MAFTIA

Yves Deswarte
LAAS-CNRS

DSN-2001 Special Track on the European Dependability Initiative
Göteborg, July 2, 2001
Motivation

- Large network infrastructures, such as the Internet, are vital for citizens to benefit from the Information Society.
- Development depends on how much the users will ‘trust’ the services.
- Such services must be made dependable, in particular w.r.t. malicious attacks by external hackers or by corrupt insiders.
MAFTIA: Malicious- and Accidental-Fault Tolerance for Internet Applications

- Systematic investigation of the 'tolerance paradigm' for constructing large-scale dependable distributed applications.
- Comprehensive approach for tolerating both accidental faults and malicious intrusions in such systems, including intrusions by external hackers and by corrupt insiders.
Contract Details

- Project Start Date: 1st Jan 2000
- Duration: 3 years
-Requested Funding: 2.5 M€
-No. of person years: 55
Partners

- Newcastle University (GB) (coordinator)
  Brian Randell, Robert Stroud

- DERA, Malvern (GB)
  Sadie Crees, Tom McCutcheon

- IBM, Zurich (CH)
  Christian Cachin, Marc Dacier, Michael Waidner

- LAAS-CNRS, Toulouse (F)
  Yves Deswarte, David Powell

- Universität des Saarlandes (D)
  André Adeslbach, Birgit Pfitzmann

- Universidade de Lisboa (P)
  Nuno Neves, Paulo Veríssimo
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)
The Dependability Tree

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

- Impairments:
  - Fault
  - Error
  - Failure

- Methods:
  - Fault Prevention
  - Fault Tolerance
  - Fault Removal
  - Fault Forecasting
The Dependability Tree

- Dependability
  - Impairments
    - Fault
    - Error
    - Failure
  - Methods
    - Fault Prevention
    - Fault Tolerance
    - Fault Removal
    - Fault Forecasting
  - Attributes
    - Availability
    - Reliability
    - Safety
    - Confidentiality
    - Integrity
    - Maintainability
  - Security
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

Dependability

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

- Impairments
  - Fault
  - Error
  - Failure

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

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

Intrusion
adjuged or hypothesized cause of an error
Example: Single Event Latchup

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

Lack of shielding

Vulnerability

Internal, active fault

SEL

Internal, externally-induced fault

External fault

Cosmic Ray
Intrusions result from (at least partially) successful attacks:

- **Internal, dormant fault Intrusions**
- **Internal, active fault Intrusions**
- **External fault**
- **Vulnerability**
  - account with default password
- **Intrusion**
  - Internal, externally-induced fault

Computing System
Fault, Error & Failure

- **Failure**: occurs when delivered service deviates from implementing the system function, violation of properties of security policy.
- **Error**: that part of system state which may lead to a failure, violation of rules of security policy.
- **Fault**: not explicitly defined in the diagram.
- **Attack**, **Intrusion**, **Bug**, **H/W fault**: causes of failure.
- **False positives in intrusion detection**: explains false positives in intrusion detection.
- **Adjuged or hypothesized cause of an error**: allows tolerance to be envisaged.
The Dependability Tree

Dependability

- Impairments
  - Fault
    - Error
    - Failure

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

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

Security
Fault Tolerance

Fault Treatment
- Diagnosis
- Isolation
- Reconfiguration

Error Processing
- Damage assessment
- Detection & Recovery
Error Processing

Backward recovery

Forward recovery

Compensation-based recovery (fault masking)
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
Fault Tolerance

Failure

Error Processing
- Damage assessment
- Detection & Recovery

Fault Treatment
- Diagnosis
- Isolation
- Reconfiguration

Fault

Error
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
  o Non-malicious or malicious (intrusion)
  o Attack (to allow retaliation)
  o Vulnerability (to allow removal)

❖ Isolation
  o Intrusion (to prevent further penetration)
  o Vulnerability (to prevent further intrusion)

❖ Reconfiguration
  o Contingency plan to degrade/restore service
    ▪ inc. attack retaliation, vulnerability removal
Intrusion-tolerance Structuring

Security administration (sub-)system

Component or (sub-)system

Error processing

Standalone sensors

Error detection

Error detection

A posteriori error detection

Error reports

Masking (FRS)

detection/recovery

Intrusion, attack and vulnerability isolation

System reconfiguration

Fault treatment

Security administration (sub-)system

Service user

Service

Insecurity signal

Intruder alert

System security officer (SSO)

Insecurity signal

Service

(from possible lower level)