M2 CyberSecurity
Threat and Risk Analysis, IT Security Audit and Norms

Security Assessment of Information System
Standards, Methods and Tools

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Objectives

- Introduction to Standards, Methods and Tools used to assess Security of Information System
  - Network or System Administrator
  - Developer
  - IT Security Professional
  - Consultant
  - Auditor
  - Security Analyst
  - CISO – Chief Information Security Officer

This Course is NOT

- Not a complete course on IT Security
- Not a complete course on IT Security Standards
- Not a complete course on IT Security Audit

Neither …

SECUR IMAG

The security team of Ensimag

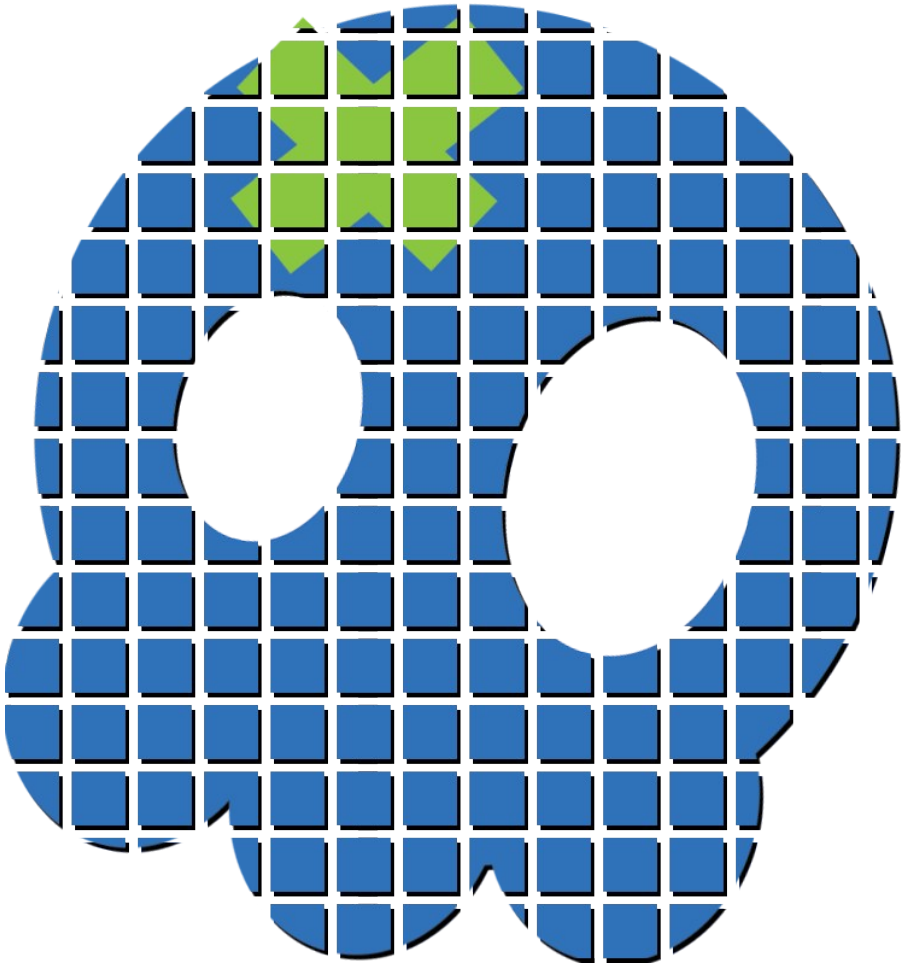
Réunion de rentrée : 29/09 – 17h30

amphi de présentation - Ensimag

Challenges divers : reverse, crypto, exploit, forensic, ...

