电类学科创新前沿导论——网络安全

网络安全之初窥

孟魁 mengkui@sjtu.edu.cn

2021年4月25日

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

主要内容

01 何谓网络安全

02 网络空间安全挑战

03 网络安全演练与竞赛

网络之双刃剑

“INTERNET的**美妙**之处在于你和每个人都能互相连接，INTERNET的**可怕**之处在于每个人都能和你互相连接。”

- 网络安全
  - ≠病毒查杀
  - ≠口令破解
  - ≠黑客
  - ≠翻墙

安全的含义

安全的含义

国家安全

- 全国人大常委会通过的《国家安全法》规定，国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

安全

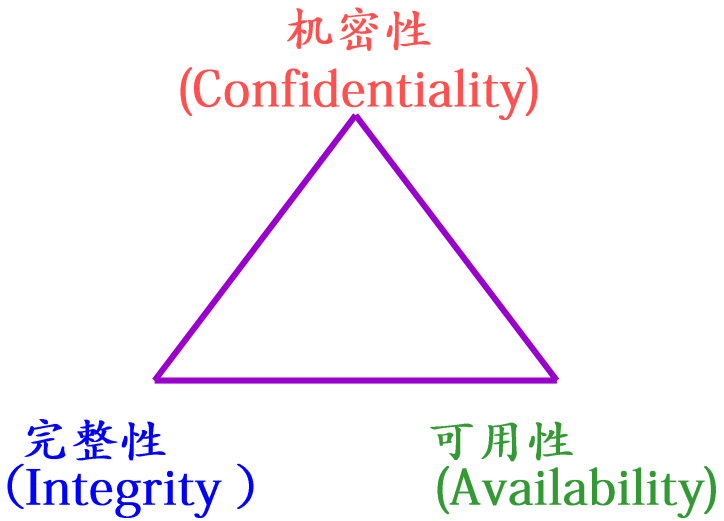
- 平安，无危险；保护，保全。 ----《汉语大词典》
- 没有危险；不受威胁；不出事故。 ----《现代汉语词典》

信息安全的含义

- **Bruce Schneier**
  - “如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是**安全**，而是**隐藏**”
  - “如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是**安全**...”

- **国际标准化委员会(ISO)定义**：
  - “为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏（可用性）、更改（完整性）、显露（机密性）”

信息安全的属性



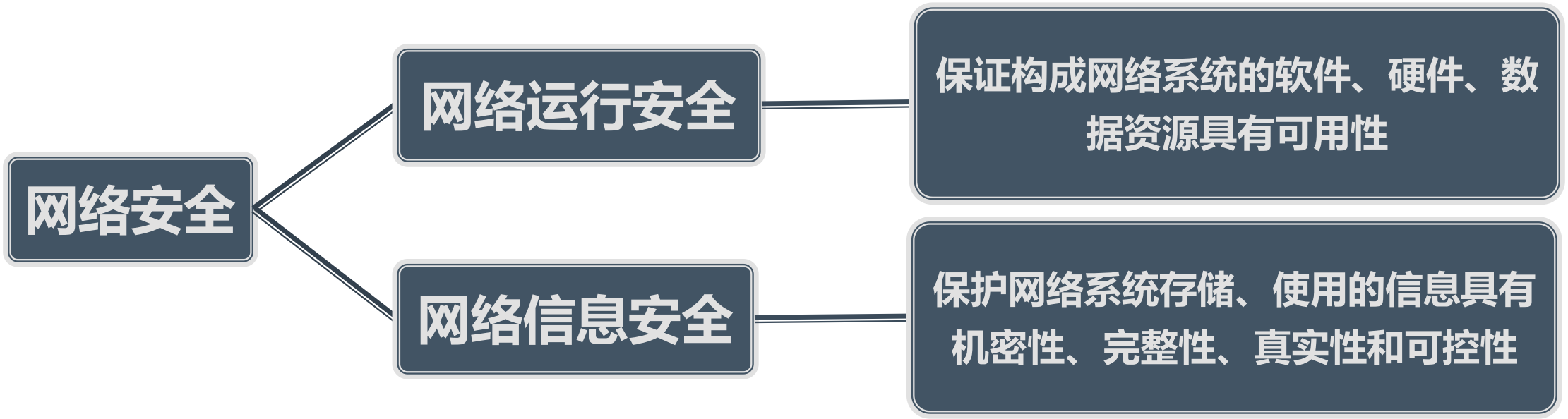
机密性、真实性

可控性、可用性

机密性、完整性、可用性、真实性、不可抵赖性

网络安全 Vs. 信息安全

- 网络安全=网络运行安全+网络信息安全



网络安全：　具有暂态性、动态性、相对性
不存在永恒的安全或者绝对的安全

主要内容

01 何谓网络安全

02 网络空间安全挑战

03 网络安全演练与竞赛

网络空间

- **网络空间（Cyberspace）**
  - **继陆、海、空、天之后的第五大空间**
  - **The interdependent network of information technology infrastructures, and includes the *Internet*, *telecommunications networks*, *computer systems*, and *embedded processors and controllers in critical industries*. Common usage of the term also refers to the virtual environment of information and interactions between people.**

