Intrusion Tolerance for Internet Applications

Yves Deswarte & David Powell
LAAS-CNRS, Toulouse, France

IFIP World Computer Congress, Toulouse, 22-27 August 2004
Topical Day on Fault Tolerance for Trustworthy and Dependable Information Infrastructures

Internet Users

Categories:

B2B, B2C, C2A, e-government, associations, private citizens, virtual communities…

Motivations:

commerce, administration, democracy, social benefit, culture, recreation…

Cannot exclude any single user category to favor another

Different security requirements and degrees of system administration

Some facts of (Internet) life

1. there are weakly-administered machines, which can be exploited by potential attackers to increase their firing power or to hide their tracks
2. there are hundreds of millions of Internet users, of which a (small) proportion are potential attackers

Internet Attackers

Categories:

disturbed teenagers, hacker groups, thieves, criminals, terrorists, government services…

Motivations:

sport, curiosity, vanity, vandalism, vengeance, greed, politics…

Varying degrees of tenacity

Various deployable resource levels

- **network vulnerabilities** (eavesdropping; jamming; message destruction, insertion, counterfeiting, modification or replay; address falsification…);
- **OS and application vulnerabilities** (buffer/stack overflows…)

availability, confidentiality, integrity

Internet

Conventional Security Techniques

User Authentication

- Identify user
- User responsibility and liability

User Authorization

- Allow only legitimate actions
- Least privilege principle: legitimate <=> needed

Deterrence <= Retaliation <= Detection

- Inefficient in Internet context:
  - Strong authentication infeasible on publicly-accessible sites
  - COTS OS and application SW
    - many flaws
    - patches not applied due to lack of time or competency, or for fear of losing needed functionality
  - Internet protocols are vulnerable (Arpanet heritage)
  - Economic pressures do not (yet) favor known defenses
    - ingress filtering,
    - trace-back facilities, …

A Tolerance Approach?

Dependability as a generic concept
[Laprie 1985]

Intrusion-tolerant file system
[Fraga & Powell 1985]

Secure systems from insecure components
[Dobson & Randell 1986]

A fault tolerance approach to computer viruses
[Joseph & Avizienis 1988]

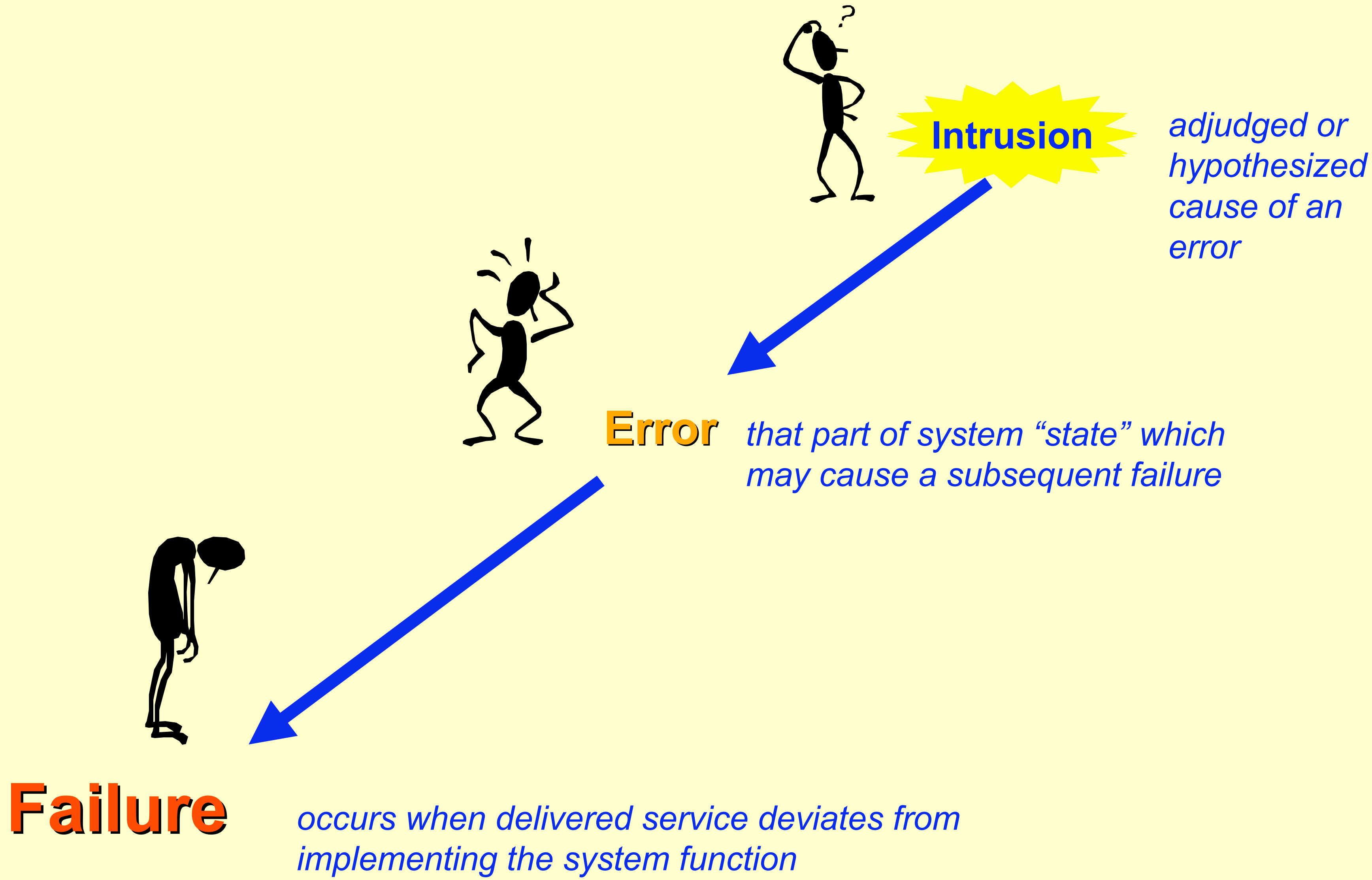
Intrusion-tolerant security server
[Deswarte, Blain & Fabre 1991]

