COMP3027J 课程
软件架构
安全及其策略

邓永健

北京工业大学计算机学院

数据挖掘与安全实验室（DMS 实验室）

大纲

1. 安全的意义

2. 提高安全性的策略

3. 我们身边的安全

大纲

1. 安全的意义
2. 提高安全性的策略
3. 我们身边的安全

安全的意义

担忧

抵御对系统的攻击，同时确保合法用户能够使用系统

攻击（威胁）

- 尝试突破系统的安全防护

安全的意义

安全的不同方面

不可否认性

- 保密性

安全的意义

安全的不同方面

- 正直

保证；担保；保险；确信；放心

安全的意义

安全的不同方面

- 可用性

- 审计（用于重建）

账号	姓名	操作时间	操作板块	操作详细内容
admin	超级管理员	2014-10-22 14:53:21	提醒管理	提醒修改成功，标题：自定义提醒2内容：提醒2222222222222222...
admin	超级管理员	2014-10-22 14:52:56	提醒管理	提醒修改成功，标题：自定义提醒2内容：提醒2222222222222222...
admin	超级管理员	2014-10-22 14:52:28	提醒管理	提醒录入成功，标题：自定义提醒2内容：提醒2222222222222222...
admin	超级管理员	2014-10-22 14:51:51	提醒管理	提醒录入成功，标题：自定义提醒内容：提醒1111111111111111...
admin	超级管理员	2014-10-22 14:01:28	储值卡充值	储值卡充值成功，卡号：10015姓名：小陈充值金额：￥1.00 赠...
admin	超级管理员	2014-10-22 11:45:47	撤销充值	撤销充值记录成功，卡号：10015姓名：小陈充值金额：100 赠送...
admin	超级管理员	2014-10-22 11:45:42	撤销充值	撤销充值记录成功，卡号：10015姓名：小陈充值金额：100 赠送...
admin	超级管理员	2014-10-22 09:06:53	登录	操作员登录成功，账号：admin姓名：超级管理员
admin	超级管理员	2014-10-21 15:44:32	员工管理	增加新员工成功，员工姓名：赵六

