Dependability Concepts for Malicious Faults

David Powell & Yves Deswarte

Dependability & Survivability Workshop
IFIP WG 10.4 meeting, Hilton Head Island, SC, USA
27 June - 1 July 2002
Aim

Dependability: Basic Concepts & Terminology
IFIP WG 10.4
J.C. Laprie (Ed.)

Glossary of Terms Used in Security & Intrusion Detection
National Security Agency

Conceptual Model

http://www.research.ec.org/maftia/
Dependability: Basic Concepts & Terminology
IFIP WG 10.4
J.C. Laprie (Ed.)

Glossary of Terms Used in Security & Intrusion Detection
National Security Agency

Conceptual Model
http://www.research.ec.org/maftia/
Summary

- Causal chain of impairments
- Security policy and security failure
- Intrusion, attack and vulnerability
- Security methods
- Intrusion detection
- Fault tolerance
- Integrated intrusion detection/tolerance framework
Causal Chain of Impairments

Fault

Error

that part of system “state” which may lead to a failure

Failure

occurs when delivered service deviates from implementing the system function

Error

adjudged or hypothesized cause of an error
Causal Chain of Impairments

Need to distinguish since detectable phenomenon (error) may have ≥ 1 cause

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

Failure occurs when delivered service deviates from implementing the system function

Fault adjudged or hypothesized cause of an error
Causal Chain of Impairments

Fault

adjudged or hypothesized cause of an error

Error

that part of system “state” which may lead to a failure

Failure

occurs when delivered service deviates from implementing the system function

Need to distinguish since detectable phenomenon (error) may have ≥ 1 cause

Need to distinguish since, otherwise, tolerance would be unattainable goal
Security Policy
Security Policy

- Security properties which are to be fulfilled by the system

Confidentiality
Integrity
Availability
Security Policy

- Security properties which are to be fulfilled by the system
- Rules according to which the system security state may evolve

Confidentiality

Integrity

Availability

- Thou shalt not...
- ...
- ...
- ...
- Thou shalt...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
Security Failure

Confidentiality

Integrity

Availability

• Thou shalt not...
  ...
  ...
  ...
  ...
  ...

• Thou shalt...
  ...
  ...
  ...
  ...
  ...
  ...
Security Failure

- Violation of a security property of intended security policy

- Confidentiality
- Integrity
- Availability

- Thou shalt not...
- ...
- ...
- ...
- Thou shalt...
- ...
- ...
- ...
- ...
Security Failure

- Violation of a security property of intended security policy

Confidentiality

Integrity

Availability

antagonistic

- Thou shalt not...
- ...
- ...
- ...
- Thou shalt...
- ...
- ...
- ...
- ...
Security Failure

- Violation of a security property of intended security policy

Confidentiality  
Integrity  
Availability

antagonistic

contradictory

• Thou shalt not...
  ...
  ...
  ...
  ...

• Thou shalt...
  ...
  ...
  ...
  ...
  ...
  ...
  ...
  ...
  ...
  ...
  ...

Thou shalt not...
Security Failure

- Violation of a security property of intended security policy.
Fault Model

intrusion → error → failure
Fault Model

other faults (non-malicious)

intrusion
error
failure
Fault Model

- Hacker
- Vulnerability
- Attack
- Intrusion
- Error
- Failure

hacker, designer or operator
- **attack** - malicious external activity aiming to intentionally violate one or more security properties; an *intrusion* attempt
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*
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 interaction fault resulting from an *attack* that has been successful in exploiting a *vulnerability*
Fault Model: Recursion
Fault Model: Recursion?

- Human malice
- Social system
- Human mistake
- Administration system
- Authentication & authorization system

Relations:
- “exploits”
- “causes”
- “is interpreted as”
Fault Model: Propagation?
Fault Model: Propagation?

