

计算机网络安全技术

李巍

liw@buaa.edu.cn

北航 计算机学院

2024年春季

教学目标

- ◆理解网络空间安全体系结构的基本概念和基本原理
- ◆掌握计算机网络安全技术的基本原理和方法
- ◆掌握主流的网络攻防基础方法和技术
- ◆了解Internet的安全性，增强安全意识



主要内容及课时安排

- ◆ 概述 (2)
- ◆ 数据加密技术：密码学基础 (4)
 - ❖ 基本概念和方法；对称密码体系；公钥密码体系
- ◆ 身份认证与密钥管理技术 (2)
- ◆ 访问控制技术 (2)
- ◆ 网络安全基础设施 (12)
 - ❖ 安全协议：网络层，传输层，应用层
 - ❖ 安全防御设施：防火墙；入侵检测IDS；IPS；VPN
 - ❖ 网络攻防技术基础
- ◆ 系统安全和应用安全 (6)
 - ❖ 恶意软件
 - ❖ Web安全
- ◆ 新技术与网络安全（物联网、云计算、AI） (4)

网络安全基础理论
学习构建安全系统

理解网络安全协议和工具

系统安全和应用安全
了解网络攻防技术

课程安排

◆ 本课程所需基础知识

- ❖ 操作系统、程序设计、计算机网络等

◆ 授课方法

- ❖ **课堂讲解** (背景知识、基本原理 + 安全主题)
- ❖ **课后习题** (巩固基本概念, 可作为期末复习题)
- ❖ **小组大作业** (**团队合作, 动手实践**: 课程提供大作业素材, 包括参考资料和基本代码等。可选择课程**指定题目**, 也可以**自选题**)

◆ 课件下载、课程参考资料、作业提交

- ❖ **在线教学平台**spoc.buaa.edu.cn, **北航云盘**bhpan.buaa.edu.cn

◆ 建立课程微信群

◆ 考核方式 (百分制)

- ❖ **平时成绩**: 50% (考勤: 5%; 作业: 45%)
- ❖ **期末考试**: 50% : 2小时, **开卷** (**最后一次课随堂考**)

计算机网络安全技术

5

参考书目

- ◆ William Stallings, Lawrie Brown, 计算机安全原理与实践 (第四版), 机械工业出版社, 2019年3月
- ◆ 龚俭, 杨望, 计算机网络安全导论 (第3版), 东南大学出版社, 2020年9月
- ◆ Michael T. Goodrich, Roberto Tamassia, 计算机安全导论, 清华大学出版社, 2012年3月
- ◆ 斯坦普 (Mark Stamp) 著; 张戈 译, 信息安全原理与实践 (第2版) [Information Security: Principles and Practice, 2nd Edition], 清华大学出版社, 2013年5月
- ◆ 参考资料

计算机网络安全技术

6

网络安全的重要性

- ◆ 云计算，物联网的普及，对信息传输、存储、共享的依赖，增加数字世界的风险
- ◆ 网络安全已经渗透到国家的政治、经济、社会稳定、军事等领域

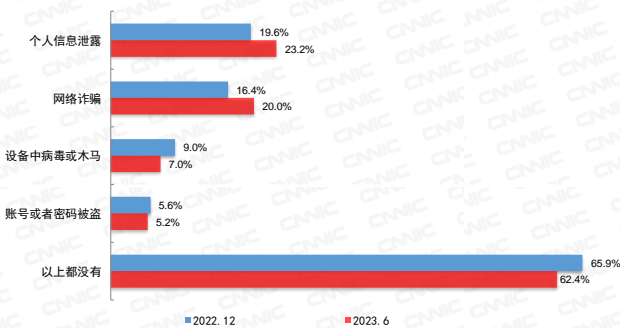


计算机网络安全技术

我国网络安全现状

- ◆ 2023年 中国互联网络信息中心(CNNIC) 发布第52次《中国互联网络发展状况统计报告》 “第五章 互联网安全状况”
 - ❖ 网民上网过程中遇到的安全问题

