XFOCUS TEAM
from internet,for internet

# The Research of Survivability Evaluation & Analysis Model

Zhu Ergang
The Information Security Center of BUPT

X'CON 2004

# X'con 2004 Outline

- Why do we need survivability？ [1]
- Some Concepts of survivability[2,3,4]
- The model of survivability evaluation & analysis [2,3,4,5,6,7]
- Case study of survivability analysis[2,3]

# Why do we need survivability?

- 1st generation technology

ü Assumption

Systems are isolated.

Intrusions can be blocked in the boundary.

ü Technology

Information protection & isolation

ü Disadvantage

Boundary control is not easy.

Insider attack can't be blocked.

# Why do we need survivability?

- 2nd generation technology

ü Principle

Intrusion detection & response

ü Technology（PDRR）

Protection, Detection, Response, Recovery

ü Disadvantage

Some intrusions will succeed.

# Why do we need survivability?

- 3rd generation technology

ü Assumption

IDS can't detect all intrusions.

The protection system can't block all intrusions.

ü Technology

Fault tolerance

Intrusion tolerance

# Concepts of Survivability

- Definition

The capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

The system is in the broadest possible sense, including networks and large-scale systems of systems.

# Concepts of Survivability

- Essential Service

Essential services are mission-critical operations that must continue despite attacks, failures, or accidents.

- Non-Essential Service

Services can be paused or degraded for the essential services in the presence of attacks,  failures, or accidents.

# Concepts of Survivability

- Resistance

  Capability to deter attacks

- Recognition

  Capability to recognize attacks and extent of damage

- Recovery

  Capability to provide essential services/assets during attack and recover full services after attack

# The Model of Survivability Evaluation & Analysis

- Related work
- Methodology
- Evaluation & Analysis Workflow
- Evaluation method

# The Model of Survivability Evaluation & Analysis

- Related work

ü SSA (Survivable System Analysis)[2,3]

ü Quantitive Evaluation Method[5]

# The Model of Survivability Evaluation & Analysis

- Methodology

ü The quantitation of survivability[5]

SURV = (performance level at new state s) **/**
**(**normal performance level)

ü SSA Framwork[2,3]

System Definition
Essential Capability Definition
Compromisable Capability Definition
Survivability Analysis

# The Model of Survivability Evaluation & Analysis

- SEA model process

ü Analysis of survivability requirements

ü Intrusion analysis and test

ü Survivability Evaluation

ü Survivability Analysis

# The Model of Survivability Evaluation & Analysis

- Step 1: Analysis of survivability Requirement

ü System Architecture Analysis

ü Essential & Non-Essential Services Analysis

ü Construct the Evaluation Items of System Survivability

# The Model of Survivability Evaluation & Analysis

- Survivability Evaluation Items

ü Survivability is determined by the performance of essential & non-essential service.

ü The performance of service is determined by the service performance evaluation items.

ü Including item weight, evaluation value etc.

# The Model of Survivability Evaluation & Analysis

- Step 2: Intrusion Analysis & Test

ü Intrusion Scenario Analysis

ü Intrusion Test

ü Service Performance State Collection

# The Model of Survivability Evaluation & Analysis

- Attack Tree Model[6]

ü Reconnaissance
ü Vulnerability Identification
ü Penetration
ü Control
ü Embedding
ü Data extraction/modification
ü Attack Relay

# The Model of Survivability Evaluation & Analysis

- Step 3: Survivability Evaluation

ü Essential & non-essential service performance evaluation

Service items quantitation

Service performance evaluation

ü Survivability Evaluation

ü Get the services which have effect on survivability

# The Model of Survivability Evaluation & Analysis

- Step 4:Survivability Analysis

ü Resistance analysis

ü Recognition analysis

ü Recovery analysis

ü Recommendation

# The Model of Survivability Evaluation & Analysis

- Improvement of Resistance

ü Current Strategies

Patch

Firewall

Authentication

Encryption etc.