- Attack (human activity)
- Attack (computational activity)
Outsiders or Insiders: Privilege

universe of object-operation pairs

D: an object-operation domain
Outsiders or Insiders: Privilege

universe of object-operation pairs

A: privilege of user a

D: an object-operation domain
Outsiders or Insiders: Privilege

A: privilege of user a

B: privilege of user b

D: an object-operation domain

universe of object-operation pairs
Outsiders or Insiders: Privilege

- Theft of privilege: unauthorized increase in privilege
Theft of privilege: unauthorized increase in privilege

Abuse of privilege: improper use of authorized operations
Outsiders or Insiders: Privilege

- **Theft of privilege**: unauthorized increase in privilege
- **Abuse of privilege**: improper use of authorized operations
- **Outsider**: current privilege does not intersect considered domain

A: privilege of user a
B: privilege of user b
D: an object-operation domain

universe of object-operation pairs
Outsiders or Insiders: Privilege

- **Theft of privilege**: unauthorized increase in privilege
- **Abuse of privilege**: improper use of authorized operations
- **Outsider**: current privilege does not intersect considered domain
- **Insider**: current privilege intersects considered domain
Dependability Methods
### Security Methods

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Attack</th>
<th>Vulnerability</th>
<th>Intrusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>how to prevent the occurrence or introduction of...</td>
<td>deterrence, laws, social pressure, secret service...</td>
<td>security policy, semi-formal and formal specification, rigorous design and management...</td>
<td>firewalls, authentication, authorization... (+ attack prevention vulnerability prevention)</td>
</tr>
<tr>
<td>Tolerance</td>
<td>vulnerability prevention vulnerability removal intrusion tolerance</td>
<td>= intrusion tolerance</td>
<td>confinement, detection/recovery, masking (eg FRS), + intrusion detection for fault treatment</td>
</tr>
<tr>
<td>how to provide a service capable of or implementing the system function despite...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removal</td>
<td>not applicable</td>
<td>formal proof, model-checking, inspection, test...</td>
<td>not applicable</td>
</tr>
<tr>
<td>how to reduce the presence (number, severity) of...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forecasting</td>
<td>intelligence gathering, threat assessment, attack warning...</td>
<td>assess presence of vulnerabilities, exploitation difficulty, potential consequences</td>
<td>vulnerability forecasting, attack forecasting</td>
</tr>
<tr>
<td>how to estimate the creation and consequences of...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Security Methods

<table>
<thead>
<tr>
<th></th>
<th>Attack</th>
<th>Vulnerability</th>
<th>Intrusion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prevention</strong></td>
<td>how to prevent the occurrence or introduction of...</td>
<td>deterrence, laws, social pressure, secret service...</td>
<td>security policy, semi-formal and formal specification, rigorous design and management...</td>
</tr>
<tr>
<td><strong>Tolerance</strong></td>
<td>how to provide a service capable of or implementing the system function despite...</td>
<td>vulnerability prevention vulnerability removal intrusion tolerance</td>
<td>= intrusion tolerance</td>
</tr>
<tr>
<td><strong>Removal</strong></td>
<td>how to reduce the presence (number, severity) of...</td>
<td>not applicable</td>
<td>formal proof, model-checking, inspection, test...</td>
</tr>
<tr>
<td><strong>Forecasting</strong></td>
<td>how to estimate the creation and consequences of...</td>
<td>intelligence gathering, threat assessment, attack warning...</td>
<td>assess presence of vulnerabilities, exploitation difficulty, potential consequences</td>
</tr>
</tbody>
</table>

- **firewalls**, **authentication**, **authorization...**
- (+ attack prevention vulnerability prevention)
- confinement, detection/recovery, masking (eg FRS), + intrusion detection for fault treatment
- **deterrence**, **laws**, **social pressure**, **secret service...**
- **intelligence gathering**, **threat assessment**, **attack warning...**
- vulnerability prevention, removal, intrusion tolerance
Prevention, Tolerance and Removal
Intrusion Detection: Purpose
Intrusion Detection: Purpose

- Intrusive behavior => alarms
Intrusion Detection: Purpose

- Intrusive behavior => alarms
- Alarms
Intrusion Detection: Purpose

- Intrusive behavior => alarms
- Alarms
  - to a system security officer (SSO), to gather information about attacks, vulnerabilities and intrusions, and possibly to initiate manual countermeasures and/or litigation, retaliation
Intrusion Detection: Purpose

- Intrusive behavior => alarms
- Alarms
  - to a system security officer (SSO), to gather information about attacks, vulnerabilities and intrusions, and possibly to initiate manual countermeasures and/or litigation, retaliation
  - to an automatic countermeasure mechanism in order to avert security failures, i.e., to tolerate intrusions
Intrusion Detection: Purpose

