--网络安全技术

计算机学与信息技术学院

刘峰　教授

交通运输网络安全技术

(1)交通运输面临的网络安全问题

(2)网络安全基本概念、方法与技术

(3)交通运输网络安全对策

(4)有关法律法规

思考题

（1）交通运输面临的网络安全问题

- 现代信息技术特别是互联网的快速发展，极大提升了交通运输装备自动化水平和服务质量，但同时也带来了安全隐患。

- 国家互联网信息办公室2016年12月27日发布《国家网络空间安全战略》中强调指出：

  “网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。”

交通行业面临的网络安全问题

随着交通运输行业越来越依赖一些网络科技，例如GPS定位、通信系统等，这些虽然可以有效的提高工作效率，但是网络安全隐患不容忽视，恶意攻击者可以通过网络来控制交通工具。

此外，交通行业网络平台通常包含大量信息数据，有些恶意攻击者开始攻击平台来窃取数据

交通网络安全案例：铁路、公路、航空

- **公路：** 2015年7月，两名美国黑客远程破解并控制了克莱斯勒旗下的JEEP汽车，克莱斯勒公司因此召回了140万辆汽车；

- **航空：**2015年6月21日，波兰航空公司的地面操作系统遭遇黑客袭击，致使系统瘫痪长达5小时，至少10个班次的航班被取消，1400多名乘客滞留华沙弗雷德里克·肖邦机场。这是全球首次发生航空公司操作系统被黑的状况。

- **铁路：**澳大利亚Metro铁路公司内部报告泄露，显现出墨尔本铁路网络中存在5800多个错误，铁路IT系统中的“安全漏洞”，令该州公共网络骨干暴露在“广泛或完全丧失铁路服务”的威胁之下。 主要问题之一是铁路控制系统的发现、预防、检测和响应网络安全事件的安全控制有限。

技术挑战

发生网络问题主要是由于对技术的依赖（例如定位、通信系统等新科技的加入），最终导致出现了风险问题，恶意攻击者可以远程对这些系统进行操作，同时也可以破坏这些系统。一旦发生恐怖主义攻击，无论是物理还是网络级别的攻击，都有可能对交通运输业造成巨大损失，并导致长期的社会经济问题。

云计算、大数据、移动互联网、物联网等新兴IT技术条件下的新挑战

国家互联网应急中心发布的《2014年我国互联网网络安全态势报告》显示，云服务正日益成为网络攻击的重点目标，移动应用程序成为数据泄露的新主体，“漏洞风险向传统领域、智能终端领域泛化演进。”

云计算、大数据、物联网、移动互联等新技术的采用，为交通运输的提升技术和服务水平带来了机遇，但同时也带来了网络安全的新的技术挑战。

交通网络安全面临的挑战

- 挑战：如何预防网络攻击，以减少网络攻击下的脆弱性，并在网络攻击发生时能减少遭受的破坏及其恢复时间。

- IT新技术的采用，使得交通网络安全问题更加突出，传统的方法已远远不能适应。

  仅仅依靠网络安全“老三样”（即入侵检测、防火墙、防病毒），已不能有效防范目前云与大数据、物联网、移动互联等新技术应用环境中的网络攻击，需要新的技术和方法（如，以数据分析为手段的预警等）。

(2)网络安全基本概念、方法与技术

网络安全，是指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络存储、传输、处理信息的完整性、保密性、可用性的能力。

（注：引自我国《网络安全法》，2016）

网络安全的实质

- 保证系统中的人、设备与设施、系统、数据、应用等要素，避免偶然的或人为的破坏或攻击，使其发挥发挥正常，保障系统能安全可靠地工作。

- 网络安全管理不仅是技术上的，更多的可能涉及到制度以及人的因素。

  美国CSI/FBI在《计算机犯罪与安全调查报告》中指出，因内网安全漏洞造成的损失占所有计算机安全事故的一半以上(主要成因：人+制度).