Plus d'infos sur https://securimag.org

Meet you in Grenoble on Nov 18th



Lectures

- Introduction
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, EBIOS, Mehari,
- Tools
  - Nessus/OpenVAS, nmap, wireshark, ntop, metasploit...
- Hand-on Labs

Tutoring / Exercices

- Availibility Model
- Security Mindset :Think as an attacker
- Risk Analysis (various scenarios)
- Attack Presentation : technical description and root cause analysis
- Attack Tree
- Inventory of Security Tools (Group work)

Practical Works

- TP1 Auditing and securing your own environment
- TP2 Software Vulnerability Patterns
- TP3 Advanced BOF (and ROP)
- TP4 Web exploitation
- TP5 Attack/Defense Game

Evaluation

- Evaluation for this class will be based on:
  - 20% - the exercices of the tutoring sessions, all of them submitted in a final report (M2CySecAudit-Exercices-<name>.pdf)
  - 30% - Individual reports from the Hand-on Labs (M2CySecAudit-TP<num>-<name>.pdf)
  - 50% - Final Exam

As well as your **attendance** to the Industrial Talks. (CC)

Books – recommended readings

- Bruce Schneier's blog

  http://schneier.com/blog

- 'Security Engineering, 2nd ed', Ross Anderson

  http://www.cl.cam.ac.uk/~rja14/book.html

- 'Thinking Security' , Steven Bellovin

  http://schneier.com/blog

Contact information

- florent.autreau@imag.fr
- Available on appointment
    - UFRIM²AG - F314
- Lecture material available on forge (*after* each lecture ... and when access will be granted to students and teacher!)

Agenda – Day 1 – Sep 26th

- Introduction
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - Nessus, nmap, wireshark, ntop, metasploit...
- Hand-on Labs

Outline

- *Introduction*
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - Nessus, nmap, wireshark, ntop, ...
- Hand-on Labs

Information Security

- A set of properties for information
  - Confidentiality,
  - Integrity,
  - Availability.
    - The classical CIA triangle
- *Goal : insure that Information is always Available ONLY to Authorized People*

Information Security (cont)

- A different set of properties for information
  - Confidentiality,
  - Control,
  - Integrity,
  - Authenticity,
  - Utility,
  - Availability.

Information Security (cont)

- Other properties of Information System to be considered :
  - Accessibility,
  - Performance,
  - Usability,
  - Manageability,
  - Last and not least Reliability.

Information System

- Conventional Support for Information
  - Desktop,
  - Server,
  - Network Equipment (switches, routers, ...)
  - Printer,
  - Laptop,
  - ...

Information System(2)

- Also :
  - Professional and personal Mobile Phone,
  - Phone System (including PABX or VoIP gears),
  - Assistant (PDA),
  - Connexion Card, Access Token,
  - USB Keys,
  - MP3 reader, Game System,
  - Credit Card, ...

Business Assets

- Availability

  Make sure that IT services and resources are available for accredited users (employees, customers, partners, contractors).

- Integrity

  Make sure that information as well as information processing is exact, reliable, trusted and eventually provable.

Business Assets (cont.)

- Confidentiality

  Make sure that IT services and resources are ONLY available to accredited users .

- Authenticity (authentication and integrity)
- Traceability, Auditability, Non-repudiation
- Reputation / Branding
- Liability

Employee's Assets

- Employee's Liability
- Personal Information
  - Political Opinion
  - Member of Work Union
  - Job Search
- Reputation / Fame

Citizen's Assets

- Privacy
  - Political opinion,
  - Religion,
  - Health, Medical Data,
  - Confidentiality (ex: Taxes),
  - Reputation (rumors), Honor
- Yours (Family, Relatives, Significant Others)
  - Personal information on forum

Citizen's Assets (cont.)

- Sensitive and/or Confidential Information
  - Codes
  - Documents related to Associations, Union
  - Accounting and Banking information
  - Passwords, Account information
- Liability
- Fame, Reputation

About Availability

Terminology

- **Fault** Defect, imperfection or fault that occurs in hardware or software.
- **Error** Occurrence of an incorrect value in some unit of information within a system. Manifestation of a fault.
- **Failure** Deviation in the expected performance of a system.

Terminology (cont.)