- Intrusive behavior => alarms
- Alarms
  - to a system security officer (SSO), to gather information about attacks, vulnerabilities and intrusions, and possibly to initiate manual countermeasures and/or litigation, retaliation
  - to an automatic countermeasure mechanism in order to avert security failures, i.e., to tolerate intrusions

- Response to intrusion is not part of intrusion detection!
Intrusion Detection: Definition
Intrusion Detection: Definition

[NSA 1998]

“Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network“
Intrusion Detection: Definition

[NSA 1998]

“Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.”

**Intrusion detection:** concerns the set of practices and mechanisms used towards:

- detection of errors that may lead to security failure
- diagnosing intrusions, vulnerabilities and attacks
Intrusion Detection: Definition

[NSA 1998]

“Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.”

intrusion detection: concerns the set of practices and mechanisms used towards:
- detection of errors that may lead to security failure
- diagnosing intrusions, vulnerabilities and attacks

intrusion detection system: is an implementation of the practices and mechanisms of intrusion detection
ID Topology

Activity

Sensor

Sensor

Sensor

Event Analyzer

Event Analyzer

Event Analyzer

Event Analyzer

Event Analyzer

Event Analyzer
Fault Tolerance

Fault

Error

Failure

Failure
Fault Tolerance

Failure

Error Processing
- Error detection
- Damage assessment
- Error recovery

Fault

Error

Error Processing

Error detection
Damage assessment
Error recovery
Fault Tolerance

Failure

Error Processing
- Error detection
- Damage assessment
- Error recovery

Fault Treatment
- Fault diagnosis
- Fault isolation
- Reconfiguration

Fault
Error Detection

- normal activity reference
- observed activity
- abnormal activity reference

= anomaly detection
≠ error report
= misuse detection
Error Detection

Could be, e.g., activity according to rules specified in security policy

normal activity reference

observed activity

abnormal activity reference

anomaly detection

error report

misuse detection
Anomaly vs Misuse Detection

- Normal
- Abnormal
Anomaly vs Misuse Detection
Anomaly vs Misuse Detection

NEAR IDEAL

REALITY
Anomaly vs Misuse Detection

Correctly declared as normal

Near Ideal

Reality

Hit
Anomaly vs Misuse Detection

Correctly declared as normal

Near Ideal

Reality

Miss

Hit

False alarm
Anomaly vs Misuse Detection

Ordinary

Correctly declared as normal

Near Ideal

Misuse detection

REALITY

Miss

Hit

False alarm
Anomaly vs Misuse Detection

Anomaly detection

Misuse detection

NEAR IDEAL

correctly declared as normal

?!

REALITY

miss

hit

false alarm
Preemptive Error Detection

[Avizienis, Laprie & Randell 2001]
(as opposed to concurrent error detection)

- Core concepts: AKA “built-in test”
  - Memory scrubbing
  - Software rejuvenation

- Interpretation wrt malicious faults
  - Vulnerability scanning
  - Configuration checking
(Damage assessment)

- **Core concepts:** aims to evaluate extent of error propagation before initiating recovery
  - How many checkpoints to rollback?
  - How many processes affected before detection?

- **Interpretation?**
  - How many files have been corrupted by an intruder, and thus need to be restored *before use?*
Error Recovery
Error Recovery

Backward recovery
Error Recovery

Backward recovery

Forward recovery
Error Recovery

Backward recovery

Forward recovery

Compensation-based recovery (fault masking)
Error Recovery
Error Recovery

- Backward recovery
  - Operating system re-installation
  - TCP/IP connection resets
  - System reboots and process re-initialisation
  - Software downgrades
Error Recovery

- **Backward recovery**
  - Operating system re-installation
  - TCP/IP connection resets
  - System reboots and process re-initialisation
  - Software downgrades

- **Forward recovery**
  - Automated re-keying procedures
  - Switching to diminished “safe” mode.
  - Software upgrades
Error Recovery

- **Backward recovery**
  - Operating system re-installation
  - TCP/IP connection resets
  - System reboots and process re-initialisation
  - Software downgrades

