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

Error

that part of system state which may lead to a failure

Intrusion

adjuged or hypothesized cause of an error

Failure
occurs when delivered service deviates from implementing the system function

Example: Single Event Upset

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

Cosmic Ray

External fault

Lack of shielding

Vulnerability

Internal, active fault

SEU

Internal, externally-induced fault

Satellite on-board computer
Intrusions

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

- **Internal, dormant fault**
- **Intrusions**
- **Internal, active fault**
- **External fault**
- **Account with default password**
- **Internal, externally-induced fault**

**Computing System**

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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability prevention</strong></td>
<td>how to prevent the occurrence or introduction of vulnerabilities</td>
</tr>
<tr>
<td><strong>Intrusion prevention</strong></td>
<td>how to prevent the occurrence of intrusions (vulnerability prevention + attack deterrence)</td>
</tr>
<tr>
<td><strong>Vulnerability tolerance</strong></td>
<td>synonym for intrusion tolerance</td>
</tr>
<tr>
<td><strong>Intrusion tolerance</strong></td>
<td>how to provide a service capable of or implementing the system function despite intrusions</td>
</tr>
<tr>
<td><strong>Vulnerability removal</strong></td>
<td>how to reduce the presence (number, severity) of vulnerabilities</td>
</tr>
<tr>
<td><strong>Intrusion removal</strong></td>
<td>not meaningful</td>
</tr>
<tr>
<td><strong>Vulnerability forecasting</strong></td>
<td>how to estimate the presence, creation and consequences of vulnerabilities</td>
</tr>
<tr>
<td><strong>Intrusion forecasting</strong></td>
<td>how to estimate the creation and consequences of intrusions (vulnerability + attack forecasting)</td>
</tr>
</tbody>
</table>

### Fault Tolerance

- **Error Processing**
  - Detection & Recovery
  - Masking

- **Fault Treatment**
  - Diagnosis
  - Isolation
  - Reconfiguration

- **Failure**
  - Error
  - Fault

- **Fault Treatment**
  - Error Processing
  - Fault Treatment
Intrusion tolerance

- Error processing:
  - Intrusion-symptom detection + recovery
  - Intrusion masking

- Fault treatment
  - Intrusion diagnosis (+ retaliation?)
  - Vulnerability removal

Intrusion Masking: Delta-4 (86-96)

[Blain & Deswarte 1994]

User Sites

Application
Windows

Storage
Sites

Networks

Application
Fragment

File
Fragment

Data Processing
Sites

Key
Shadows

[Deswarte et al. 1991]

Smartcard

[Blain & Deswarte 1994]

[Fraga & Powell 1985]

[Fray et al. 1986]

[Fabre et al. 1994]
Ideal Fault-tolerant Component Administration

- Component or (sub-)system
- Error processing
- Fault diagnosis
- Faulty unit isolation and system reconfiguration

Service user

Exception

API

Error reports

Error detection

Recovery

Detection/recovery

Fault treatment

Intrusion Tolerant Component Security Administration

- Component or (sub-)system
- Error processing
- Intrusion diagnosis
- Intrusion isolation and system reconfiguration

Service user

Exception

API

Error reports

Error detection

Recovery

Detection/recovery

Fault treatment

System security officer (SSO)
References


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