

COMP3027J

Software Architecture

Security and its Tactics

DENG, YONGJIAN

Faculty of Computer Science, BJUT

Data Mining & Security Lab (DMS Lab)



北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

Outline

1. The Meaning of Security
2. Tactics to Improve Security
3. Security Around Us



Outline

1. The Meaning of Security

2. Tactics to Improve Security

3. Security Around Us



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

The Meaning of Security

Concerns

- Resisting attacks on the system while ensuring legitimate users can use the system

Attacks (Threats)

- Attempts to break through the system's security protection



The Meaning of Security

Different Aspects of Security

- Non-repudiation
- Confidentiality



北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

The Meaning of Security

Different Aspects of Security

- Integrity
- Assurance

 大小: 20.1 MB	宏汇专家交易终端 支持策略交易, 下载使用前请联系开户分支机构详细了解。 【适用客户】 更新日期: 2019-09-02 MD5:C48819847AD9E058335B06D9807DDE29
 大小: 28K	MD5生成工具 比对下载软件的MD5码, 提醒客户该软件是否被篡改。使用方法: 1 拖动已下载的安装文件到此工具界面里, 生成MD5串码; 2 将此验证码与官方网站提供的客户端程序和补丁包版本的验证码比较。若一致则表示为正规版本, 可以使用。 【适用客户】 更新日期: 2019-09-02 MD5:6248D99DB0D0C4EB7F7F3F7ABDE9AAE4



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

The Meaning of Security

Different Aspects of Security

- Availability
- Auditing (for reconstruction)

当前位置: 会员管理系统 -> 系统设置 -> 系统操作日志

 系统日志高级查询  系统日志自动清除设置

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111111111111111111...
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 赠送...
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



The Meaning of Security - Scenarios

Sources of Stimulus

- Attacks may be initiated by people or other systems

Stimulus

- Attacks on the system (or attempts to break through system security protection)
- Common forms: Stealing or modifying information, obtaining superuser services, reducing system availability



The Meaning of Security - Scenarios

Artifacts

- Services provided by the system or data within the system

Environment

- The system may be in different situations (networked/unnetworked, online/offline, inside/outside the firewall)



The Meaning of Security - Scenarios

Response

- Allow legitimate users to use normally, deny illegal users
- Deterrence against attacks



北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

The Meaning of Security - Scenarios

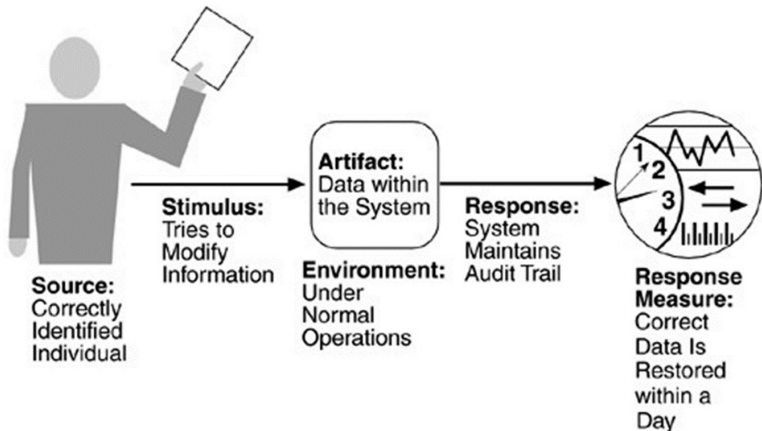
Response Measurement

- Difficulty of launching an attack
- Difficulty of recovering from an attack



北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

Security Scenario Example



Outline

1. The Meaning of Security

2. Tactics to Improve Security

3. Security Around Us



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

Tactics to Improve Security - Overview

Direction 1: Resisting Attacks

Direction 2: Detecting Attacks

Direction 3: Recovering from Attacks



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

Tactics to Improve Security

-Resisting Attacks

User Authentication

- Passwords, CAPTCHA, Biometrics...

User Authorization

- Ensuring user actions are within their permission scope...