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

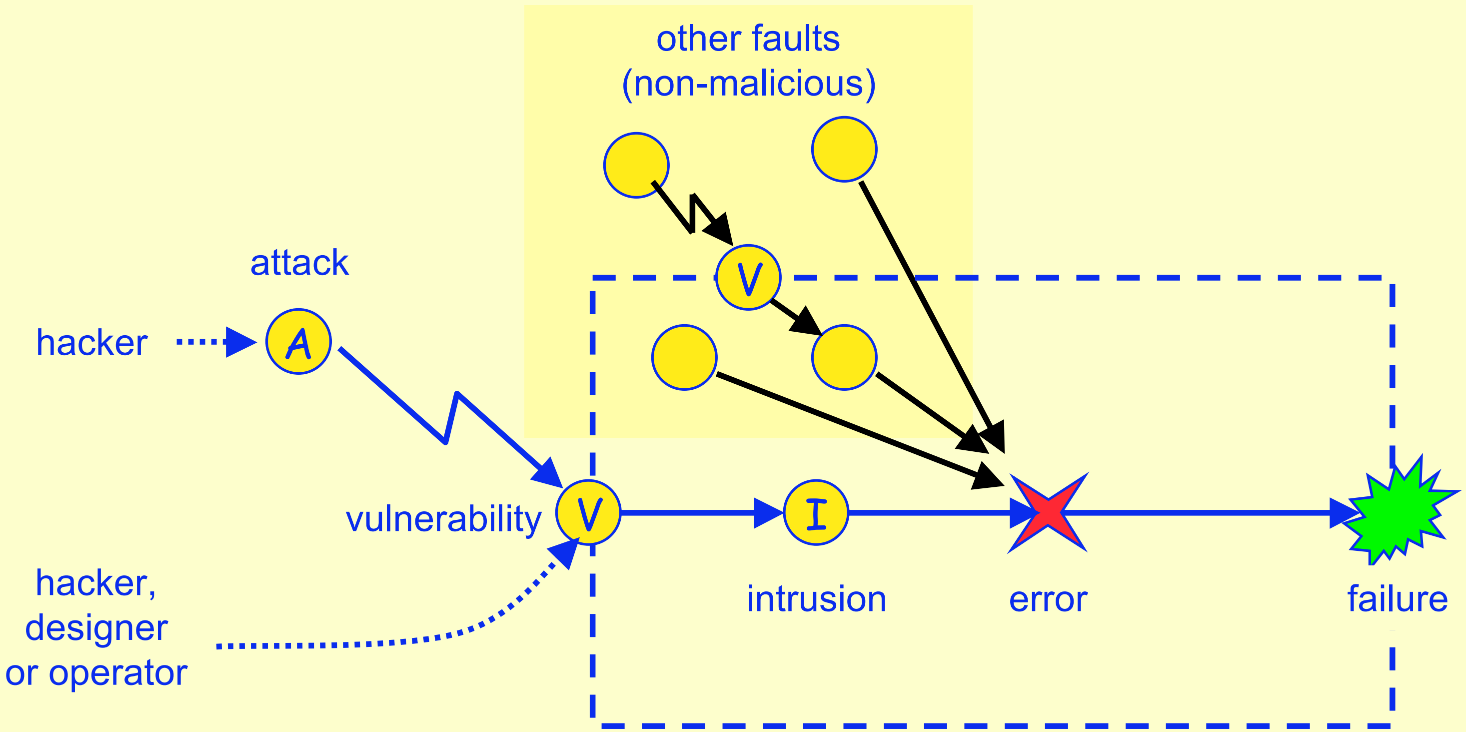
ist information society technologies **MAFTIA**