网络安全管理发展趋势：协同和整合（技术+制度+人）

- 国内外计算机犯罪统计数字表明，网络安全管理不仅仅是技术上的，更多的可能涉及到制度以及人的因素。

- 网络安全管理的重要性日趋重要，并呈现协同和整合的发展趋势。

网络安全管理：框架、系统与技术

- **安全框架与评估标准**

  国际安全评价标准

  我国计算机安全等级划分与相关标准

- **网络安全管理系统**

  安全系统的一体化监管

- **网络安全管理技术**

  访问控制、入侵检测、灾难恢复与业务持续等

常用网络安全技术

1、 防火墙（Firewall）

是位于两个信任程度不同的网络之间的软件或硬件设备的组合，用于防止网络之间发生未经授权的访问，其筛选检测依据是所部署的安全策略（服务、用户和行为等）。

2、入侵检测系统IDS(Intrusion Detection System)

是一种计算机设备或软件，用于实时监视和报告网络中的恶意行为。可根据用户历史行为模型、专家知识及模型对用户当前操作进行判断，有入侵迹象即断开其与主机的连接，并收集证据和实施数据恢复。

3、虚拟专用网VPN(Virtual Private Network)

可替代租赁专用线路，用于在公网中提供保密通道，即保证信息在传输过程中不被窃听、篡改、复制。核心技术包括隧道技术、密码技术和服务质量保证技术（QoS）。

网络示意图

- 参见第五章内容（或ITU标准）

(3)交通运输网络安全对策

交通网络安全面临的技术挑战

计算机网络的脆弱性，将可能使交通运输基础设施和信息系统的安全面临威胁。

- 问题： 如果黑客未经授权远程接入交通运输电子设备系统，那么现代交通工具持续增加的网络互联特性（云、大数据、物联网等）将使其本身暴露在网络威胁中。
- 对策：采用国际上先进的方法、技术和管理经验，是交通领域积极防御和有效应对网络安全威胁的有效途径。

交通网络安全的三种模式：防御+制止+检测

交通网络安全的三种模式防御、制止、检测。三者互为补充，同样重要。

- **防御策略：**能使攻击者无法进入，并减少内部滥用和事故；防火墙、病毒过滤等
- **制止策略：**能防止商业目标和处理过程遭到破坏，并使公司保持效率以提高生产率
- **检测策略：**能对决策者起到警告作用，以进行防范。审计跟踪、入侵检测、安全态势感知等

航空案例：美国将提高网络安全水平

- 美国政府2015年发布报告**《为了下一代机构转型：美国联邦航空管理局（FAA）需要更综合的解决方案以解决网络安全问题》**，提出网络互联特性带来的网络威胁及其对策。

飞机网络系统及其防御对策：

- 网络互联设备系统：飞机卫星导航的监测和广播服务子系统（SBSS）。
- 防御网络威胁对策：改善安全控制和入侵检测。

汽车网络安全

2016年11月，美国国家公路交通安全管理局（NHTSA）正式发布《汽车最佳网络安全指南》，帮助汽车制造商应对网络攻击可能给联网汽车带来的安全威胁，提供了如何防止汽车被接入未授权网络，如何保护关键安全系统与个人数据，以及如何从网络攻击中快速恢复等方法，并藉此进行了广泛的网络安全测试。

要点：网络安全问题应当是汽车厂商和供应商关注的重中之重，新车产品研发的过程中就该妥善处理。车企和供应商应当进行“渗透测试”找到潜在的问题，测试结果报告要指出易受入侵的问题是如何解决的或解释测试漏洞无法解决的原因。

