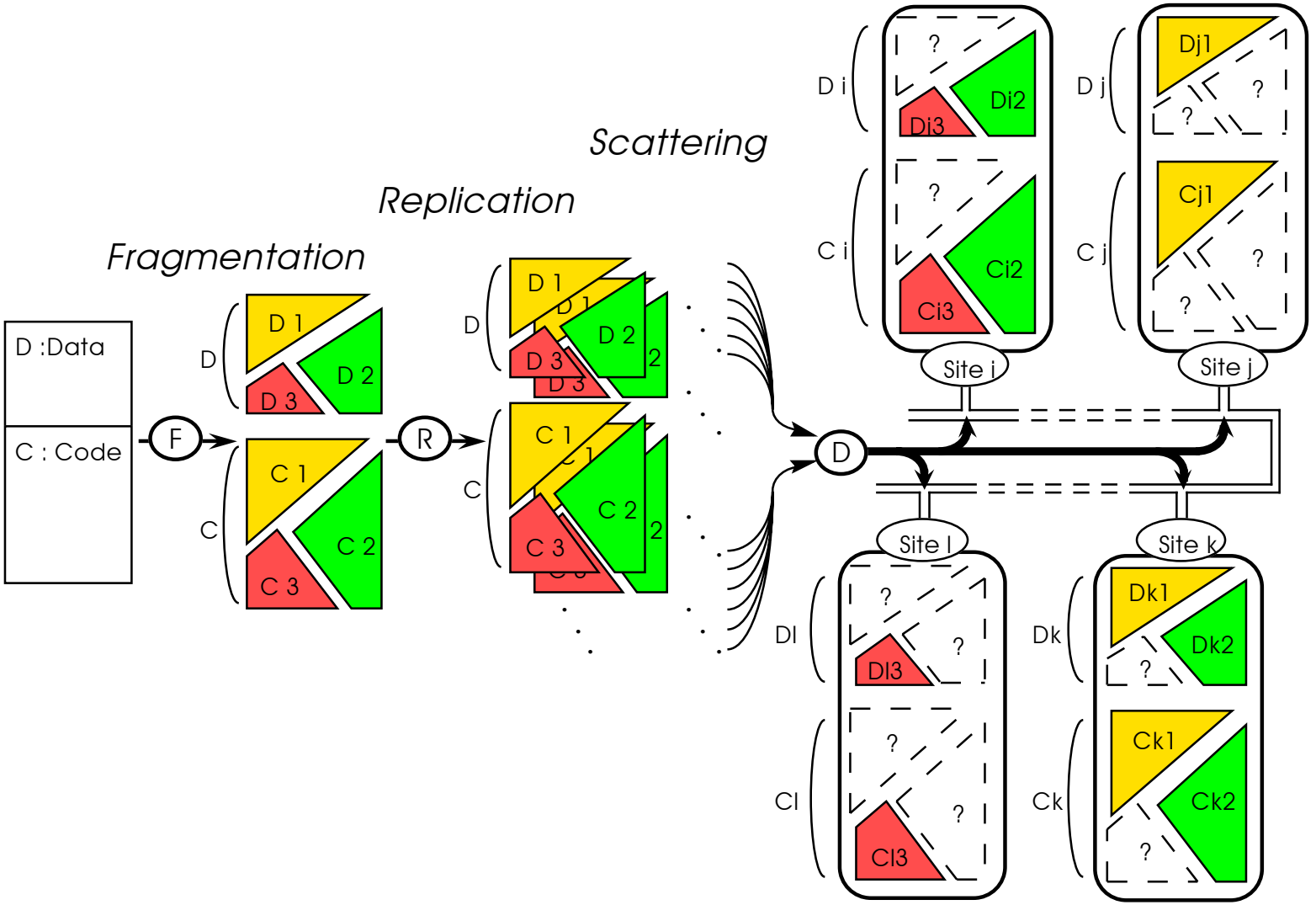


Authorization



File name	ACL	Key shadow

Fragemented Data Processing



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)	Peter Ryan, 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