安全的意义——场景

刺激源

- 攻击可能由人或其他系统发起。

刺激

- 对系统的攻击（或试图突破系统安全防护的行为）

常见形式：窃取或篡改信息、获取超级用户服务、降低系统性能

可用性

安全的意义——场景

文物

- 系统提供的服务或系统内的数据

环境

该系统可能处于不同的情况（联网/未联网、在线/离线、防火墙内/防火墙外）

安全的意义——场景

反应

- 允许合法用户正常使用，拒绝非法用户

- 对攻击的威慑

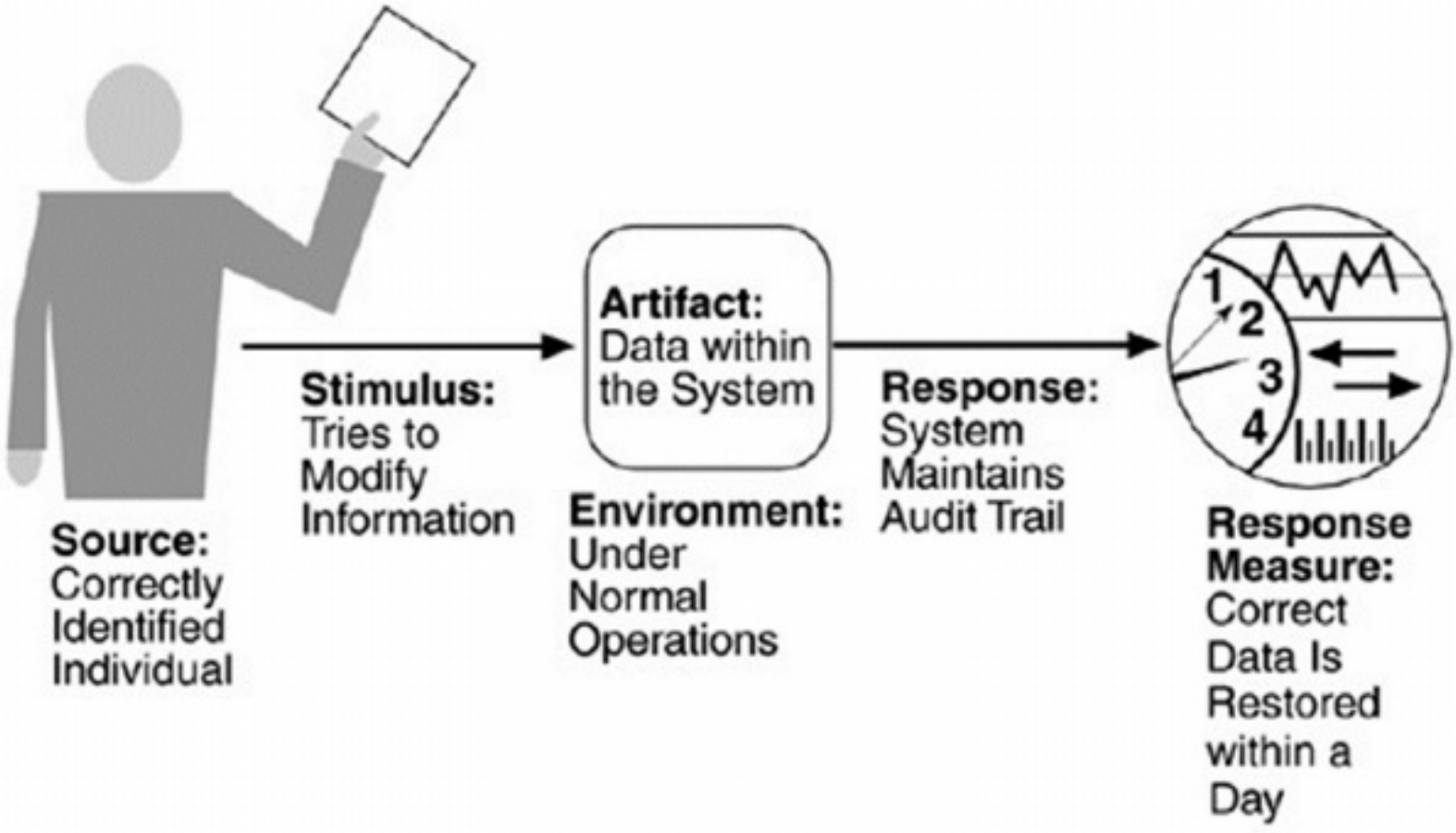
安全的意义——场景

响应测量

发动攻击的难度

- 从攻击中恢复的难度

安全场景示例


Source:
Correctly
Identified
Individual
Stimulus:
Tries to
Modify
Information
Artifact:
Data within
the System
Environment:
Under
Normal
Operations
Response:
System
Maintains
Audit Trail
1
2
3
4
Response
Measure:
Correct
Data Is
Restored
within a
Day

