# COMP3027J
# Software Architecture
## Security and its Tactics

DENG, YONGJIAN

Faculty of Computer Science, BJUT

Data Mining & Security Lab (DMS Lab)

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

# Outline

# Outline

# 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



北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

# The Meaning of Security

## Different Aspects of Security

- Integrity
- Assurance

# 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 |

# 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

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

# 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

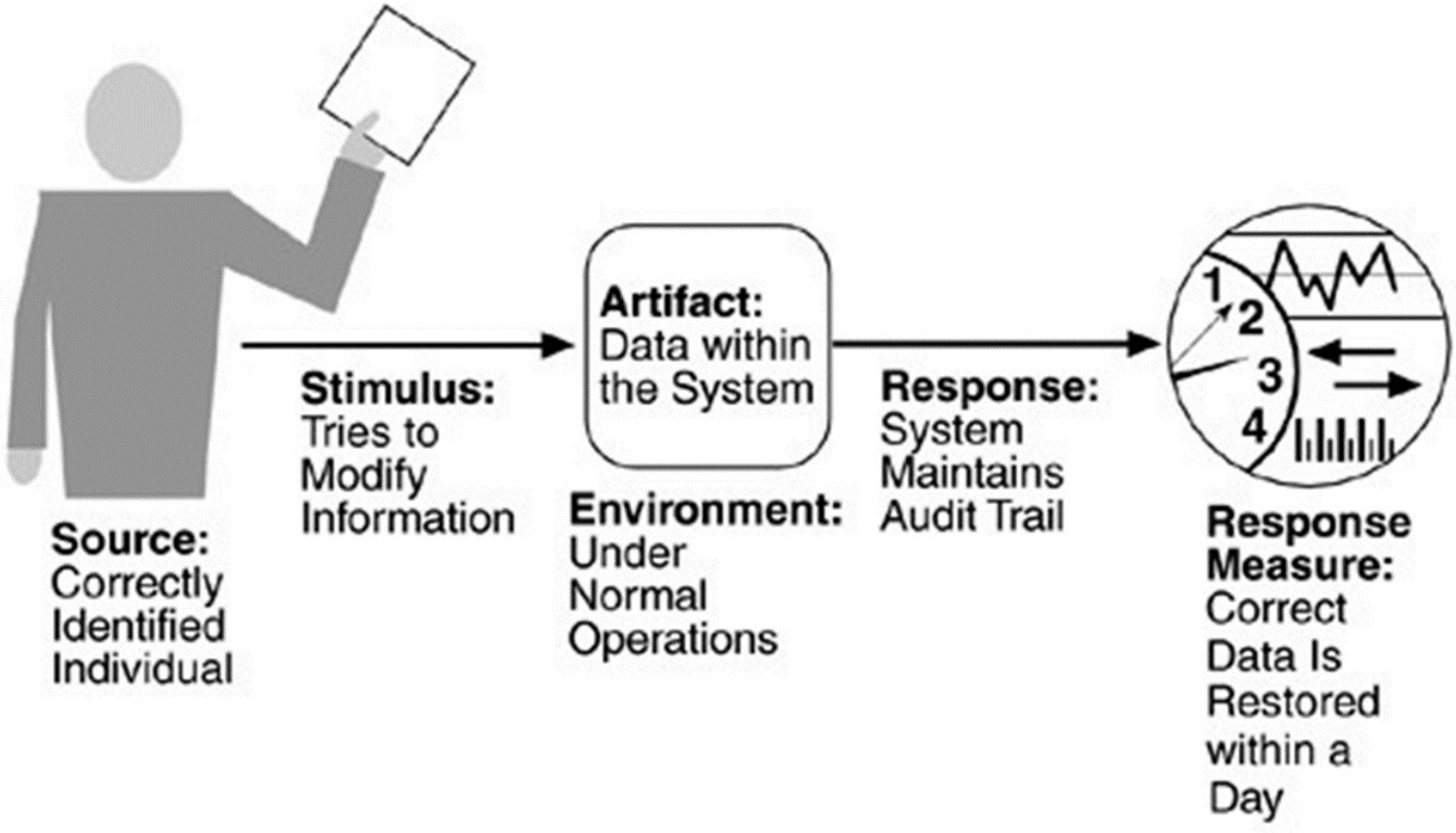
# The Meaning of Security - Scenarios

## Response Measurement

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


北京工業大學 BEIJING UNIVERSITY OF TECHNOLOGY

# Security Scenario Example



# Outline

# Tactics to Improve Security - Overview

**Direction 1: Resisting Attacks**

**Direction 2: Detecting Attacks**

**Direction 3: Recovering from Attacks**

# Tactics to Improve Security

## -Resisting Attacks

### User Authentication

- Passwords, CAPTCHA, Biometrics...

### User Authorization

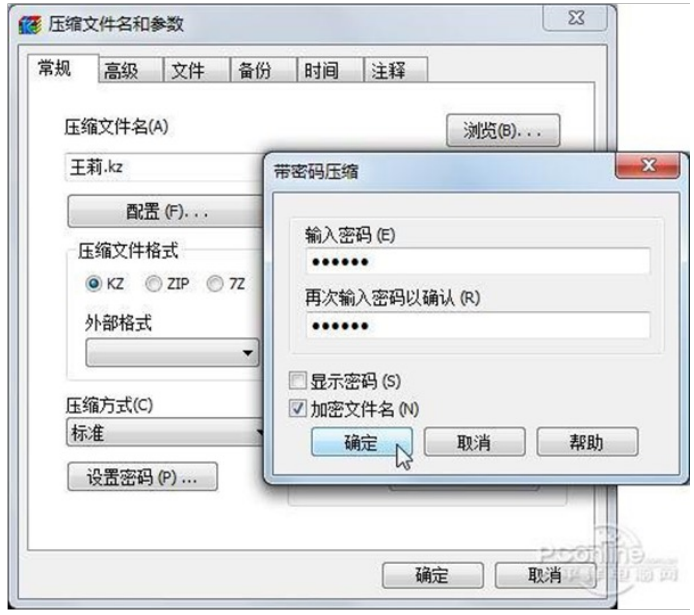
- Ensuring user actions are within their permission scope...

# 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

# Tactics to Improve Security

## -Resisting Attacks

### Reducing Exposure

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


# Tactics to Improve Security

## -Resisting Attacks

### Access Control

- Whitelists, Blacklists

# Tactics to Improve Security

## -Detecting Attacks

**Combination of Software and Humans**

- Intrusion Detection Systems
- Security Experts

# Tactics to Improve Security

## -Detecting Attacks

**Restoring State**

- Using Tactics from "Availability"

**Identification of Attackers**

- Can also deter potential attackers

# Outline

# 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


# 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


北京工業大學 BEIJING UNIVERSITY OF TECHNOLOGY

# Security - Summary

**Concerns of Security**

- Minimize the impact of attacks on the system

**Tactics to Improve Security**

- Resisting Attacks
- Detecting Attacks
- Recovering from Attacks

# Thank you!