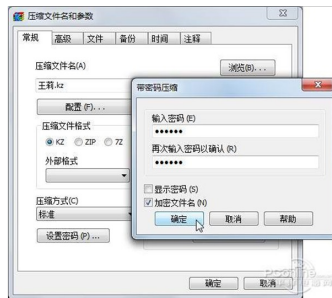
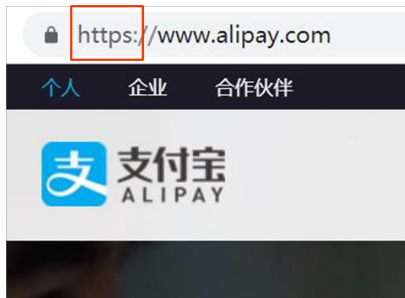
北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

Tactics to Improve Security

-Resisting Attacks

Maintaining Data Confidentiality

- Encrypting data and transmission processes



Tactics to Improve Security

-Resisting Attacks

Maintaining Data Integrity

- MD5 code verification

DOTA2 最新客户端下载

更新日期: 2019-07-10 | 文件大小: 11.6GB

MD5码: bb6859da6b5b8d27a67b95e878928410

↓ 官方HTTP下载



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

Tactics to Improve Security

-Resisting Attacks

Reducing Exposure

- Disabling unnecessary ports, auto-starting services, wireless router SSID, etc.

此规则应用于 TCP 还是 UDP?

☒ TCP
☐ UDP

此规则应用于所有本地端口还是特定的本地端口?

☐ 所有本地端口(A)
☒ 特定本地端口(S):
示例: 80, 443, 5000-5010

☒ 启用无线功能

无线工作模式 ☒ 无线接入点 (AP) ☐ 网桥 (WDS)

网络模式

主SSID

次SSID

广播 (SSID) ☒ 开启 ☐ 关闭

AP 隔离 ☐ 开启 ☒ 关闭

信道



Tactics to Improve Security

-Resisting Attacks

Access Control

- Whitelists, Blacklists

无线网络MAC地址过滤设置

本页设置MAC地址过滤来控制计算机对本无线网络的访问。

注意： 64位密钥、128位密钥和152位密钥（16进制形式）只有在安全认证方式为开放系统、共享密钥或自动选择而且设置默认密钥时才有效（否则视为允许通过）。

MAC地址过滤功能：☐ 已关闭 ☒ 启用过滤

过滤规则

☒ **允许** 列表中生效规则之外的MAC地址访问本无线网络

☐ **禁止** 列表中生效规则之外的MAC地址访问本无线网络

显示内容：

☒ 描述

☐ 密钥

ID	MAC地址	状态/类型	描述	编辑
1	00-0A-EB-00-07-8A	128位密钥	王五	修改 删除
2	00-0A-EB-00-07-5F	禁止	李四	修改 删除
3	00-21-27-B7-7E-15	允许	张三	修改 删除



Tactics to Improve Security

-Detecting Attacks

Combination of Software and Humans

- Intrusion Detection Systems
- Security Experts



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY

Tactics to Improve Security

-Detecting Attacks

Restoring State

- Using Tactics from "Availability"

Identification of Attackers

- Can also deter potential attackers



Outline

1. The Meaning of Security
2. Tactics to Improve Security
3. Security Around Us



Security Around Us – Usernames + Passwords

Features

- Revolutionary significance: Distinguishes identity from credentials
- Usernames ensure unique identity and are unchangeable after establishment
- Passwords ensure identity security and are changeable

Risks

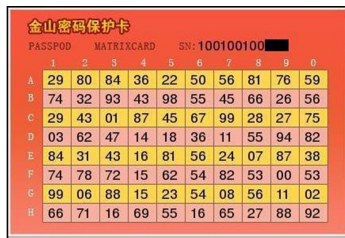
- Guessing single username and large password files, guessing common passwords for multiple users
- Credential stuffing, data dumping
- Fake Wi-Fi hotspots



Security Around Us - Security Cards

Features

- Based on "password books", a typical "two-factor" security concept
- Physical cards cannot be intercepted, scratch cards prevent distribution channel photography



北京工业大学
BEIJING UNIVERSITY OF TECHNOLOGY

Security Around Us - Security Cards

Risks

- Pseudo "one-time password", may be subject to location accumulation attacks
- Limited by the size of the card, can only be resolved by frequent replacement
- Physical card printing requires specialized equipment, high cost



Security Around Us - SMS Verification Codes

Features

- Typical "two-factor" security concept
- Only requires existing telecommunication services, no additional user cost
- Not suitable for multiple users to share one account

Risks

- Delays, not received, blocked
- Mobile networks being monitored
- Malware on smartphones eavesdropping



Security Around Us - Dynamic Passwords

Features

- Based on random number seeds + time, automatically generates dynamic passwords every certain period (e.g., 1 minute)

Risks

- Can be cracked



Concerns of Security

- Minimize the impact of attacks on the system

Tactics to Improve Security

- Resisting Attacks
- Detecting Attacks
- Recovering from Attacks

availability的备份/冗余操作类似，但关注点不一样
可以对比学习



Thank you!



北京工业大学
BEIHANG UNIVERSITY OF TECHNOLOGY