大纲

1. 安全的意义
2. 提高安全性的策略
3. 我们身边的安全

提升安全性的策略——概述

方向 1：抵御攻击

方向 2：检测攻击

方向 3：从攻击中恢复

提高安全性的策略

-抵御攻击

用户认证

- 密码、验证码、生物识别……

用户授权

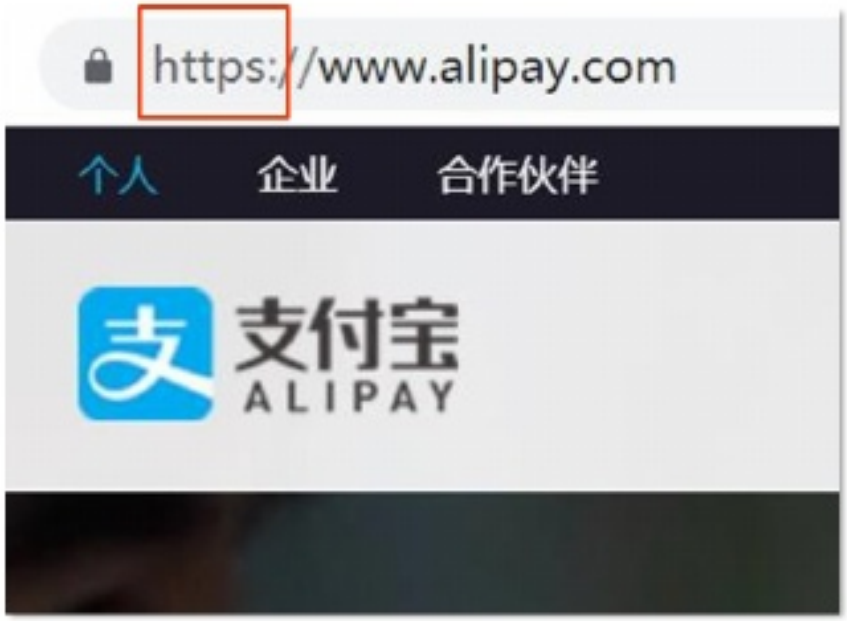
- 确保用户操作在其权限范围内……

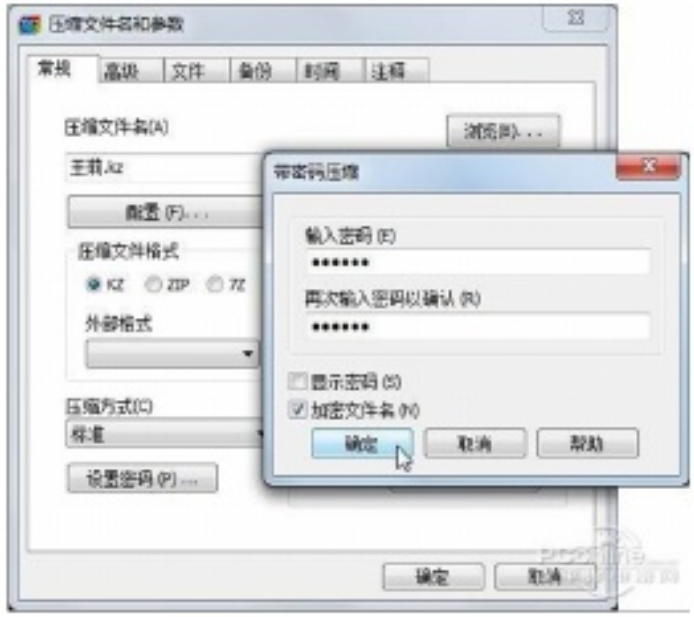
提高安全性的策略

-抵御攻击

维护数据机密性

- 对数据及传输过程进行加密





提高安全性的策略

-Resisting Attacks

维护数据完整性

- MD5 码验证

提高安全性的策略

-抵御攻击

减少暴露

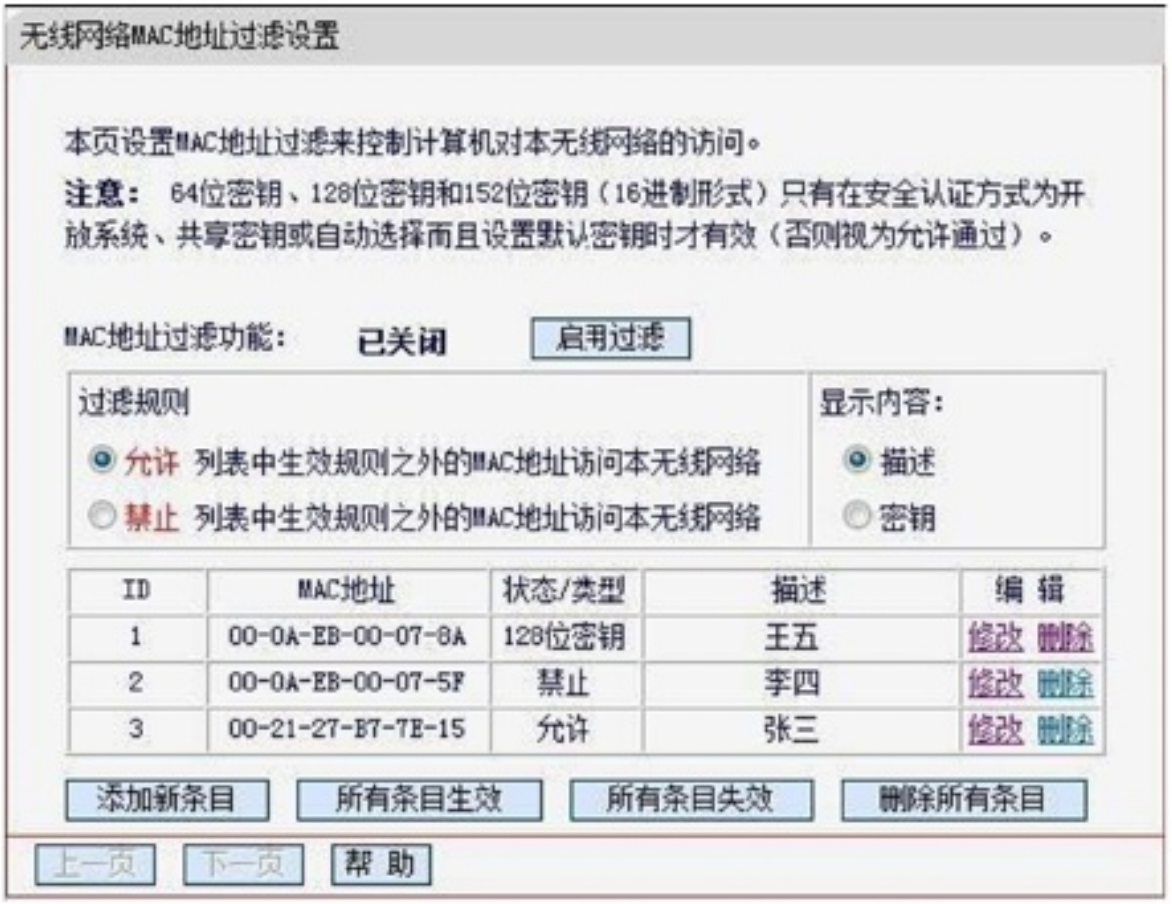
- 禁用不必要的端口、自动启动的服务、无线路由器的 SSID 等。

提高安全性的策略

-抵御攻击

访问控制

白名单、黑名单



提高安全性的策略

-检测攻击

软件与人的结合

入侵检测系统

- 安全专家

提高安全性的策略

-检测攻击

恢复状态

- 运用“可得性”策略

攻击者识别

也能威慑潜在的攻击者

大纲