- **Detection** - Recognising that a fault/error has occurred.
- **Containment/Isolation** - Isolating a fault and preventing its propagation throughout a system.
- **Recovery** - Restoring the system to a stable (operational) state.
- **Repair** - Repairing a faulty FRU

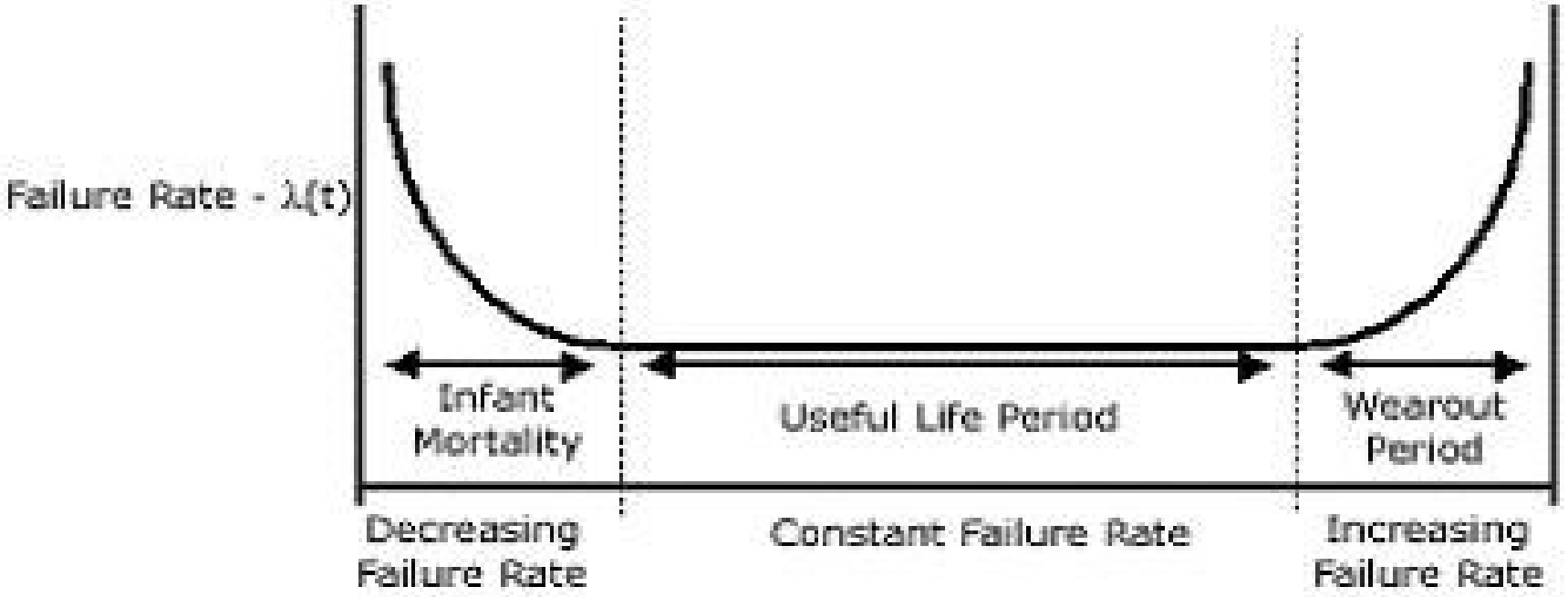
Reliability & Availability ?

- **Reliability** - Ability to function correctly over a specified period of time.

  $R(t) = 1 - F(t) = P(X > t)$, X : Time to failure

- **Availability** - Probability that a system is performing at the instant t, regardless the number of times it has been repaired.

Typical Failure Rate - BathTub



What is Availability ?

- Availability is the measure of time the system is available and operating
  - Inherent availability = MTTF / (MTTF + MTTR)
  - Operational availability = Uptime / (Uptime + Downtime)
- MTTF = Mean Time To Failure
- MTTR = Mean Time To Repair

What is Availability ? (cont.)

As an example, the average lifetime for a given component is 10000 hours and the average time to repair is 4 hours.

