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

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

Fundamental Concepts of Dependability
[Avizienis, Laprie & Randell 2001]

Dependability: Basic Concepts and Terminology
[Laprie 1992]

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

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

Secure systems from insecure components
[Dobson & Randell 1986]

Intrusion-tolerant file system
[Fraga & Powell 1985]

Dependability as a generic concept
[Laprie 1985]
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)
University of Lisbon (P)
DERA, Malvern (UK)
University of Saarland (D)
LAAS-CNRS, Toulouse (F)
IBM Research, Zurich (CH)

- Brian Randell, Robert Stroud
  Paulo Verissimo
  Tom McCutcheon, Colin O’Halloran
  Birgit Pfitzmann
  Yves Deswarte, David Powell
  Marc Dacier, Michael Waidner

- c. 55 man-years, EU funding c. 2.5M€

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)

Authorisation

- **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


The Dependability Tree

- Attributes:
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability

- Impairments:
  - Fault
  - Error
  - Failure

- Methods:
  - Fault Prevention
  - Fault Tolerance
  - Fault Removal
  - Fault Forecasting

Security
The Dependability Tree

Attributes
- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability

Impairments
- Fault
- Error
- Failure

Methods
- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting

Are these attributes sufficient?

Attributes
- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability

Impairments
- Fault
- Error
- Failure

Methods
- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting
Security Properties

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

- Confidentiality
- Integrity
- Availability

\{
\text{Confidentiality} \\
\text{Integrity} \\
\text{Availability}
\} \quad \text{of} \quad \{ \text{Information} \\
\text{Meta-information} \}

\begin{align*}
\text{Accountability} & \quad A+I \\
\text{Anonymity} & \quad C \\
\text{Privacy} & \quad C \\
\text{Authenticity} & \quad I \\
\text{Non-repudiation} & \quad A+I
\end{align*}

\begin{itemize}
\item existence of operation
\item identity of person
\item personal data
\item message content
\item message origin
\item sender, receiver identity
\end{itemize}

The Dependability Tree

- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability

- Fault
- Error
- Failure

- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting

\text{Security}
Fault, Error & Failure

Error
that part of system state which may lead to a failure

Failure
occurs when delivered service deviates from implementing the system function

Example: Single Event Latchup

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

Cosmic Ray
External fault

Lack of shielding

Vulnerability
Internal, active fault

SEL
Internal, externally-induced fault

Satellite on-board computer
Intrusions

Intrusions result from (at least partially) successful attacks:

- External fault
- Internal, active fault
- Internal, externally-induced fault

Who are the intruders?

1: Outsider

- Outsider
- Authentication
- Authorization

2: User

- User
- Authentication
- Authorization

3: Privileged User

- 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

- **Computer Crime and Security Survey 2001 (Computer Security Institute and the FBI)**
  
  [http://www.gocsi.com/prelea_000321.htm](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

![Diagram](attachment:diagram.png)
The Dependability Tree

Dependability

- Attributes
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability

- Impairments
  - Fault
  - Error
  - Failure

Methods

- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting

Fault Tolerance

Fault Treatment

- Diagnosis
- Isolation
- Reconfiguration

Error Processing

- Damage assessment
- Detection & Recovery
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

User Sites

Storage Sites

Data Processing Sites

Networks

Application Windows

Smartcard

Key Shadows

Security Sites

File Fragment

File

Fragments

User Site

Multicast Network

Storage Sites

FRSed File Server

Fragmentation  Replication  Scattering

File Site  File Fragment  File Site  File Fragment  File Site  File Fragment  File Site  File Fragment  File Site  File Fragment  File Site  File Fragment

[Blain & Deswarte 1994]

[Deswarte et al. 1991]

[Deswarte et al. 1991]

[Fraga & Powell 1985]

[Fray et al. 1986]

[Fabre et al. 1994]
File Fragmentation

Fragment name := OWHF(file name, page #, frgt #, key)

FRSed Security Management

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

1. Smartcard Activation
2. Local Authentication
3. Global Decision
4. Session key distribution

Authorization

1. Request to open a session
2. Global Decision
3. tickets
4. direct access

Security Server

File name  ACL  Key shadow

Secured Servers
Fragmented Data Processing

Fault Tolerance

Error Processing
- Damage assessment
- Detection & Recovery

Failure

Fault Treatment
- Diagnosis
- Isolation
- Reconfiguration
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
references