- **Forward recovery**
  - Automated re-keying procedures
  - Switching to diminished “safe” mode.
  - Software upgrades

- **Masking**
  - Voting mechanisms
  - Fragmentation-Redundancy-Scattering
  - Sensor correlation
Fault Tolerance

Error Processing
- Error detection
- Damage assessment
- Error recovery

Fault Treatment
- Fault diagnosis
- Fault isolation
- Reconfiguration

Failure

Fault
Fault Diagnosis

- Core concepts: identification and locations of faults; prerequisite to isolation & reconfiguration
- **Intrusion diagnosis**, i.e., trying to assess the degree of success of the intruder in terms of system penetration
- **Vulnerability diagnosis**, i.e., trying to understand the channels through which the intrusion took place so that corrective maintenance can be carried out
  (diagnosis immediate if errors signaled by vulnerability scanner or configuration checker)
- **Attack diagnosis**, i.e., finding out who or what organisation is responsible for the attack in order that appropriate litigation or retaliation may be initiated
Fault Isolation

- Core concepts: needed to prevent further errors
- Interpretation wrt intrusions
  - Blocking traffic from an intrusion containment domain that is diagnosed as corrupt, by, for example, changing the settings of firewalls or routers
  - Removing a corrupted file from the system
- Interpretation wrt root causes (vulnerability/attack)
  - Taking off line software versions with newly-found vulnerabilities
  - Arresting the attacker
System Reconfiguration

- Core concepts: redeployment of fault-free resources + corrective maintenance

- Interpretation wrt intrusions
  - Change a voting threshold, e.g., $3/5 \Rightarrow 2/3$ after 2 corruptions
  - Deployment of countermeasures, inc. probes and traps

- Corrective maintenance actions
  - Vulnerability removal
    - software revision and upgrade
    - security patches
  - Attacker rehabilitation
Integrated Intrusion Detection/Tolerance Framework
Integrated Intrusion Detection/Tolerance Framework
Integrated Intrusion Detection/Tolerance Framework component or (sub-)system security administration (sub-)system
Integrated Intrusion Detection/Tolerance Framework

component or (sub-)system

security administration (sub-)system

detection/recovery intrusion-tolerance

error detection

recovery
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

Masking intrusion-tolerance

Detection/recovery intrusion-tolerance

Error detection

Recovery

Security administration (sub-)system
Integrated Intrusion Detection/Tolerance Framework

- Component or (sub-)system
  - Error and event reports
  - Event analysis
  - Error detection
  - Recovery
  - Intrusion-tolerance
  - Masking

- Security administration (sub-)system
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

Error and event reports

Event analysis

External sensor

Internal sensor

Error detection

A posteriori error detection

Masking intrusion-tolerance

Error detection

Detection/recovery intrusion-tolerance

Recovery

Security administration (sub-)system
Integrated Intrusion Detection/Tolerance Framework

- Component or (sub-)system
- Security administration (sub-)system
- Error and event reports
- Event analysis
- Error detection
- Recovery
- Intrusion-tolerance masking
  - Internal sensor
  - External sensor
  - A posteriori error detection
  - Error detection/recovery intrusion-tolerance

Diagram shows the flow of data from sensors to event analysis and back to security administration.
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

Error and event reports

External sensor

Internal sensor

Error detection

A posteriori error detection

Masking intrusion-tolerance

Detection/recovery intrusion-tolerance

Error detection

Recovery

Event analysis

Fault diagnosis (inc. intrusions, attacks and vulnerabilities)

Security administration (sub-)system

Intruder alert

System security officer (SSO)
Integrated Intrusion Detection/Tolerance Framework

- Component or (sub-)system
- Error and event reports
- Event analysis
- A posteriori error detection
- Intrusion-tolerance masking
- Detection/recovery intrusion-tolerance
- Recovery
- Fault diagnosis (inc. intrusions, attacks and vulnerabilities)
- Fault isolation (inc. intrusions, attacks and vulnerabilities)
- System reconfiguration
- Security administration (sub-)system
- Intruder alert
- System security officer (SSO)
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