The availability of this single repairable system is :

Availability = 10000 / (10000 + 4) = 0.9996

Measuring Availability

% Uptime	%Downtime	Downtime/year	Downtime/week
99 %	1 %	3.65 days	1 h 41 min
99.9 %	0.1 %	8 h 45 min	10 min 5s
99.99 %	0.01 %	52.5 min	1 min
99.999 %	0.001 %	5.25 min	6 s
“six nines”	0.0001 %	31.5 s	0.6 s

What is Unavailability ?

Unplanned causes of downtime:

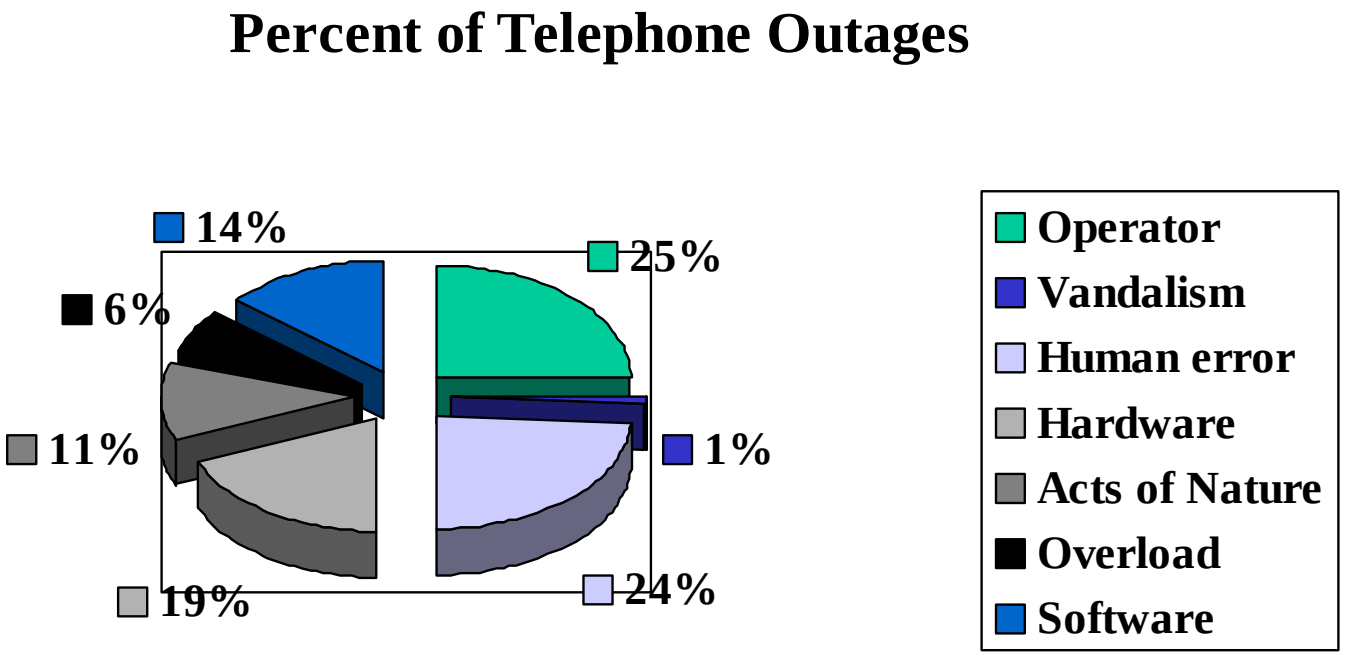
- Extended Planned Downtime
- Human Error
- Software (OS, Application, Database, Middleware) Failure
- Network Failure
- Disk / Hardware Failure
- Disasters (fire, tornado, earthquake, …)

What is Unavailability ? (cont.)