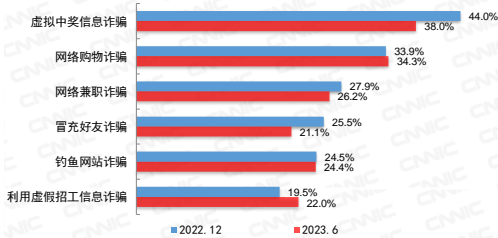
网民遭遇各类网络安全问题的比例



来源：CNNIC 中国互联网络发展状况统计调查

2023.6

网民遭遇各类网络诈骗问题的比例



来源：CNNIC 中国互联网络发展状况统计调查

2023.6

计算机网络安全技术

我国网络安全现状与挑战

◆ 网络安全监测仍是重点

- ❖ 公共互联安全事件不断增加：2022年钓鱼邮件攻击凸显，峰值超200Gbps中大型DDoS攻击同比增幅大
- ❖ 融合领域安全风险突出：工业互联网僵尸网络感染隐患严重，车联网漏洞利用风险较高

◆ 网络安全仍然面临严峻的挑战，对防御技术手段也提出更高要求

- ❖ 勒索软件攻击
- ❖ 网络钓鱼攻击
- ❖ 软件供应链安全
- ❖ 物联网安全
- ❖ 基于人工智能（AI）的攻击

计算机网络安全技术

9

思考

◆ 你的网络面临的最大威胁是什么？

◆ 你的网络可能受到攻击吗？

◆ 如何保护你的网络？

◆ 网络安全的法律规章？

◆ 你的个人信息如何保护？

◆ 信息系统有哪些漏洞？

◆ 如何保护系统和数据的安全？

◆ 谁能访问你的信息？

◆ 通信数据在网络传输中能否被泄露？

聚焦 网络

术语
工具
方法

聚焦 信息


计算机网络安全技术

10

案例与问题

密码学的应用-1



◆ 浏览器  https://www.baidu.com

证书

预期目的(N): <所有>

个人 其他人 中间证书颁发机构 受信任的根证书颁发机构 受信任的发布者 未受信任的发布者

颁发给	颁发者	截止日期	友好名称
360 OV Server C...	Certification Autho...	2029/4/9	<无>
COMODO RSA ...	COMODO RSA Ce...	2029/2/...	<无>
DigiCert Global ...	DigiCert Global Ro...	2028/8/1	<无>
DigiCert SHA2 S...	DigiCert Global Ro...	2023/3/8	<无>
Encryption Every...	DigiCert Global Ro...	2027/11/...	<无>
Gandi Standard ...	US&K.Irust: RSA Ce...	2024/9/...	<无>
GeoTrust RSA C...	DigiCert Global Ro...	2027/11/...	<无>
GeoTrust SSL CA...	GeoTrust Global CA	2022/5/...	<无>
GlobalSign Du...	GlobalSign Root CA	2024/2/...	<无>
GlobalSign Ext...	GlobalSign	2026/9/...	<无>

导入(I)... 导出(E)... 删除(R) 高级(A)

协议https如何保证安全？

证书的作用是什么？

密码学的应用-2

◆ 区块链 (Blockchain) 是一种由多方共同维护, 使用**密码学**保证传输和访问安全, 能够实现数据一致存储、难以篡改、防止抵赖的记账技术, 也称为**分布式账本技术 (Distributed Ledger Technology)**



- ❖ 点对点的分布式记账方式、多节点共识机制、**非对称加密**、智能合约
- ❖ 不可篡改、防伪、可追溯
 - 保密性, 完整性如何保证? (数据指纹: **哈希算法**)
 - 隐私保护
 - 零信任协议

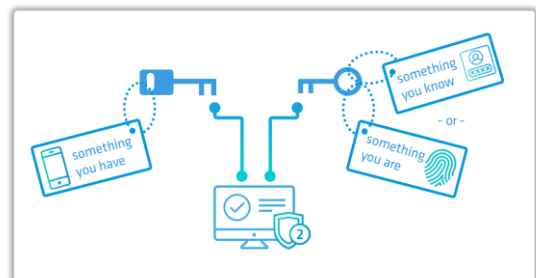
◆ 挖矿病毒?

身份认证

◆ 双因素认证 (Two-factor authentication, 简称 2FA)



- 为什么需要双 (多) 因素认证?
- 2FA的安全性如何?
- 忘记密码, 如何恢复?