- Error and event reports
  - External sensor
  - Internal sensor
  - Error detection
    - A posteriori intrusion-tolerance
    - Detection/recovery intrusion-tolerance
  - Recovery
- Event analysis
- Fault diagnosis (inc. intrusions, attacks and vulnerabilities)
- Fault isolation (inc. intrusions, attacks and vulnerabilities)
- System reconfiguration
- Intruder alert

Security administration (sub-)system

System security officer (SSO)
Integrated Intrusion Detection/Tolerance Framework

- Internal sensor
- External sensor
- Error detection
- A posteriori error detection
- Masking intrusion-tolerance
- Detection/recovery intrusion-tolerance
- Error and event reports
- Event analysis
- Fault isolation (inc. intrusions, attacks and vulnerabilities)
- Fault diagnosis (inc. intrusions, attacks and vulnerabilities)
- System reconfiguration
- Security administration (sub-)system
- Error processing
- Recovery
- Fault treatment
- Intruder alert
- System security officer (SSO)
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

Service user

API

Error processing

Event analysis

Fault treatment

Fault diagnosis (inc. intrusions, attacks and vulnerabilities)

Fault isolation (inc. intrusions, attacks and vulnerabilities)

System reconfiguration

Security administration (sub-)system

Error and event reports

Detection/recovery intrusion-tolerance

Masking intrusion-tolerance

Detection of error

Recovery

Service

(Intrusion-tolerance (from possible lower level))

Service user

System security officer (SSO)

Intruder alert

Error and event reports

Internal sensor

External sensor

A posteriori error detection

Recovery

Fault treatment

Detection/aposteriori intrusion-tolerance

Error detection

Masking intrusion-tolerance

Error and event reports

Service

(from possible lower level)
Integrated Intrusion Detection/Tolerance Framework

Component or (sub-)system

Service user

API

Error processing

Fault treatment

Event analysis

Fault diagnosis (inc. intrusions, attacks and vulnerabilities)

Fault isolation (inc. intrusions, attacks and vulnerabilities)

System reconfiguration

Security administration (sub-)system

Error and event reports

Detection/recovery intrusion-tolerance

Masking intrusion-tolerance

Service (from possible lower level)

Insecurity signal

Intruder alert

System security officer (SSO)
A (very) Simple Example
Security Properties

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

Confidentiality

Integrity

Availability

Data

Meta-data
Security Properties

Confidentiality

Integrity

Availability

personal data
message content
etc.

identity of person
message origin
sender, receiver identity
existence of operation
etc.
Security Properties

- Anonymity
  - personal data
  - message content
  - identity of person
  - message origin
  - sender, receiver identity
  - existence of operation
  - etc.

- Confidentiality
- Integrity
- Availability
Security Properties

- Confidentiality
- Integrity
- Availability

Privacy

- personal data
  - message content
    - etc.
- identity of person
  - message origin
  - sender, receiver identity
  - existence of operation
    - etc.
Security Properties

- Authenticity
  - personal data
  - message content
  - identity of person
  - message origin
  - sender, receiver identity
  - existence of operation
  - etc.

- Confidentiality
- Integrity
- Availability
Security Properties

- Non-repudiability
- Confidentiality
- Integrity
- Availability

personal data
message content
identity of person
message origin
sender, receiver identity
existence of operation
etc.
Security Properties

- **Confidentiality**
- **Integrity**
- **Availability**

- **Accountability**
  - personal data
  - message content
  - etc.
  - identity of person
  - message origin
  - sender, receiver identity
  - existence of operation
  - etc.
ID Event Generator

- **Target**: monitored component
- **Sensor**: raw data collector (e.g., sniffer, audit log)
- **Deployment trade-offs**
  - Sensitivity: false alarms vs. misses
  - Deployment: ease vs. completeness
  - User rights: privacy vs. visibility
  - Encryption: attacker view vs. system-administration view
ID Event Analysis

- Successively transform, filter, normalize, and correlate data, adding semantic relevance and reducing volume at each stage
- Single event analysis box
  - May take its input from several different producers (both from sensor boxes and other event analysis boxes)
  - May feed its output to several different consumers in a topologically arbitrary manner
ID Event Database

- Provides persistence to IDS
  - Off-line error detection
  - Intrusion analysis
  - Evidence justifying response

- Text file or relational database
- Need to be able to view data with varying degrees of resolution