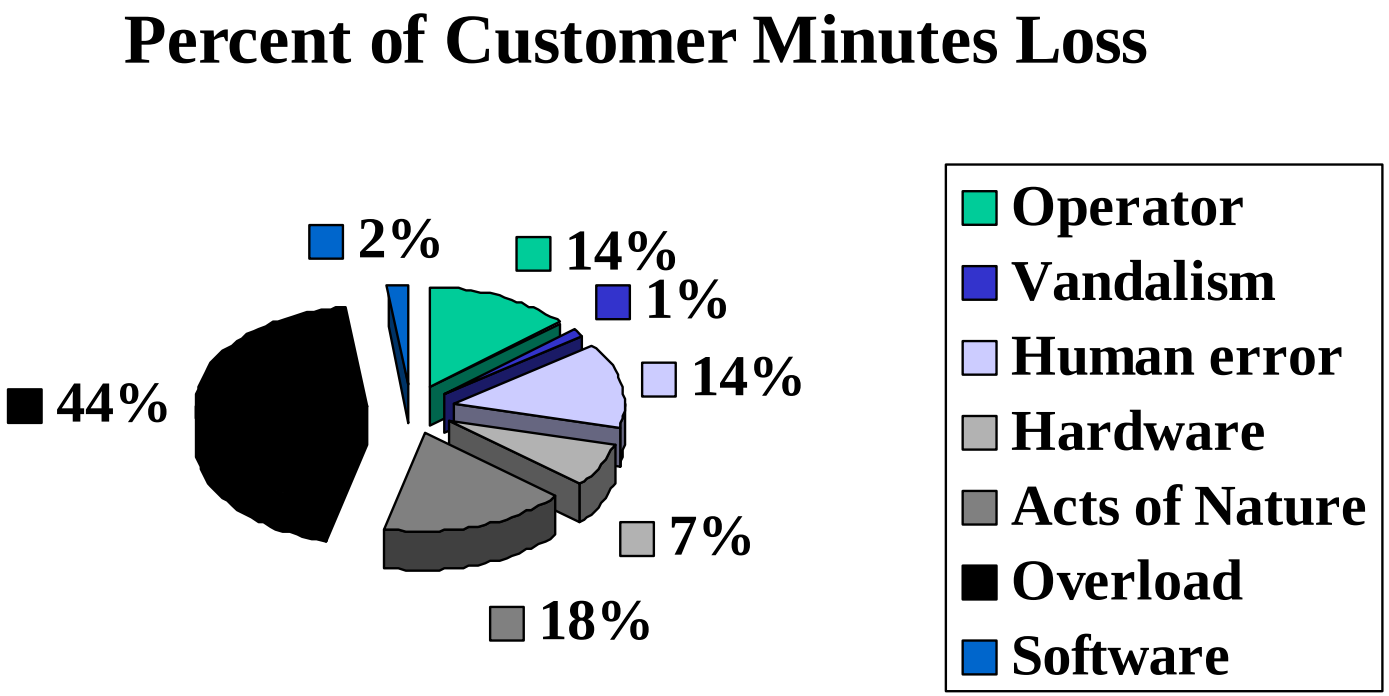
Planned causes of downtime:

- Backup
- Software Maintenance
- Hardware Maintenance
- Application / Database Upgrade
- Operating System Upgrade
- Hardware Upgrade

What is Unavailability ? (cont.)



What is Unavailability ? (cont.)



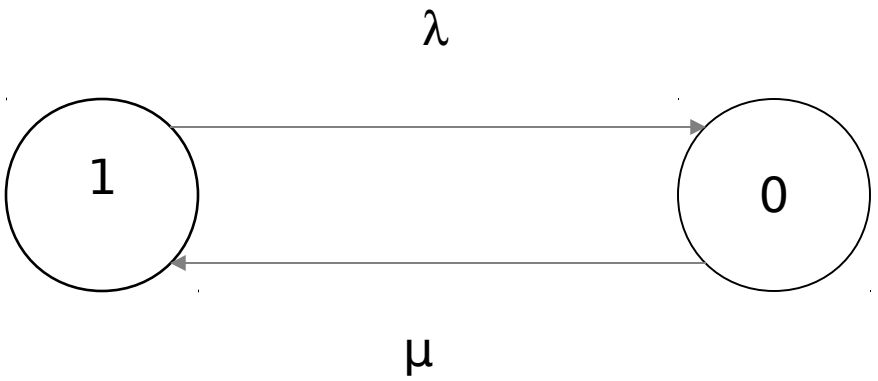
Availability Objectives

- Requirement as Platform supplier:
  - 40 sec/year (99.999873 %)
  - 20 sec/year (99.999937 %)
- Mechanisms for
  - Preservation of States
  - Detect and Recover failure in given budget.
- Number of Scheduled Outages
  - ex: 4 Software/Hardware Updates per year