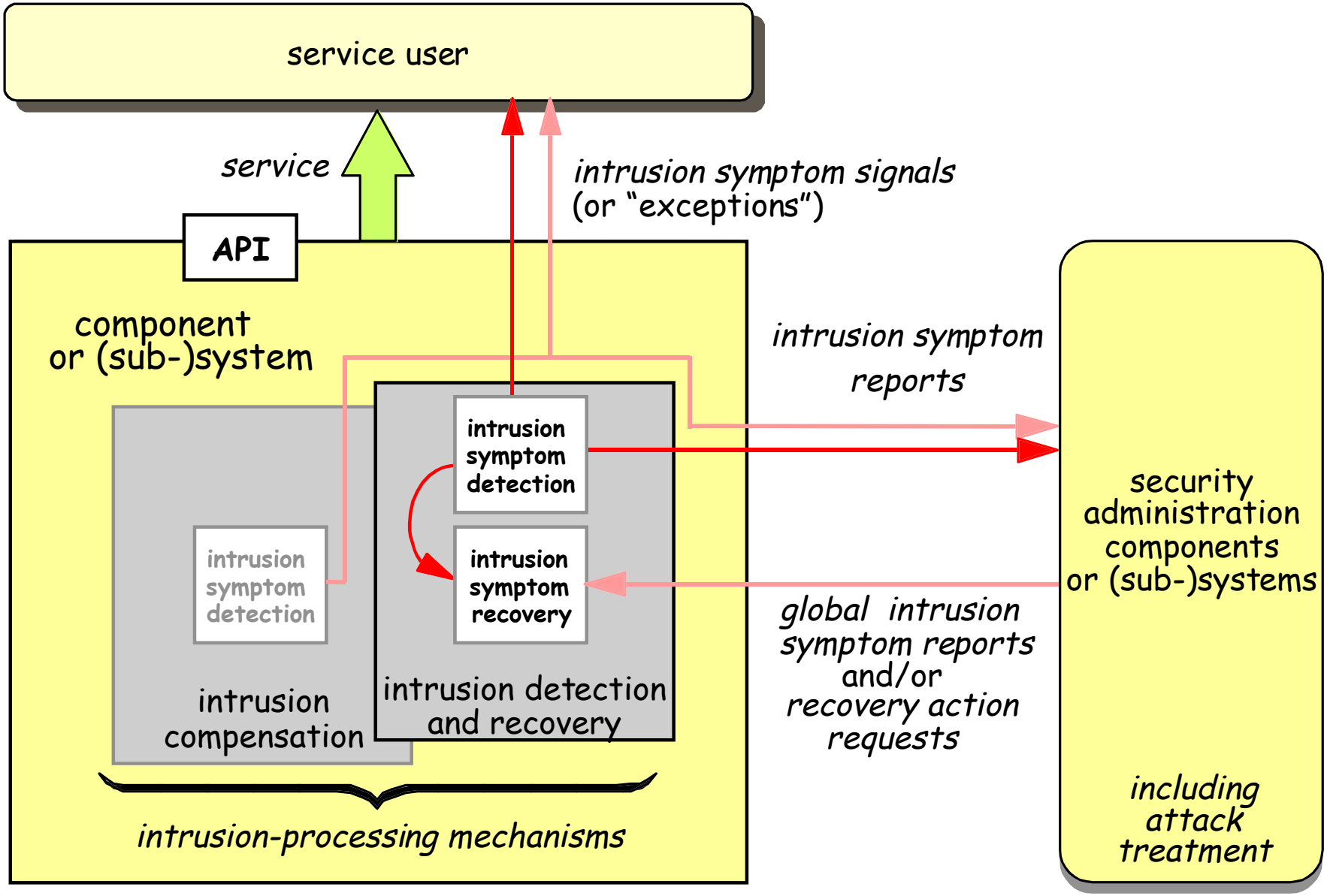
c. 45 man-years, c. 2.5M euro

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

Workplan

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

Intrusion-tolerance framework



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.