安全事件：WannaCry勒索软件

◆ 2017年5月12日，WannaCry勒索软件

- ❖ 导致100多个国家的数十万用户的计算机遭到攻击，其中包括医疗、教育等公共事业单位和一些大公司
- ❖ 这款**恶意代码**对计算机内的文档、图片、程序等实施高强度的加密锁定，并向用户索取**以比特币支付**的赎金。



◆ 工具：攻击者利用NSA(美国国家安全局)设计的Windows系统黑客工具“永恒之蓝Eternal Blue”

- ❖ 利用Windows的**445端口**传播，该端口在Windows主要是提供局域网中文件或打印机共享服务。
- ❖ **蠕虫病毒**

计算机网络安全技术

16

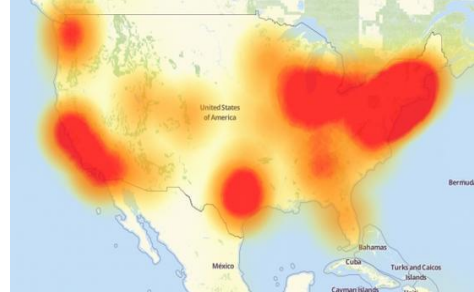
WannaCry ransomware



安全事件：Mirai僵尸网络

◆ 物联网Mirai僵尸网络攻击

- ❖ 2016年10月21日，美国多个城市出现互联网瘫痪情况，包括Twitter、Shopify、Reddit等在内的大量互联网知名网站数小时无法正常访问。
- ❖ 美国域名服务提供商Dyn公司遭到大规模的“分布式拒绝访问服务（DDoS）”攻击。



◆ 工具：Mirai僵尸网络工具，僵尸网络中包含了大量可联网设备

- ❖ 例如监控摄像头、路由器以及智能电视等等。
- ❖ 有大约60万台的物联网设备参与

安全事件：心脏出血Heartbleed漏洞



◆ 开源软件包OpenSSL

- ❖ 提供主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议

◆ 2014年4月爆出了OpenSSL的Heartbleed漏洞，该漏洞是近年来影响范围最广的高危漏洞，涉及各大网银、门户网站等。

- ❖ 该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码



◆ OpenSSL又被曝出存在“水牢DROWN漏洞”（2016年3月）

- ❖ 由于全球2/3的网站服务器都是采用OpenSSL协议加密，为全球网站带来巨大安全挑战。

安全事件：核弹级漏洞log4shell

- ◆ 2021年12月10日公开的核弹级漏洞log4shell席卷全球，多国机构相继发出警告
- ◆ 全球近一半企业因为该漏洞受到了黑客的试图攻击。已证实服务器易受到漏洞攻击的公司包括苹果、亚马逊、特斯拉、谷歌、百度、腾讯、网易、京东、Twitter、Steam等。
- ◆ Log4j 漏洞可能需要数月甚至数年时间才能妥善解决
- ◆ Apache Log4j2是阿帕奇软件基金会（专门为支持开源软件项目而办的一个非营利组织）下的一个开源项目，它可以灵活控制日志生成过程，控制每一条日志的输出格式和输送的目的地。

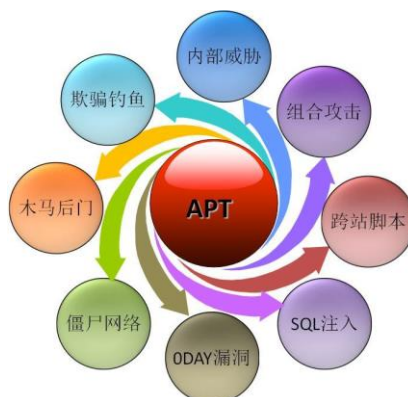
- ◆ 攻击者向Log4j2组件传入一个精心构造的指向恶意软件的地址，便可将恶意软件下载到本地并执行，导致之前精心设计的安全防护体系被轻松绕过，服务器完全落入攻击者的掌控中
- ◆ 漏洞
 - ❖ CVE-2021-4428，该漏洞使攻击者能够实现远程代码执行
 - 通过受影响的设备或应用程序访问整个网络
 - 运行任意代码
 - 访问受影响的设备或应用程序上的所有数据
 - 删除或加密文件