ü Future Strategies

Redundancy

Diversity

etc.

# The Model of Survivability Evaluation & Analysis

- Improvement of Recognition

ü Current Strategies

Intrusion Detection

Error Detection

ü Future Strategies

Self Awareness

Trust Maintenance

Black-Box Reporting

# The Model of Survivability Evaluation & Analysis

- Improvement of Recovery

ü Current Strategies

Replication of Critical Information

Fault Tolerance

ü Future Strategies

Dynamic System Adaptation

# The Model of Survivability Evaluation & Analysis

- Evaluation Method

Gray Evaluation Method Based on Triangular Whitenization Weight Function[7]

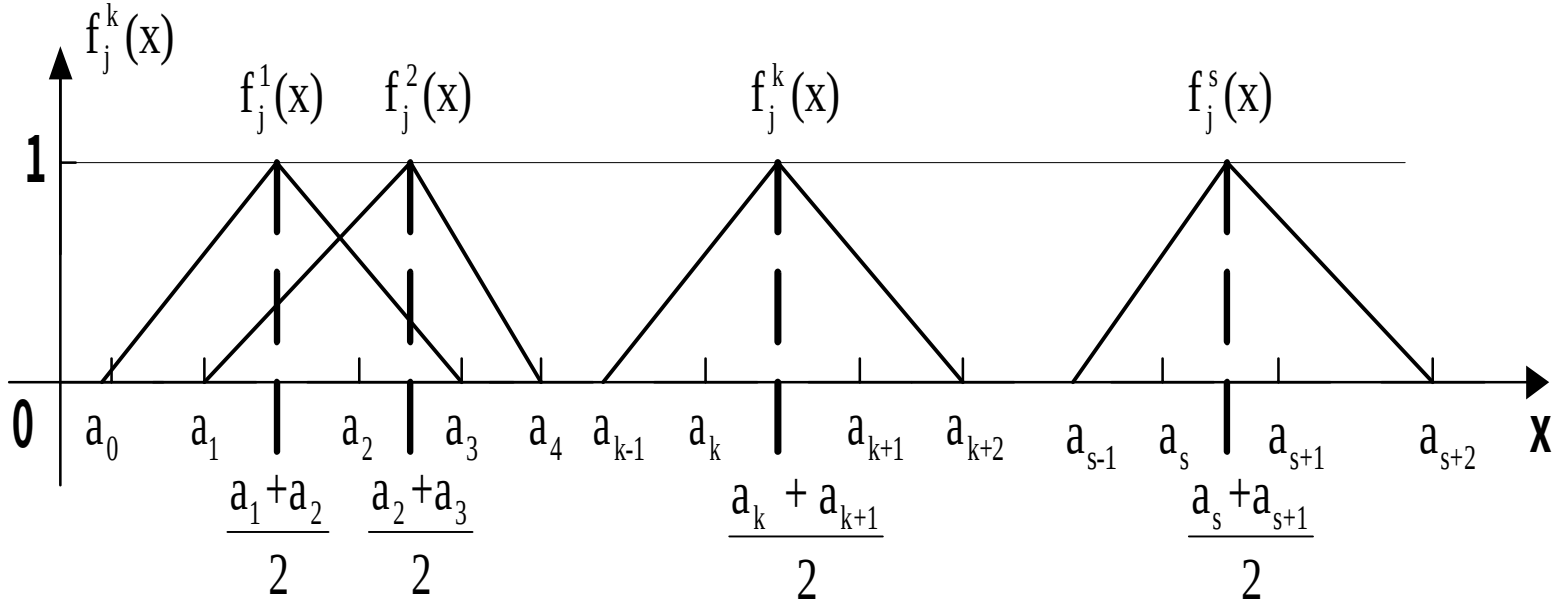
1. Evaluation items system should be constructed.