DARPA **OASIS**

Fault Tolerance



Fault Model



- **attack** - malicious external activity aiming to intentionally violate one or more security properties; an *intrusion* attempt
- **vulnerability** - a malicious or non-malicious fault, in the requirements, the specification, the design or the configuration of the system, or in the way it is used, that could be exploited to create an *intrusion*
- **intrusion** - a malicious fault resulting from an *attack* that has been successful in exploiting a *vulnerability*

Dependability Methods

PROVISION

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*

ASSESSMENT

Fault removal - how to reduce the presence (number, severity) of *faults*

Fault forecasting - how to estimate the presence, creation and consequences of *faults*

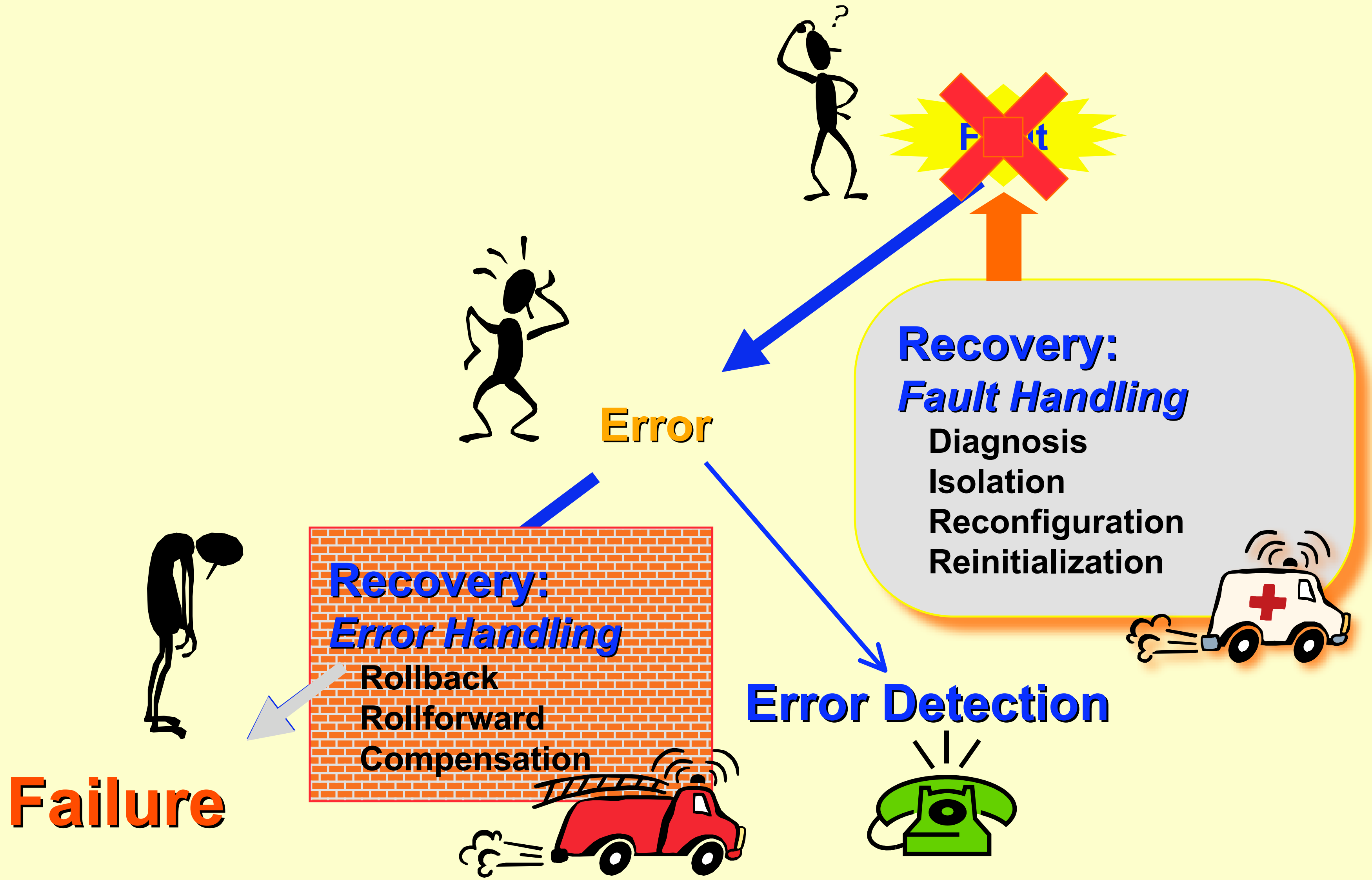
Fault avoidance

Fault acceptance

Security Methods

Fault	Attack (human sense)	Attack (technical sense)	Vulnerability	Intrusion
Prevention (how to prevent occurrence or introduction of…)	deterrence, laws, social pressure, secret service…	firewalls, authentication, authorization…	semi-formal and formal specification, rigorous design and management…	= attack & vulnerability prevention & removal
Tolerance (how to deliver correct service in the presence of…)	= vulnerability prevention & removal, intrusion tolerance		= attack prevention & removal, intrusion tolerance	error detection & recovery, fault masking, intrusion detection & response, fault handling