APT攻击事件



- ◆ **APT攻击(Advanced Persistent Threat, 高级持续性威胁)**是利用**先进**的攻击手段对**特定目标**进行**长期持续性**网络攻击的攻击形式。

- ❖ 90%以上的APT目标攻击采用**鱼叉式网络钓鱼**攻击手法。
- ❖ **高危漏洞**修复率偏低



计算机网络安全技术

25

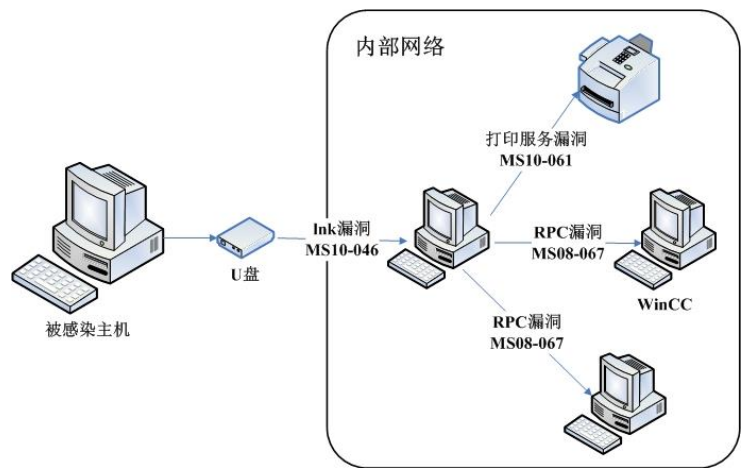
例：震网攻击(超级工厂病毒攻击)

- ◆ 2010年**伊朗**布什尔核电站遭到**Stuxnet**蠕虫的攻击，导致离心机超速运转并损毁
- ◆ 核电站计算机系统实际上是与外界**物理隔离**的，理论上不会遭遇外界攻击。
- ◆ 超级工厂病毒的攻击者针对**核电站**相关工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击，以此为第一道攻击跳板，进一步感染相关人员的U盘
- ◆ 病毒以**U盘**为桥梁进入“堡垒”内部，利用多种漏洞，包括当时的一个**0day漏洞**进行破坏
- ◆ 有效控制攻击范围

计算机网络安全技术

26

震网攻击（续）

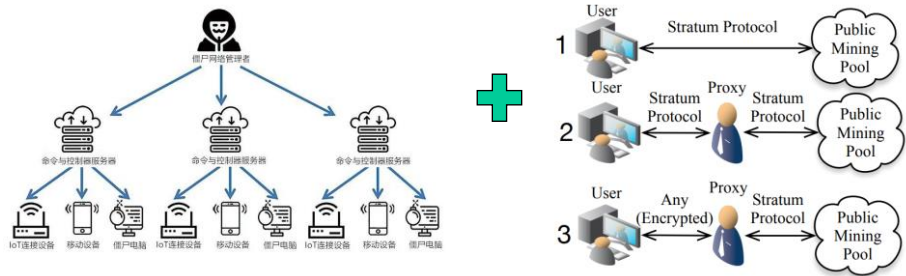


计算机网络安全技术

27

安全事件：挖矿病毒

- ◆ 僵尸网络 (Botnet)、木马 (trojan)
- ◆ 挖矿行为：虚拟货币（比特、以太、**门罗币**）
- ◆ 挖矿病毒 (Crypto-mining botnet)：利用**木马**控制他人的计算机组建**僵尸网络**集群进行挖矿
 - ❖ 丢失算力，耗电巨大
 - ❖ 被植入勒索病毒，携带APT攻击代码等，导致组织重要数据泄露等严重安全事件

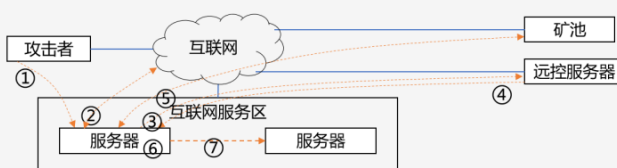


计算机网络安全技术

29



- ①发起攻击
- ②请求DNS
- ③回连远控
- ④下发指令
- ⑤连接矿池
- ⑥更新策略
- ⑦扩散感染



安全事件：钓鱼邮件

◆钓鱼邮件（phishing）

- ❖ 通过发送欺骗性垃圾邮件，意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID、ATM PIN 码或信用卡详细信息）的一种攻击方式
- ❖ 善于利用人们的心理，针对社会热点事件、节假日等特定要素，攻击成本低，技术门槛低
- ❖ 社会工程学攻击