2. Qualitative result can be obtained based on quantitative information.

3. The effect of evaluation item's importance to evaluation result can be reflected.

# The Model of Survivability Evaluation & Analysis

- Whitenization Weight Function



# The Model of Survivability Evaluation & Analysis

- Service Performance Evaluation

ü Construct Evaluation Items System

| Item name | Item weight | low | moderate | high |
|---|---|---|---|---|
| Availability | 50 | [0.1,0.5] | [0.5,0.8] | [0.8,0.9] |
| Integrity | 30 | [0.1,0.7] | [0.7,0.9] | [0.9,1] |
| Confidentiality | 20 | [0,0.2] | [0.2,0.5] | [0.5,1] |

# The Model of Survivability Evaluation & Analysis

- Service Performance Evaluation

ü Service Performance Item Evaluation

| Item name | Availability | Integrity | confidentiality |
|---|---|---|---|
| value | 0.5 | 0.8 | 0.3 |

ü Construct whitenization weight function & Calculate degree of membership

| Performance state | normal | compromised | breakdown |
|---|---|---|---|
| Degree of membership | 46 | 83.5 | 15.6 |

# The Model of Survivability Evaluation & Analysis

- Survivability Evaluation

The evaluation items are service performances.

The operation is similar to service performance evaluation.