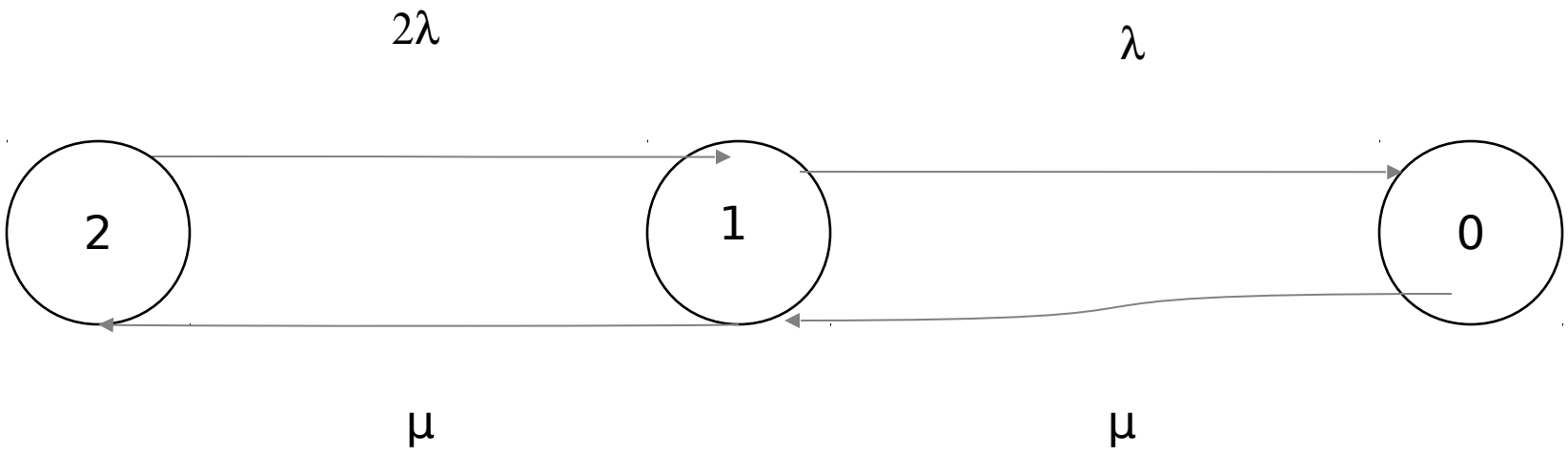
Markov Model Diagram

- Diagram of boxes, lines and text to visually and automatically portray possible system states.
- It is a convenient representation of failure/repair situations
- Boxes represent States.
- Transitions are indicated with Rate between States
    - λ = failure rate
    - μ = repair rate

Markov Model Diagram (cont.)