◆主要有两种类型

- ❖ 广撒网型：发送大量的钓鱼邮件，愿者上钩。获取银行账号和密码，社交账号和密码。可用于实施后续的攻击。
- ❖ 鱼叉攻击：这是高级持续性威胁APT的一种渗透方式。攻击者针对特定的目标，有针对性的构造邮件。邮件或者带有附件，或者是恶意URL，受害者打开附件或者点击链接后，植入木马后被控制。通常是以长期的潜伏，窃取机密情报为目的。

钓鱼邮件实例

◆ 诱导回复

 **Dykim** <dykim@sbmetal.co.kr>
2021/8/31 23:21

To: [REDACTED]

Good day,

Our company is interested in your products
May we know your MOQ and Delivery time to Singapore.

Note: Our company profile, Products Specifications and Samples will be
sent to you upon the receipt of your feedback via WeTransfer, please
kindly confirm the same as soon as possible.

In case of any discrepancies, please get back to us within 2 working days.

Waiting for your kind reply.

Dykim,

HACO TRADING SERVICE CO.,LTD
[REDACTED]

诱导性语句

32

钓鱼邮件实例

◆ 骗取口令

 **buaa.edu.cn** <marie@forum8.co.jp>
2021/8/31 20:06

To: [REDACTED]

ID: [REDACTED]

Your [REDACTED] password expires today 8/31/2021 12:06:14 p.m.

Use the button below to continue with same password

[Continue](#)

Note: Your mails may not be delivered until you verify your account.

Sincerely,

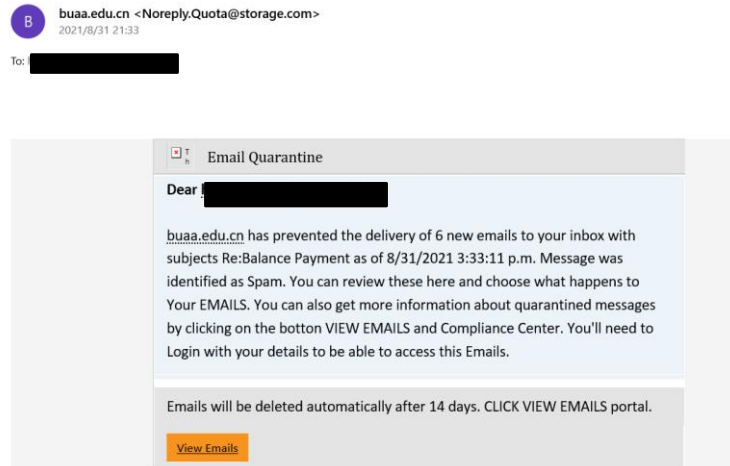
buaa.edu.cn IT-Support.

伪造网站链接

33

钓鱼邮件实例

◆ HTML伪装



34

网络安全的趋势

- ◆ 网络威胁的边界将逐步消失（传统以防火墙为边界）
 - ❖ 钓鱼邮件、勒索病毒等传播途径、加密手段多样化
- ◆ 针对**关键基础设施**的网络攻击升级，攻防两端的对抗将加剧
- ◆ **机器学习和人工智能**加入网络安全对抗
 - ❖ 人工智能将是下一代安全解决方案的核心
- ◆ 云端服务包含了大量的犯罪、恶意的服务，包括勒索攻击、DDoS攻击等行为，采用网络服务即可实现
 - ❖ **零信任框架**将成为企业安全的必然选择
- ◆ 威胁情报导向的网络安全
 - ❖ 通过对所获取的**威胁情报**进行攻击动机、威胁类别的分析研判，能够更加主动地应用多种响应策略进行网络安全对抗。**威胁狩猎**也将获得更广泛的应用，形成威慑性防御能力，提高犯罪成本。

