生存性评估分析模型

朱而刚
北京邮电大学信息安全中心

报告内容

- 为什么需要生存性？[1]
- 生存性(Survivability)的概念[2,3,4]
- 生存性评估分析模型[2,3,4,5,6,7]
- 生存性分析示例[2,3]

为什么需要生存性？

- 第一代安全技术（信息保护与隔离）

ü 基本假设

能够明确划分网络边界并且能够在边界上阻止非法入侵

ü 基本技术

保护和隔离

ü 缺点

边界划分与控制

对内部攻击无能为力

为什么需要生存性？

- 第二代安全技术（信息保障技术）

ü 基本原理

发现入侵及其造成的破坏，采取相应对策

ü 基本技术（PDRR）

保护、检测、响应、恢复

ü 缺点

过于依赖检测系统

恢复技术短时间难以达到效果

为什么需要生存性？

- 第三代安全技术（生存性技术）

ü 基本假设

检测系统不可能检测到所有的入侵

保护措施不可能阻止所有的入侵

关键设施必须不间断提供服务

ü 基本原理

容错、容侵

ü 基本技术

目前安全研究的热点

生存性概念介绍

- 定义

  生存性(Survivability)是指系统在遭受攻击(Attacks)、出现故障(Failures)或发生意外事故(Accidents)时，依然能够及时完成任务(Mission)的能力。

生存性概念介绍

- 必要服务(Essential Service)

  系统在遭受攻击、失效（Failure）或意外事故（Accident）时仍然必须提供的服务

- 次要服务(Non-Essential Service)

  系统在面临入侵或受损时，为保证必要服务的持续提供，可以暂时挂起、停止或受损的服务

生存性概念介绍

- 抵抗攻击能力(Resistance)

  当系统遭受攻击的时候，抵抗和忍受攻击的能力

- 可识别性(Recognition)

  识别攻击的策略,了解系统当前状态，判断系统受损程度的能力

- 可恢复性(Recovery)

  恢复受损信息或功能，隔离破坏区，在允许的时间间隔内维护恢复必要服务，条件允许时恢复所有服务的能力

生存性评估分析模型

- 相关工作
- 总体思路
- 评估分析流程
- 评估方法

生存性评估分析模型

- 相关工作

ü 文献[2,3]提出SSA分析方法

缺点:

只是定性分析,缺少定量评估

ü 文献[5]提出定量评估方法

缺点:

定量评估采用加权求和

生存性评估分析模型

- 总体思路

ü 生存性的量化[5]

损伤状态下，必要服务性能与次要服务性能之和同正常状态下必要服务性能与次要服务性能之和的比率

ü SSA的分析框架[2,3]

系统定义

必要能力定义

易损性能定义

生存性分析

生存性评估分析模型

- 总体思路

ü 结合前两种评估分析方法的优点

ü 通过充分模拟真实的攻击依次突破系统生存性进行生存性测试

ü 通过评估必要服务和次要服务的性能对系统的生存性进行评估

ü 通过分析系统的抵抗攻击能力、可识别性、可恢复性提出系统生存性的改进建议

生存性评估分析模型

- 生存性评估分析的四个步骤

ü 生存性需求分析

定义系统生存性需求

ü 入侵分析与测试

引入入侵,测试对必要服务和次要服务的影响

ü 生存性评估

定量评估,确定生存性等级

ü 生存性分析

提出生存性改进建议

生存性评估分析模型

- 生存性需求分析的主要内容

ü 系统架构分析

网络拓扑

应用架构等

ü 必要服务和次要服务分析

引入UML的分析机制,跟踪系统基本功能,确定必要服务和次要服务及其服务组件

ü 建立评估系统生存性的指标体系

生存性评估分析模型

- 评估系统生存性的指标体系

ü 通过必要服务和次要服务的性能来评估系统的生存性

ü 通过服务性能指标来评估服务的性能

ü 指标包括权重、评估目的对该指标的要求范围等

生存性评估分析模型

- 入侵分析与测试的主要工作

ü 入侵情景分析

引入攻击树模型,分析系统面临的威胁

ü 动态的攻击测试

测试威胁是否真正存在

ü 服务性能采集

根据服务性能指标判断服务性能状态

生存性评估分析模型

- 攻击树模型[6]

ü 主机勘查

ü 漏洞发现

ü 目标渗透

ü 权限提升

ü 潜伏隐藏

ü 信息攫取

ü 跳板攻击

生存性评估分析模型

- 生存性评估的主要工作

ü 必要服务和次要服务性能评估

服务性能指标量化

服务性能评估

ü 系统生存性评估

ü 找出影响系统生存性提高的服务

生存性评估分析模型

- 生存性分析的主要工作

ü 抵抗攻击能力分析

ü 可识别性分析

ü 可恢复性分析

ü 提出改进建议

生存性评估分析模型

- 抵抗攻击能力改进

ü 目前常用的措施

打补丁

防火墙

认证

加密等

ü 发展方向

冗余

多样性等

生存性评估分析模型

- 可识别性改进

ü 目前常用的措施

入侵检测

ü 发展方向

自识别

信任维护

黑盒报告等

生存性评估分析模型

- 可恢复性改进

ü 目前常用的措施

容错技术

信息备份

ü 发展方向

结合冗余和多样性的动态自适应

生存性评估分析模型

- 评估方法

采用基于三角白化权函数的灰色评估法[7]