Removal (how to reduce number or severity of…)	physical countermeasures, capture of attacker	preventive & corrective maintenance aimed at removal of attack agents (i.e., some forms of malicious logic)	1. formal proof, model-checking, inspection, test… 2. preventive & corrective maintenance, including security patches	⊆ attack & vulnerability removal
Forecasting (how to estimate present number, future incidence, likely consequences of…)	intelligence gathering, threat assessment…	assessment of presence of latent attack agents, potential consequences of their activation	assessment of: presence of vulnerabilities, exploitation difficulty, potential consequences…	= vulnerability & attack forecasting

Fault Tolerance



Error Detection

Property checks

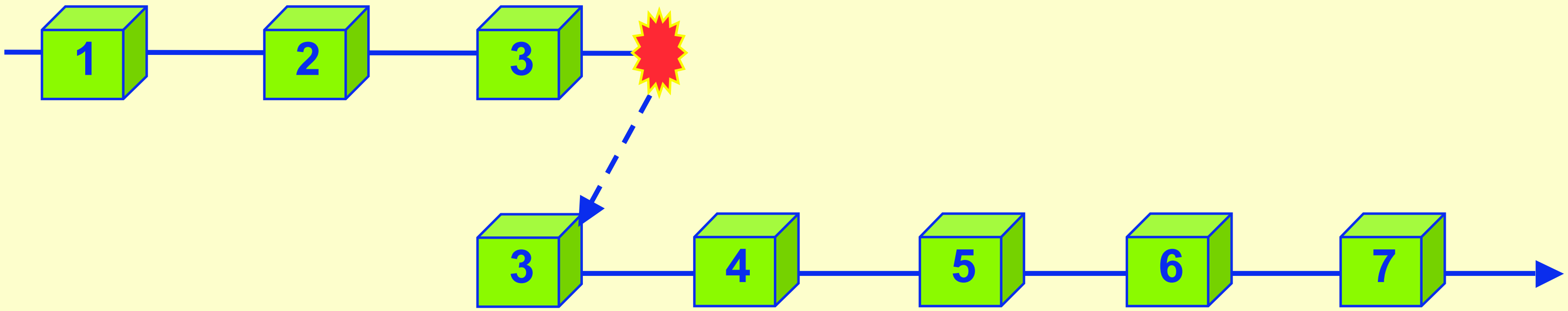
- System state/events satisfy properties or rules
  - inexistent/unauthorized instructions/commands
  - inexistent addresses
  - unauthorized access modes
  - watchdog timers
  - likelihood tests
  - error-detecting codes
  - run-time model checking
  - …
- Low redundancy overhead

Comparison checks

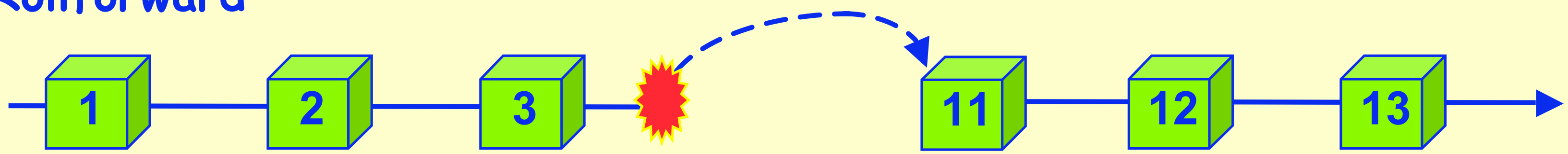
- Several executions in parallel or in series give same results
  - requires deterministic executions and identical inputs
  - assumes fault independence between executions
  - independence wrt design faults requires diversification
- High redundancy overhead