网络安全形势：国内

- ◆ 维护网络安全首次列入我国政府工作报告
 - ❖ 2014年2月27日，中央网络安全和信息化领导小组宣告成立
 - ❖ 研究制定网络安全和信息化发展战略，不断增强国家安全保障能力
 - ❖ 信息安全问题上升到国家战略层面
 - ❖ 2014年4月，中国国家安全委员会第一次会议提出总体国家安全观的概念，其中网络安全是重要组成部分
 - ❖ 2018年4月，全国网络安全和信息化工作会议，推进“网络强国”战略

“没有网络安全就没有国家安全”

我国的法律法规

- ◆ 2021年3月9日，《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）
- ◆ 《中华人民共和国网络安全法》（简称《网络安全法》）经第十二届全国人大常委会第二十四次会议表决通过，于2017年6月1日施行
- ◆ 2019年5月13日，我国《信息安全技术网络安全等级保护基本要求》（简称：等保2.0）正式发布，2019年12月1日起正式实施
- ◆ 2021年8月17日，我国发布《关键信息基础设施安全保护条例》
- ◆ 2021年6月10日，《中华人民共和国数据安全法》正式发布，2021年9月1日起实施
- ◆ 2021年8月20日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，并于2021年11月1日起正式施行

《中华人民共和国网络安全法》

- ◆ 《中华人民共和国网络安全法》（简称《网络安全法》）经第十二届全国人大常委会第二十四次会议表决通过，于2017年6月1日施行
 - ❖ 提高网络空间管理水平
 - ❖ 增强网络空间安全综合防御能力
 - ❖ 推进网络社会法治创新
 - ❖ 提升我国在网络空间的国际话语权和规则制定权

《信息安全技术网络安全等级保护基本要求》

- ◆ 2019年5月13日，我国《信息安全技术网络安全等级保护基本要求》（简称：**等保2.0**）正式发布，2019年12月1日起正式实施。标志着等级保护标准正式进入2.0时代。
 - ❖ 是我国网络安全领域的基本国策、基本制度和基本方法
 - ❖ 在1.0的基础上更加注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。

《关键信息基础设施安全保护条例》

- ◆ 2021年8月17日，我国发布《关键信息基础设施安全保护条例》，旨在通过配套立法进一步明确**关键信息基础设施**安全保护的具体要求，保障国家关键信息基础设施安全。
 - ❖ 关键信息基础设施的范围：明确公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等属于基础设施范围。

《中华人民共和国数据安全法》

- ◆ 2021年6月10日，《中华人民共和国数据安全法》正式发布，2021年9月1日起实施。
- ◆ 《中华人民共和国数据安全法》是为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益而制定的法律。

《中华人民共和国个人信息保护法》

- ◆ 2021年8月20日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，并于2021年11月1日起正式施行。
- ◆ 《个人信息保护法》从自然人个人信息的角度出发，给个人信息上了一把“法律安全锁”，成为中国第一部专门规范个人信息保护的法律法规，对我国公民的个人信息权益保护以及各组织的数据隐私合规都将产生直接和深远的影响。

网络安全形势：国际

- ◆ 各国加速网络安全战略部署
- ◆ 美国从90年代后期开始注重关键基础设施来自网络空间的威胁，并先后制定出成熟的国家网络空间安全战略
 - ❖ 2014年2月，美国启动《网络安全框架》
 - ❖ 2017年8月18日，将美军网络司令部升级为美军第十个联合作战司令部，**网络空间**正式与海洋、陆地、天空和太空并列成为美军的第五战场
 - ❖ 2018年4月16日美国商务部国家标准与技术研究院（简称NIST）发布《提升关键基础设施网络安全的框架》（也被称为《**网络安全框架1.1**》），侧重于对美国国家与经济安全至关重要的行业（能源、银行、通信和国防工业等）
- ◆ 欧洲各国合作保障升级，加强网络安全立法，以应对日益严峻的网络攻击。制定《通用数据保护条例》；建立了欧盟网络安全认证框架，加强在线服务和消费设备的网络安全
- ◆ 日本尤其注重保障个人信息安全，大力发展网络作战能力。2018年1月，日本宣布拟设立网络和太空防卫指挥中心

作业-1

- ◆ 调研一个网络安全事件，分析该事件产生的原因和基本原理
- ◆ 准备：
 - ❖ 加入课程微信群
 - ❖ 组队：每个小组2-3人