铁路对策

- 案例？

交通领域面临的新兴IT技术所带来的网络安全技术挑战

- **云网络安全**

  交通业务系统开始从传统的IT架构迁移到云架构，享受云计算和云服务带来的便捷，挑战：安全合规的云计算环境、云端安全等问题。

- **大数据安全**

  大数据分析技术为实现智慧交通提供了可行支撑条件，并在交通智能分析与预测等应用中开始显现其强大威力，，但同时带来数据安全、隐私保护等瓶颈问题需要解决。

- **物联网安全**

  交通数据采集越来越依赖于物联网中的智能传感器技术，同时传感，其网络特性带来了新的网络安全技术挑战，而负责信息处理的工业控制计算机的安全问题日趋突出。

- **移动互联安全**

  移动通信与互联网融合的产物，为交通信息资源的随处漫游访问提供了条件，但其安全问题是移动互联网健康课持续发展的关键所在（移动端身份认证与授权、加密保护等）。

（4）网络安全有关法律法规

- 法律法规是构建信息系统安全的第一道防线，可用于防范计算机犯罪，并维护信息系统所有者及合法用户的安全权益。（维权）
- 法律还可使公众了解什么是网络时代的违法行为，创 造良好社会环境。（自律）
- 在推进人工智能应用中加强隐私保护。 习近平同志强调，要加强人工智能发展的潜在风险研判和防范，维护人民利益和国家安全，确保人工智能安全、可靠、可控。 在人工智能应用中加强隐私保护，需要加强人工智能应用的风险研判和防范，综合运用技术创新、伦理规范、法律制度等手段方式，防止其“野蛮生长”，确保在符合伦理规范的前提下实现人工智能健康发展。

掌握网络安全法律法规的必要性

- 信息系统相关人员在制定法律和管理有效的网络信息安全策略和方法时，需要理解处理计算机犯罪的法律和法规。

- IT专业人员将在防止、减少及恢复计算机攻击的损失过程中扮演重要角色，不仅需要技术，同时需要法律知识（还进一步要求及时更新这些不断完善的法律和法规）。

国内外立法与规划情况

1987 美国《计算机安全法》

2001 美国《确保网络空间安全的国家战略》

2023 全球首部全面监管AI欧盟版《人工智能法案》出炉

2016 中华人民共和国《网络安全法》

2016《国家网络空间安全战略》国家网信办

中华人民共和国《网络安全法》

- 2015年　7月8日　征求意见稿
- 2016年11月7日　正式通过立法
- 2017年　6月1日　施行

《网络安全法》共有七章七十九条，突出六部分内容。

一是明确了网络空间主权的原则；

二是明确了网络产品和服务提供者的安全义务；

三是明确了网络运营者的安全义务；

四是进一步完善了个人信息保护规则；

五是建立了关键信息基础设施安全保护制度；

六是确立了关键信息基础设施重要数据跨境传输的规则。

《网络安全法》要点

一、相关义务

- **网络运行安全**

  国家实行网络安全等级保护制度，并对**交通行业等重点行业**和领域，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法**由国务院制定。**

- **网络信息安全**

  网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

- **监测预警与应急处置**

  负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

《网络安全法》要点（续）

二、相关法律责任

规定了网络运营者、关键信息基础设施的运营者、电子信息发送服务提供者、应用软件下载服务提供者在履行义务不力情况下的惩罚条例。

小结

- 网络安全的本质是保证系统中的人、设备与设施、系统、数据、应用等要素，避免偶然的或人为的破坏或攻击，使其发挥发挥正常，保障系统能安全可靠地工作。
- 网络安全的三维结构：防御、制止、检测，三者互为补充。AI技术应用带来新的技术挑战。
- 交通领域网络安全的建设重点，应依据法律法规（如《网络安全法》等），针对IT新技术运营环境，注重网络安全防御体系、安全态势感知、安全事件处置与应急响应等。

思考题

1　简述网络安全的本质

2　简述网络安全的三维结构

3　给出物联网网络安全案例

4　简述AI技术带来的网络安全挑战。

延伸阅读建议

1、《中华人民共和国网络安全法》

2、《国家网络空间安全战略》国家网信办