Error Handling

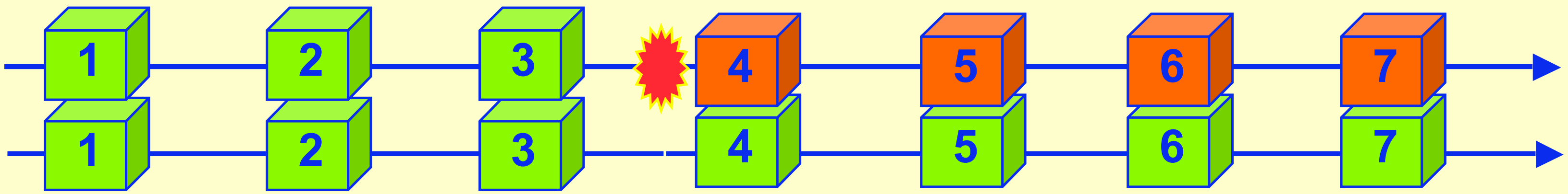
Rollback



Rollforward



Compensation (masking)

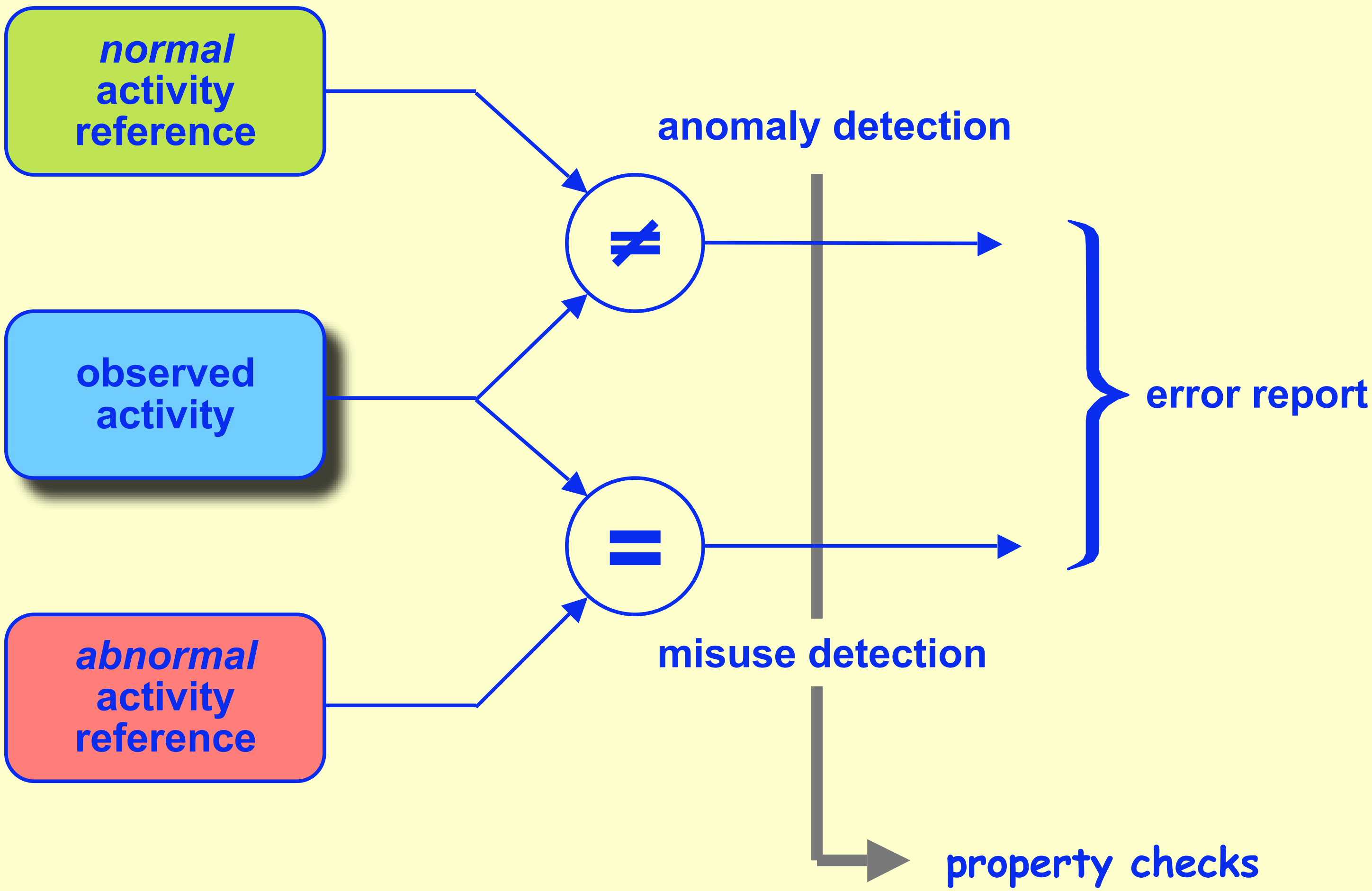


Intrusion Tolerance (IT)

- Intrusions are faults
- Faults can be tolerated
- But:
  - cannot rely on low likelihood of near-coincident attacks on different parts of system
- So, need to ensure that:
  - each part is sufficiently protected (no trivial attacks)
  - intrusion into one part does not facilitate intrusion into other parts
    - intrusion should not allow access to confidential data