1. 需要建立评估的指标体系

包括指标权重、指标评价值、评估等级对指标的要求范围等

2. 根据定量信息给出定性评估结果

聚类评估

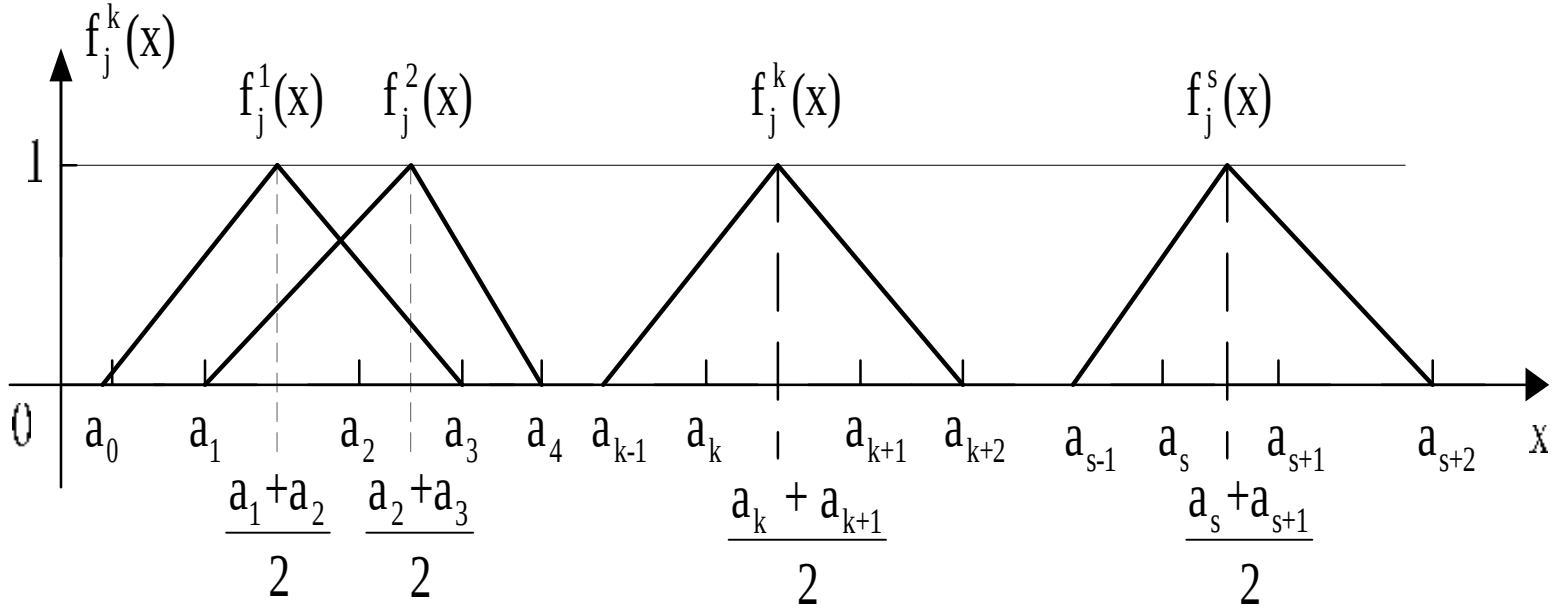
根据隶属度判断所处的等级

3. 能够反映指标重要性对评估结果的影响

加权求和法容易出现“重要指标得分低，而评估结果偏好”的情况

生存性评估分析模型

- 白化权函数



生存性评估分析模型

- 服务性能评估

ü 建立指标体系

指标名称	指标权重	低	中	高
可用性	50	[0.1,0.5]	[0.5,0.8]	[0.8,0.9]
完整性	30	[0.1,0.7]	[0.7,0.9]	[0.9,1]
保密性	20	[0,0.2]	[0.2,0.5]	[0.5,1]