# The Model of Survivability Evaluation & Analysis

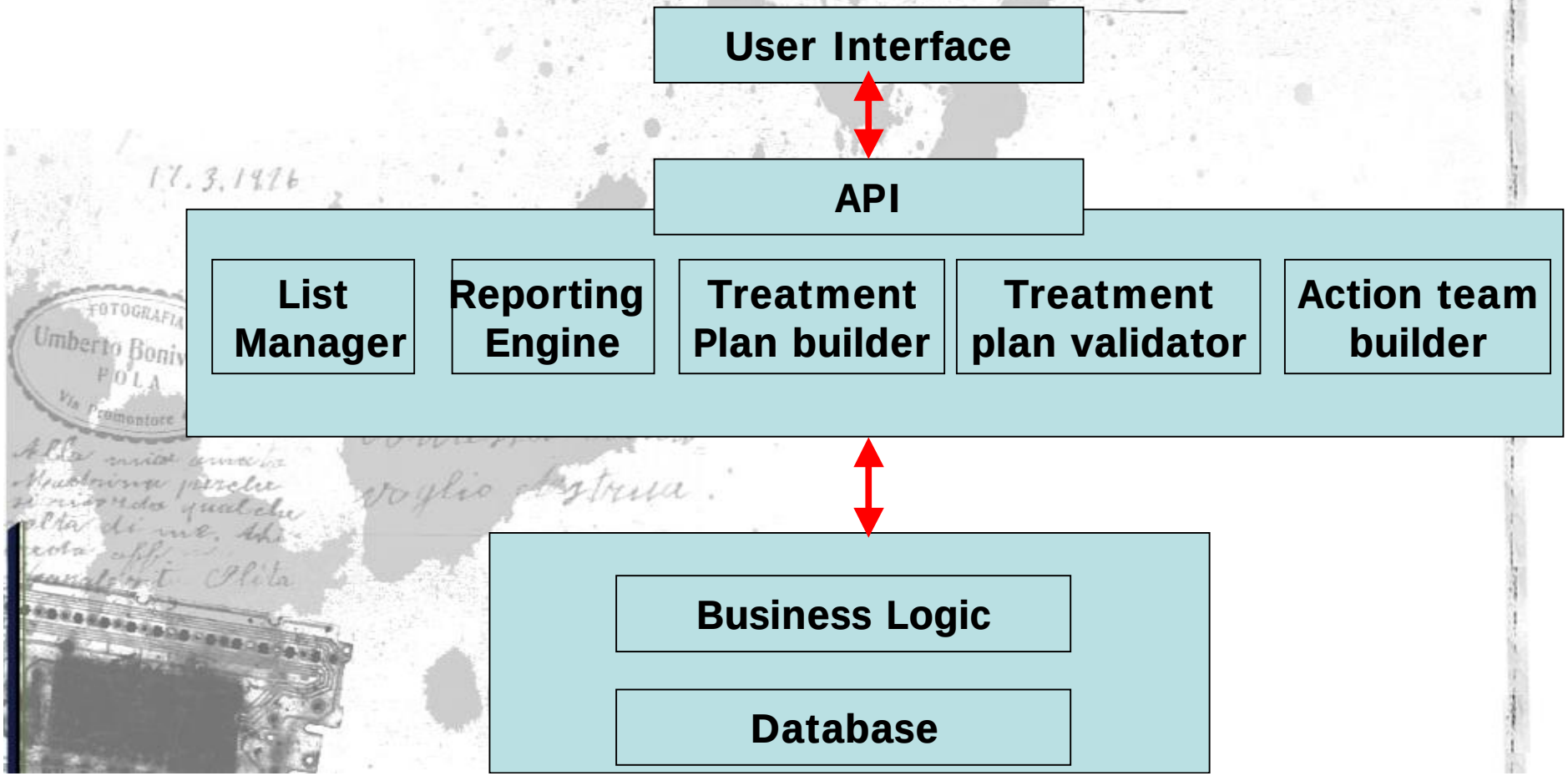
- Future Work

ü Simulation mechanism of survivability evaluation & analysis

ü Cost-Benefit analysis mechanism

# Case Study[3]

- Medical Management System Architecture



# Case Study

- Essential Capability

ü Add a new treatment plan

ü Update treatment plans

ü View a treatment plan

ü Create or modify an action team

ü Report the treatment plans

ü Etc.

X'con 2004

# Case Study

- Essential Service

ü View a treatment plan

- Essential Components
- Treatment plan builder

ü Database

# Case Study

- Possible Intrusion Scenarios
  - ü An unauthorized user modifies the treatment plan.
  - ü An intruder corrupts the database.
  - ü Etc.
- Intrusion Test
- Service Performance Evaluation
- Survivability Evaluation
- Survivability Analysis

# Case Study

- Recommendation Example(1)

| Intrusion Scenario | Resistance Strategy |
|---|---|
| Intruder corrupts database leading to loss of trust in validated treatment plans. | Current:<br>Security model in the database protects data against corruption. |
| | Recommended:<br>Implement live replicated database systems that cross check for validity (supported in many commercial database system). |

# Case Study

- Recommendation Example(2)

| Intrusion Scenario | Resistance Strategy |
|---|---|
| Intruder corrupts database leading to loss of trust in validated treatment plans. | Current:<br>None, except when provider happens to recognize a corrupted treatment plan. |
| | Recommended:<br>Add and check crypto-checksums on records in the database. |

# Case Study

- Recommendation Example(3)

| Intrusion Scenario | Resistance Strategy |
|---|---|
| Intruder corrupts database leading to loss of trust in validated treatment plans. | Current:<br>Locate an uncorrupted backup or reconstruct treatment plans from scratch. |
| | Recommended:<br>Reduce the backup cycle to quickly rebuild once a corrupted database is detected. |

# Reference


1. 荆继武，在攻击中生存，计算机世界，2004. 11
2. Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff, John McHugh, Survivable Network Analysis Method, SEI Technical Report CMU/SEI-2000-TR-013 ESC-2000-TR-013
3. R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, A Case Study in Survivable Network System Analysis, SEI Technical Report CMU/SEI-98-TR-014 ESC-TR-98-014
4. John C. Knight, Kevin J. Sullivan, Matthew C. Elder, Chenxi Wang, Survivability Architectures: Issues and Approaches
5. 夏春和，王继伟，赵勇，吴震，可生存性分析方法研究，计算机应用研究，2002 Vol.19 No.12
6. 卢继军，黄刘生，吴树峰，基于攻击树的网络攻击建模方法，计算机工程与应用，2003 Vol. 39 No.27
7. 刘思峰等，灰色系统理论及其应用，科学出版社，1999


# Thanks!