Error Detection for IT

❖ Classic error detection + "intrusion" detection



Error Recovery for IT

Error Handling

- Rollback
  - restore from backups
  - system reboots
  - OS re-installation
  - TCP/IP connection resets
- Rollforward
  - rebuild healthy state?
  - switch to “safe” mode
- Compensation (masking)
  - voting mechanisms
  - ID sensor correlation
  - fragmentation-redundancy-scattering

Fault Handling

- Diagnosis
  - intrusions, vulnerabilities and attacks
- Isolation
  - corrupted zones
  - vulnerable software
- Reconfiguration
  - software downgrade & upgrade
  - voting threshold adjustment

Proactive Error Detection & Handling

- Check for latent errors and dormant faults

- For accidental faults
  - periodic (built-in) test
  - memory scrubbing

- Interpretation wrt malicious faults
  - vulnerability scanning
  - configuration checking
  - re-keying procedures

Intrusion Masking

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

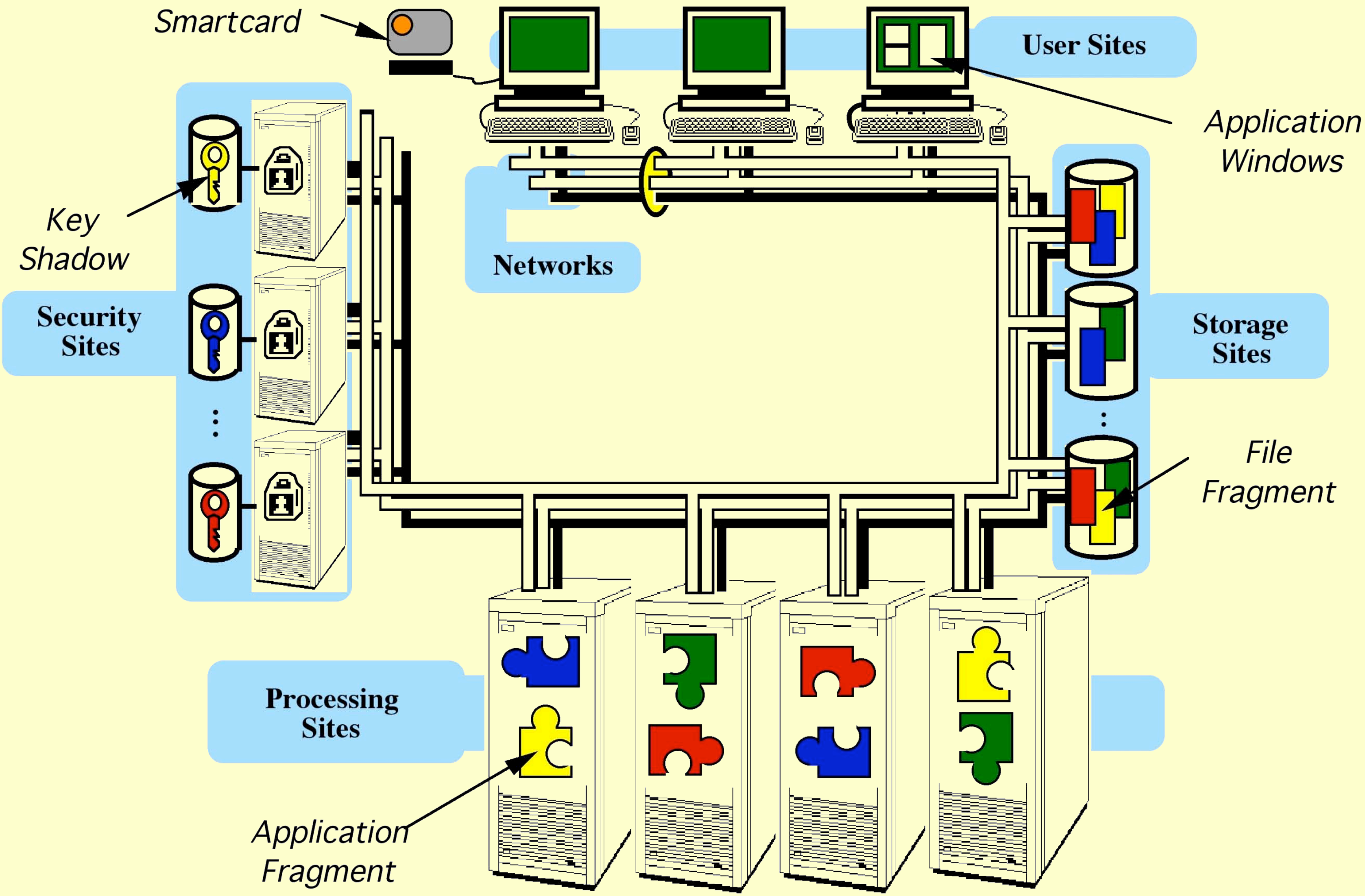
- FRS: Fragmentation-Redundancy-Scattering