生存性评估分析模型

- 服务性能评估

ü 服务性能指标评价值

指标名称	可用性	完整性	保密性
评价值	0.5	0.8	0.3

ü 构造白化权函数,计算隶属度

服务性能状态	正常	损伤	瘫痪
隶属度	46	83.5	15.6

生存性评估分析模型

- 生存性评估

将服务性能作为指标

操作类似于服务性能评估

生存性评估分析模型

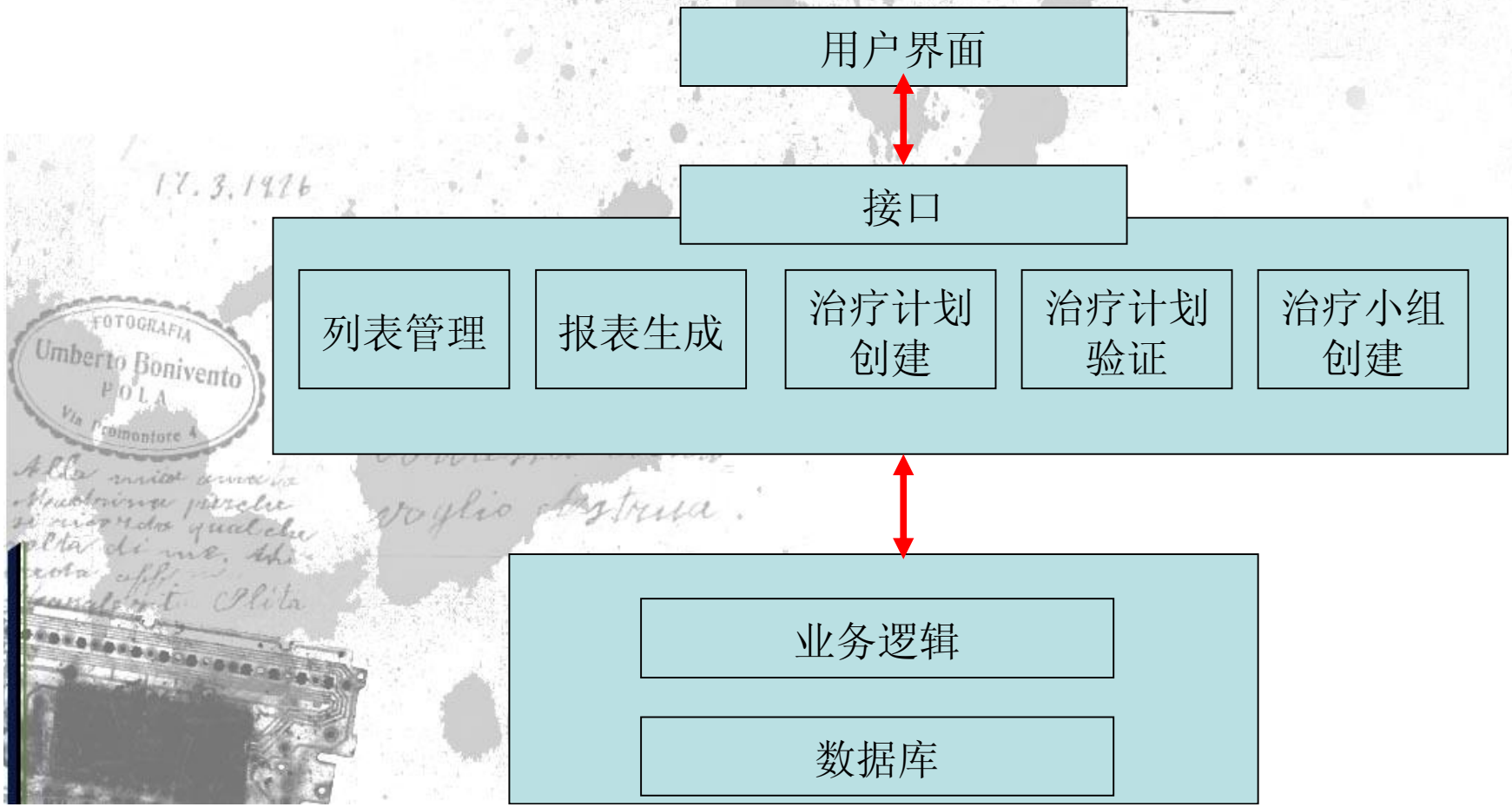
- 模型需要改进之处

ü 生存性测试的仿真机制

ü 成本－收益分析机制

生存性评估分析示例

- 医疗健康管理系统架构图



生存性评估分析示例

- 基本功能

ü 添加新的治疗计划

ü 更新治疗计划

ü 查看治疗计划

ü 创建或修改治疗小组

ü 以报表的形式显示治疗计划

ü 等等

生存性评估分析示例

- 必要服务
  - ü 查看治疗计划
- 必要组件
  - ü 报表生成组件
  - ü 数据库

生存性评估分析示例

- 可能的入侵情景
  - ü 未授权用户修改病人的治疗计划
  - ü 入侵者破坏数据库
  - ü 等等
- 入侵测试
- 服务性能采集
- 生存性评估

生存性评估分析示例

- 生存性改进建议示例

入侵情景	抵抗攻击能力		可识别性		可恢复性	
	目前	推荐	目前	推荐	目前	推荐
入侵者破坏数据库导致治疗计划提供者的信誉受到破坏，病人生命受到威胁	数据库自身的安全模型保护治疗计划	数据库现场复制，对数据库有效性进行交叉检验	无，除非医生偶然发现治疗计划被破坏	添加数据库中治疗计划有效性校验	查找未被破坏的治疗计划的备份，重构治疗计划	降低备份周期，快速重构治疗计划

参考文献

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-%R-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

谢谢！