第二章 基于隐私保护的数据挖掘

网络安全事件

- **网络开放性为各类网络安全事件提供了可乘之机**

- 2014年，CNCERT/CC协调处置涉及基础电信企业的漏洞事件1578起，是2013年的3倍
- 2014年我国境内感染木马僵尸网络的主机为1108.8万余台。
- 2014年针对我国域名系统的流量规模达1Gbit/s以上的拒绝服务攻击事件日均约187起，约为2013年的3倍。
- 2014年通报处置通用软硬件漏洞事件714起，较2013年增长1倍。

其它网络安全事件

- **网络安全是关系国计民生的大问题**

- 国内通用顶级域的根服务器忽然出现异常，导致DNS解析故障
- 比特币交易平台Mt.Gox由于系统漏洞，比特币失窃导致破产
- Heartbleed漏洞波及网银及各大门户网站
- BadUSB漏洞
- Ebay遭遇黑客密码窃取，要求用户全部重置密码
- 。。。。。。

目录

隐私保护技术介绍

1. **基于限制发布的技术**
2. **基于数据加密的技术**
3. **基于数据失真的技术**
4. **隐私保护技术对比分析**

- **网络安全**是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。主要强调了保密性、完整性、可用性、可控性、可审查性等主要特性。

隐私保护中的数据挖掘应用

1. **基于隐私保护的关联规则挖掘方法**
2. **基于聚类的匿名化算法**
3. **基于决策树的隐私保护**
4. **基于贝叶斯分类的隐私保护**
5. **基于特征选择的隐私保护**

- **网络安全**是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。主要强调了保密性、完整性、可用性、可控性、可审查性等主要特性。

大数据安全与隐私保护

1. 大数据安全概述
2. 大数据安全与

- **网络安全**是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。主要强调了保密性、完整性、可用性、可控性、可审查性等主要特性。

隐私保护中的数据挖掘应用

1. **基于隐私保护的关联规则挖掘方法**
2. **基于聚类的匿名化算法**
3. **基于决策树的隐私保护**
4. **基于贝叶斯分类的隐私保护**
5. **基于特征选择的隐私保护**

- **网络安全**是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。主要强调了保密性、完整性、可用性、可控性、可审查性等主要特性。

网络安全定义

- **网络空间**
- **网络空间安全**

- **网络空间**（Cyberspace）是通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。
- **网络空间安全**（Cyberspace Security）研究网络空间中的安全威胁和防护问题，即在有攻击者的对抗环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施、以及网络和系统本身的威胁和防护机制。

网络安全面临的挑战

- **网络安全面临不同层次、多种多样挑战和威胁**

- 自然威胁（自然灾害、场地环境遭受破坏、设备老化等）；
- 信息泄露（如商业间谍、窃听、流量分析等）；
- 非授权访问（如非授权用户进行入侵）；
- 操作系统缺陷（如操作系统楼梯、后门、I/O非法访问等）；
- 软件漏洞（如数据库的安全漏洞、TCP/IP协议的安全漏洞、网络软件与网络服务的漏洞）；
- 病毒和木马；
- 拒绝服务；
- 甚至还包括网络舆情威胁、网络色情、网络欺诈、网络暴力等

网络安全的重要性

- **习总书记指出：“没有网络安全就没有国家安全”，并要求“加强网络空间安全人才建设，打造素质过硬、战斗力强的人才队伍”。**

- 国际上围绕网络安全的斗争愈演愈烈，夺取网络空间控制权是战略制高点
- 网络安全人才已成为国家竞争的核心所在
- 网络安全技术作用日益彰显
  - 保护个人隐私、
  - 保障经济发展、
  - 维持社会稳定、
  - 保障国家安全

网络空间（信息）安全学科

- 学科概况
- 学科培养目标
- 主要研究方向
- 主要研究内容

- 学科概况
  - “网络空间安全”为“工学”门类下一级学科，学科代码为“0839”，授与“工学”学位。
  - 网络空间由互联互通网络、网络节点和系统及数据组成，可分为物理层、逻辑层和行为体层。
  - 网络空间涉及数学、计算机科学与安全、信息与通信工程等学科，已形成独立教学和研究领域

学科培养目标

- **通过网络空间安全学科培养，力求让学生**
  - 掌握网络空间安全基础理论和技术方法
  - 掌握信息系统安全、网络基础设施安全、信息内容安全和信息对抗等相关专门知识
  - 能够承担科研院所、企事业单位和行政管理部门网络空间安全方面的科学研究、技术开发及管理工作

主要研究方向

- **安全基础**
- **密码学及应用**
- **系统安全**
- **网络安全**
- **应用安全**

- 为其他方向提供理论、架构和方法学指导
- 为其他方向提供密码体制机制
- 保证网络空间中单元计算系统安全、可信
- 保证连接计算机的网络自身安全和传输信息安全
- 保证网络空间中大型应用系统安全

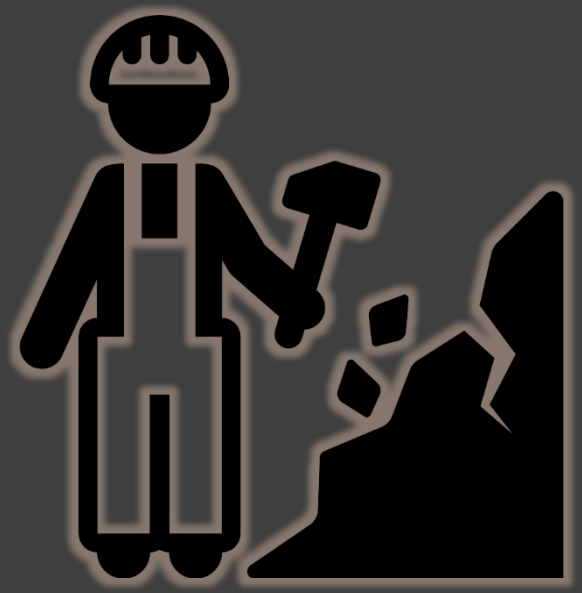
主要研究内容

- **网络空间安全学科囊括的研究内容包括**

- 可信计算体系、新型密码体制、密码编码与密码分析、网络通信安全、信息安全风险评估、信息安全管理、灾难备份和应急响应、操作系统安全、数据库安全、信息隐藏与检测、内容识别与过滤、信息对抗理论与技术，以及信息安全工程

数据挖掘简介

- 数据挖掘含义
- 数据挖掘定义
- 数据挖掘原因
- 数据挖掘特点



数据挖掘简介

- 数据挖掘含义
- 数据挖掘定义
- 数据挖掘原因
- 数据挖掘特点

- **数据**
  - 人能看到的，听到的，闻到的，能感觉到的事物都是数据
  - 而我们人看不见的，听不见的，感觉不到的事物或者关系同样是数据，而且很多关键的数据正是隐藏在某些关系之中。
- **挖掘**
  - 一是从众多的数据中提取处理出有用的数据；
  - 二是从已知的数据中，通过研究它们之间的关系来发现总结出隐藏的数据和一般规律。


数据库
数据库
数据库
数据库
数据库