  - 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

Fragmentation-Redundancy-Scattering



MAFTIA Project

FP5 IST Dependability Initiative

Cross Program Action

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
DSTL + QinetiQ (ex-DERA) (UK)	Tom McCutcheon, Sadie Creese
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 (Feb. 2003)

MAFTIA Achievements

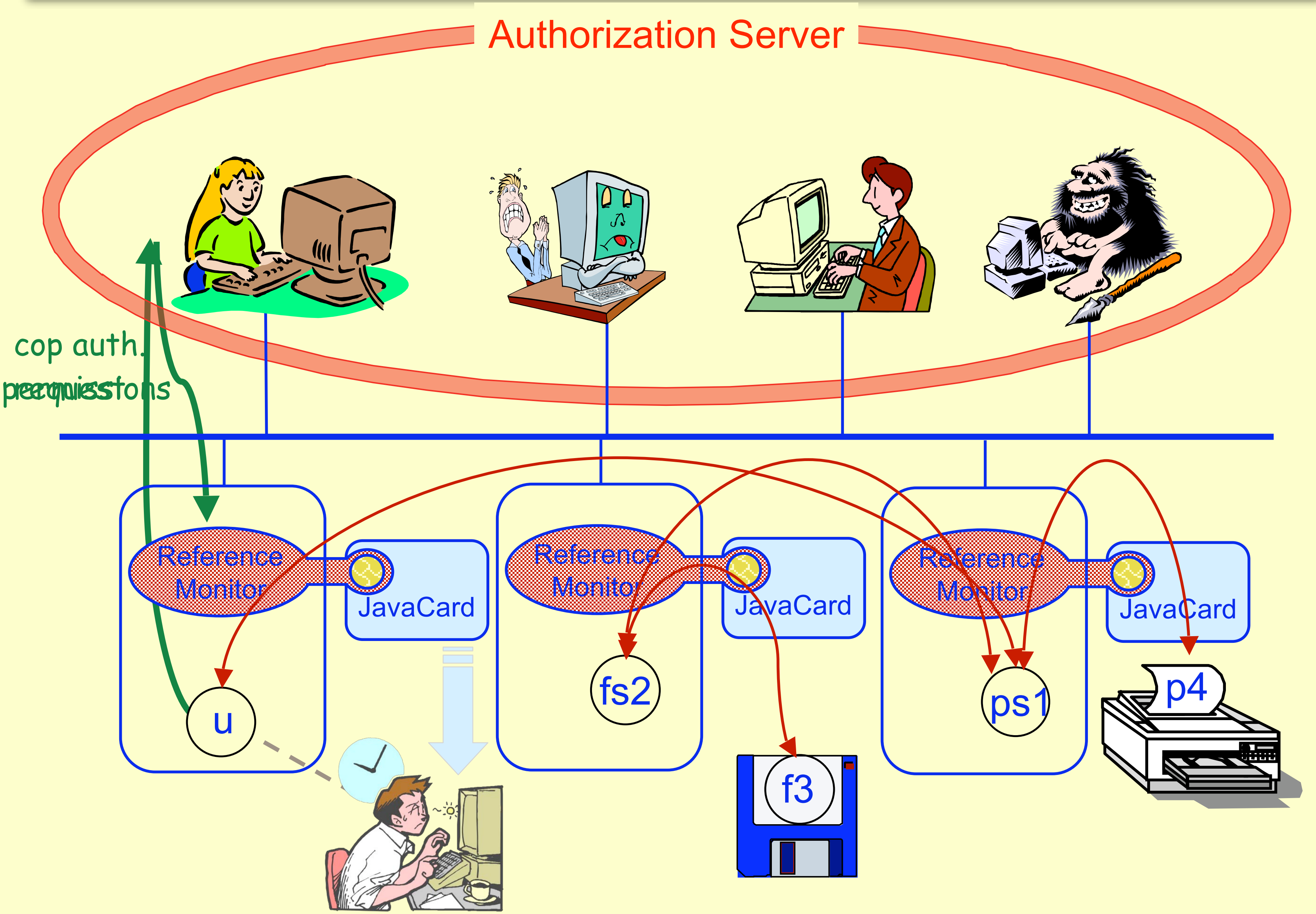
- Architectural framework and conceptual model

- Mechanisms and protocols:
  - dependable middleware
  - large scale intrusion detection systems
  - dependable trusted third parties
  - distributed authorization mechanisms