1. 安全的意义
2. 提高安全性的策略
3. 我们身边的安全

身边的网络安全——用户名与密码

特性

- 革命性意义：区分身份与资质证明

用户名确保身份的唯一性，创建后不可更改。

密码确保身份安全且可更改

风险

- 猜测单个用户名和大型密码文件，猜测多个用户的常见密码

- 凭证填充、数据倾销

虚假 Wi-Fi 热点

我们身边的安保——安全卡

特性

基于“密码本”的典型“双因素”安全理念

实体卡无法被拦截，刮刮卡可防止分销渠道拍照。

我们身边的安保——安全卡

风险

伪“一次性密码”可能会遭受位置累积攻击

由于卡片尺寸的限制，只能通过频繁更换来解决。

实体卡的打印需要专用设备，成本高昂

我们身边的安全——短信验证码

特性

典型的“双因素”安全概念

- 仅需现有电信服务，无需用户额外付费
- 不适合多个用户共用一个账户

风险

延误、未收到、被拦截

正在对移动网络进行监测

智能手机上的恶意软件窃听

我们身边的安全——动态密码

特性

基于随机数种子和时间，每隔一定时间（例如 1 分钟）自动生成动态密码。

风险

- 可被破解

安全 - 概要

安全问题

将攻击对系统的影响降至最低

提高安全性的策略

- 抵御攻击
- 检测攻击
- 从攻击中恢复

谢谢你!