《数据安全技术》

-段方

某世界 **100** 强企业大数据总设计师

教授 北京大学博士后

1 概述

1.1 信息安全的概念及范围

1.1.1 概述

1.1.2 信息系统潜在威胁

被动攻击

主动攻击

黑客攻击手法

1.1.3 信息安全技术概览

1.1.4 信息安全注重体系安全

防

护

检测

响应

恢复

1.2 信息安全等级分类

1.2.1 分级的概念

1.2.2 分级保护涉及的标准

1.2.3 职责和角色

1.2.4 企业信息等级选择依据

1.3 信息安全的层级界定

1.3.1 网络层

1.3.2 硬件层

1.3.3 操作系统层

1.3.4 应用层

1.3.5 数据层

1.4 信息安全的**“**维度 **”**

1.4.1 硬件故障

1.4.2 人为过失

1.4.3 软件失误

1.4.4 电脑病毒

1.4.5 自然灾害等

1.5 信息安全的现状

1.5.1 中国国家层面的法律、法规等

1.5.2 美国 **NSA** 等安全保障体系

1.5.3 一些黑客攻击案例

1.6 客户隐私保护

1.6.1 客户隐私的界定

1.6.2 客户隐私保护的内容

1.6.3 客户隐私的国际情况

欧洲的 **GDPR** 说起

1.6.4 【思考】不同企业客户隐私的界定

1.7 常见问题的防范

1.7.1 培养良好习惯

1.7.2 电脑病毒的防护

1.7.3 浏览器的防护

1.7.4 操作系统的安全防护

1.7.5 网络层面的防护等

1.8 【案例】信息安全防护的具体案例

2 网络安全发展形势分析（可选）

2.1 国内外一些网络安全事件

2.1.1 英特尔处理器漏洞

2.1.2 英国智能电表漏洞

2.1.3 思科安全攻击事件

2.1.4 勒索病毒事件

2.1.5 美国大选干预等

2.2 物联网和工业互联网安全凸显

2.2.1 物联网的安全风险点

2.2.2 工业互联网安全的风险点

2.3 全球网络对抗态势升级

2.3.1 美国网络对抗战略明显

2.3.2 美国完善网络空间作战机构

2.3.3 强化多方合作

2.4 完善数据保护法律

2.4.1 欧洲 **GDPR**

2.4.2 美国相关法律

2.4.3 中国数据安全法

2.5 数据安全检查

2.5.1 美国的安全处罚案例

2.5.2 欧洲安全处罚案例

2.5.3 我国的数据安全防护工作

2.6 我国网络安全防护

2.6.1 不断推出网络安全产品

2.6.2 加强网络安全人才培养

2.6.3 网络安全企业通过多渠道合作

2.6.4 网络信息内容管理

2.6.5 关键信息基础设施安全防护

2.6.6 网络产品管理

2.6.7 个人信息和重要数据保护

2.7 几个关键问题

4.2.3 PGD 方法

4.3 AI 对抗攻防的防御基本方法

4.3.1 主动防御与被动防御

4.3.2 对抗训练

4.3.3 对抗样本检测

4.3.4 使用辅助识别工具

cleverHans

foolbox 等

4.4 AI 对抗攻防的范围及举例

4.4.1 目标检测

目标检测的原理

目标检测的攻击方

法 目标检测的防御

方法 **4.4.2** 图像

识别

从 **YOLO** 算法说起

标注的安全

算法的识别矫正

4.4.3 语音识别

语音识别的原理

语音识别的攻击方法

语音识别的防御方法

4.4.4 自然语言处理

chatGPT 的价值

chatGPT 的攻击

方法 **chatGPT** 的

防御方法

4.4.5 人脸识别

人脸识别的算法原理

人脸识别的攻击原理

人脸识别的防御原理

4.4.6 恶意软件检测等

蜜罐技术举例

5.6 态势感知的兵法运用

5.6.1 态势感知与兵法

5.6.2 从攻击的方法论入手

5.6.3 《火攻篇》的感知启示

5.7 态势感知与算力网络

5.7.1 感知与算力的正相关

5.7.2 算法的算力消耗

5.7.3 算力网络改善态势感知能力

5.8 【思考】 **5G** 成为可信信息网络基础设施

5.8.1 所有的通信都要通过电信网络

5.8.2 物联网的安全问题更严重

5.8.3 丢掉 **5G**、丢掉信息安全

5.9 【案例】附件——基于车联网的安全监控案例

6 数据安全实际案例

6.1 层层防御的技术理念

6.1.1 从敏感数据角度的层层防御

6.1.2 从数据出来环节的层层防御

6.1.3 从数据生命周期的层层防御

6.2 数据访问策略

6.2.1 隐私数据策略管理

6.2.2 告警策略管理

6.3 “ 三分技术、七分管理 **”**

6.3.1 安全管理的重要性

6.3.2 安全管理的内容和范围

6.3.3 技术围绕管理需求

6.4 与网络安全的关系

6.4.1 层次不同

6.4.2 解决网络突破后的数据安全问题

6.5 数据导出管理与监控

6.5.1 数据水印技术