- Validation and assessment

http://www.maftia.org/

MAFTIA Authorization Scheme

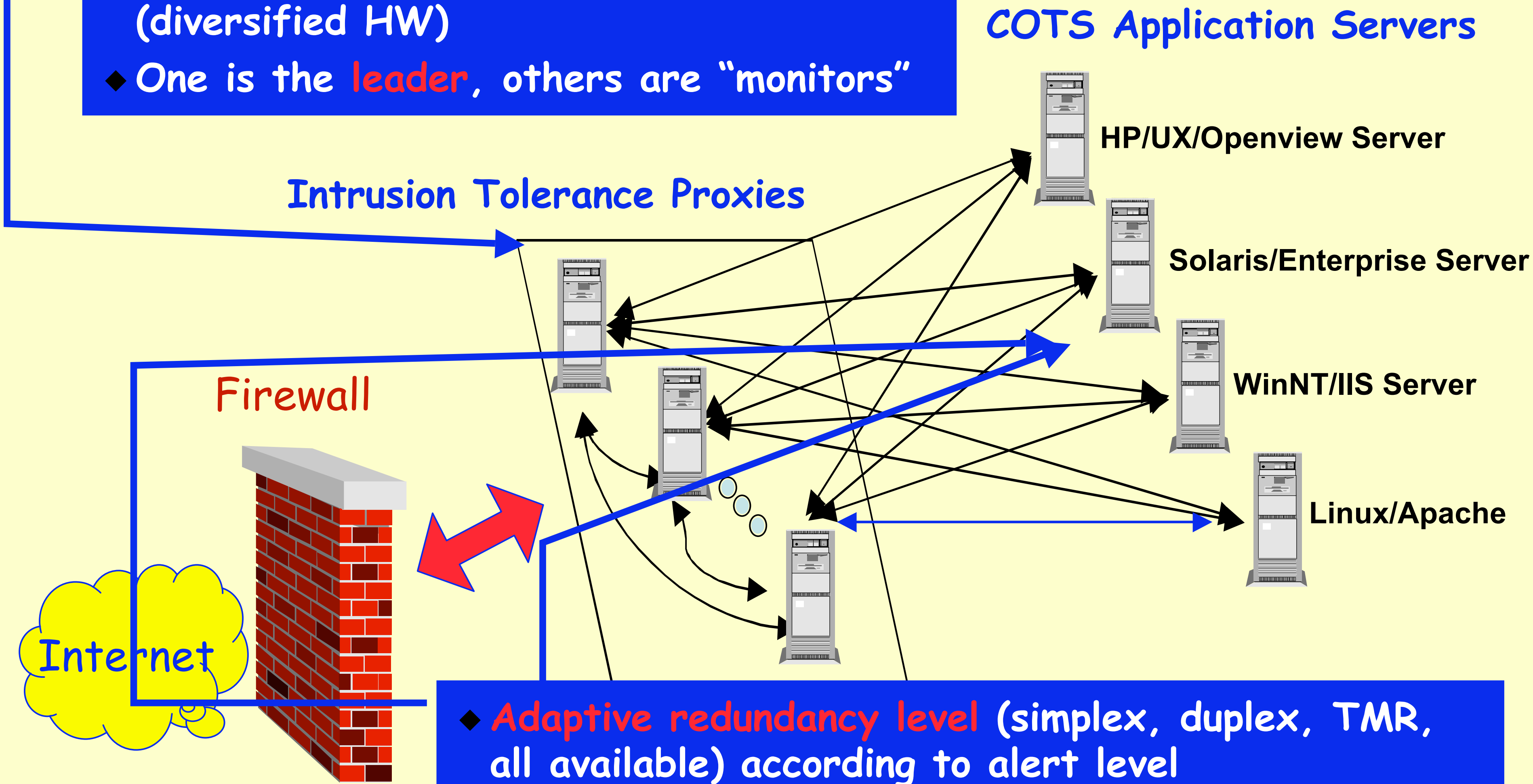


DIT Project

- DIT = Dependable Intrusion Tolerance
- DARPA OASIS (Organically Assured and Survivable Information Systems) program
- Partly sub-contracted to LAAS by SRI-International
- Design and implementation of a prototype intrusion-tolerant web server

DIT Architecture

- Purpose-built software on set of proxies (diversified HW)
- One is the leader, others are “monitors”



- Adaptive redundancy level (simplex, duplex, TMR, all available) according to alert level
- Alert level: info from CERTs… + on-line error detection: cross-checks, integrity checks, IDS…

Conclusion

- Given
  - current rate of attacks on Internet
  - large number of vulnerabilities in contemporary computing systems
- Intrusion tolerance is a promising technique
  - achievable with COTS
  - with moderate HW redundancy, some specific SW
- Not cheap
  - support of multiple, diverse platforms (vulnerability independence)
  - independent operators/administrators (tolerance of insider attacks)
- Price to pay for security in an open and uncertain world?