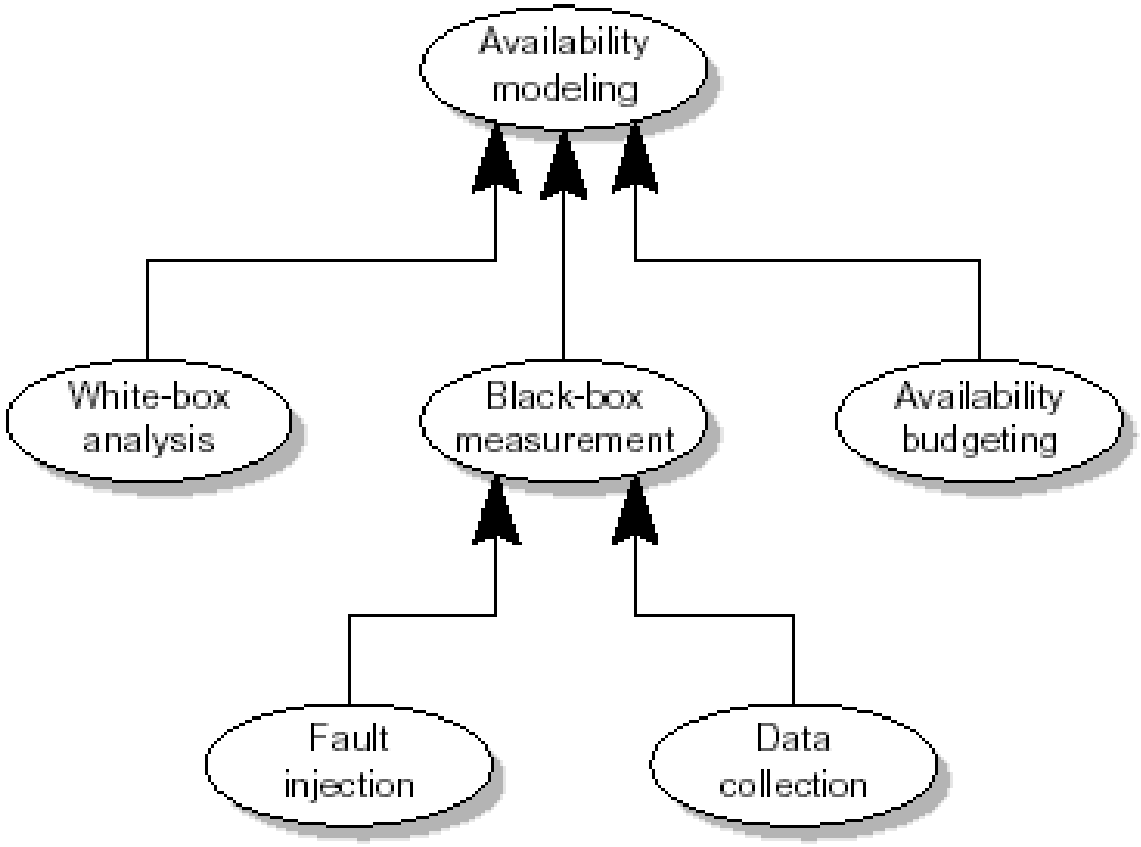
Markov Model Diagram (cont.)



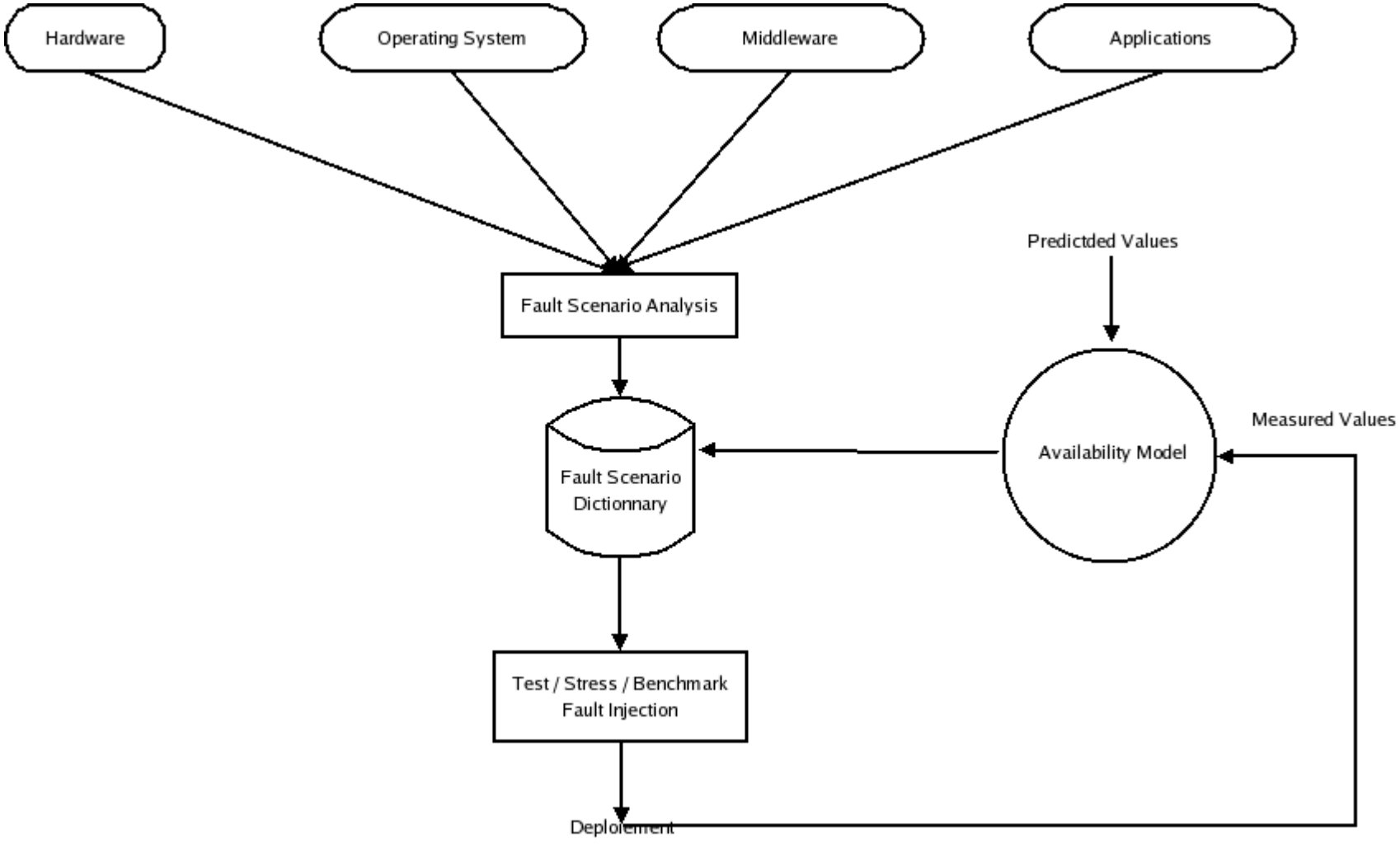
Purpose of Availability Model

- Availability can be improved in several ways :
  - Increase the MTTF
  - Decrease MTTR
  - Introduce Redundancy
  - Reduce Detection time
  - ...
- Modeling allows to easily assert availability by validation of various design.

- Availability Modeling – an Hybrid approach



- Availability in PLC - Example



Availability Modeling ?

Prediction is fine as long as it is not about the future.

Measures to be Evaluated

- Reliability-based :
  - Reliability : R(t), System MTTF
  - Availability

“Does it works, and for how long?”

- Performance
  - Throughput, Response Time, Blocking Probability, Workload

“If it works, how well does it work ?”

- Combination

Reference – More readings

- 'Blueprints for High Availability', Marcus/Stern
- 'Applied Reliability', Tobias/Trindade

Exercise 1

- Model Service Availability for the following system :
    - Web server with warm replication (primary and secondary)
        - Enumerate and describe the different states;
        - Idem with the transitions;
        - Idem with recovery/restore strategies;
        - Present a simple Markov Model.
- Investigate how software replication / load balancing mechanisms can improve availability for apache web server (failover and session support)

Correction Exercise 1

2 node systems parameters are:

- Mean Time between Failures (MTBF)
- Probability of successful reconfiguration (p)
- Recovery_Time—time taken for reconfiguration to complete
- Mean Time To Repair a node (MTTR_1)
- Node_Rejoin_Time—time for a node to join cluster.
- Percent increase in failure rate due to increased load (a)
- Mean Time To Repair two nodes (MTTR_2)

Correction Exercise 1 (cont.)