    --National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23)，2008

网络空间发展

网络融合性：互联网，通信网络，广电网络，物联网IoT，工控网络…
终端多样性：PC，手机，平板，电视，手环，手表，智能终端…
内容多样化：云计算，社交网络，对等网络服务…
领域广泛性：涉及政治，经济，文化，军事等社会各个层面

20世纪90年代中期以前

技术发展阶段

INTERNET

NSFNET

ARPANET

20世纪90年代中期-2010年

商业化阶段

yahoo! amazon ebay

icq 網易 搜狐 SOHU.com

Google Tencent 腾讯 sina

Alibaba Group 阿里巴巴集团 Baidu 百度

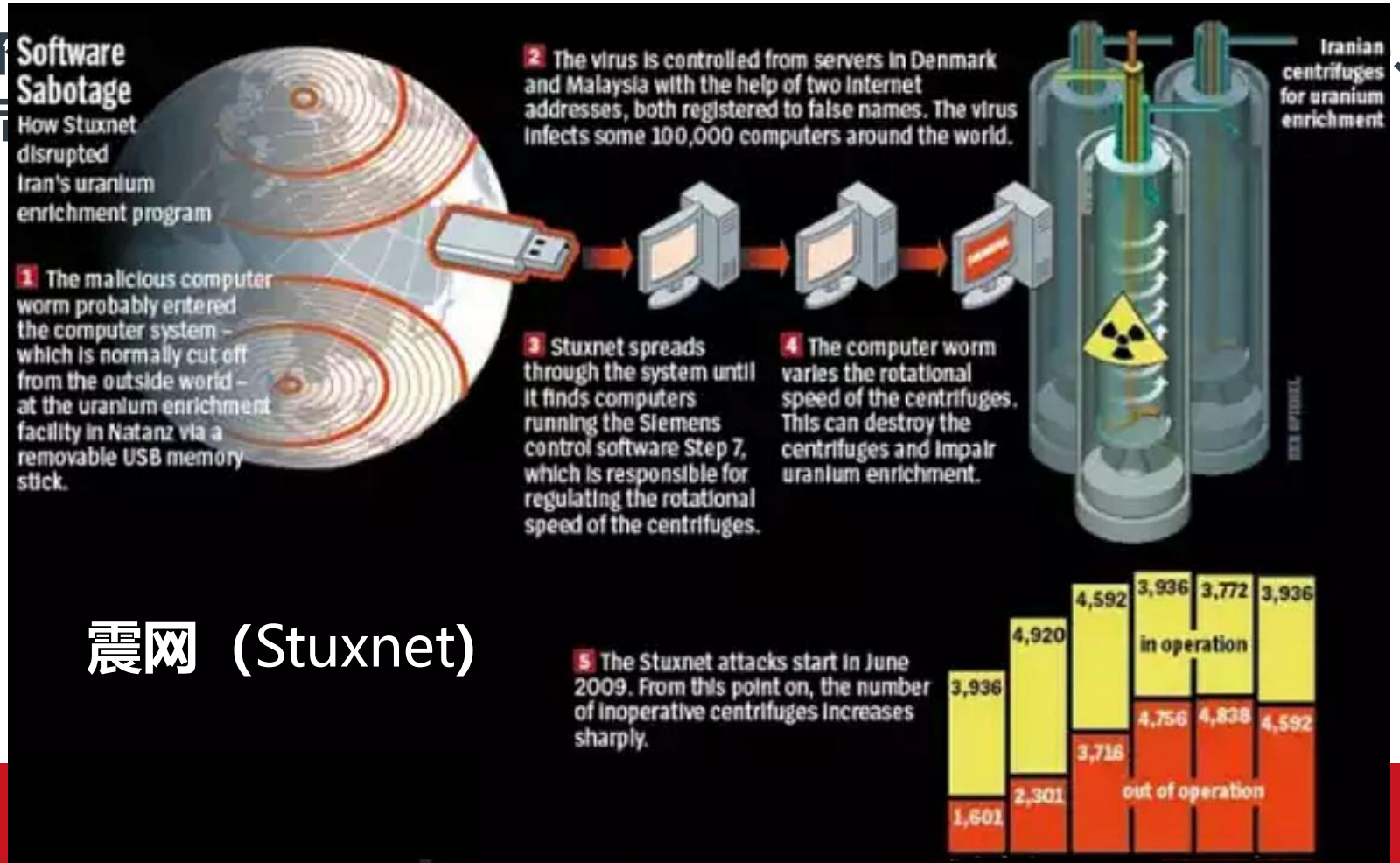
2010年以来

社会化阶段

WhatsApp facebook

网络空间泛在安全威胁

- 关键基础设施存在安全隐患
  - 电力、石化、供水、交通等城市基础设施信息设备存在大量漏洞
  - 据不



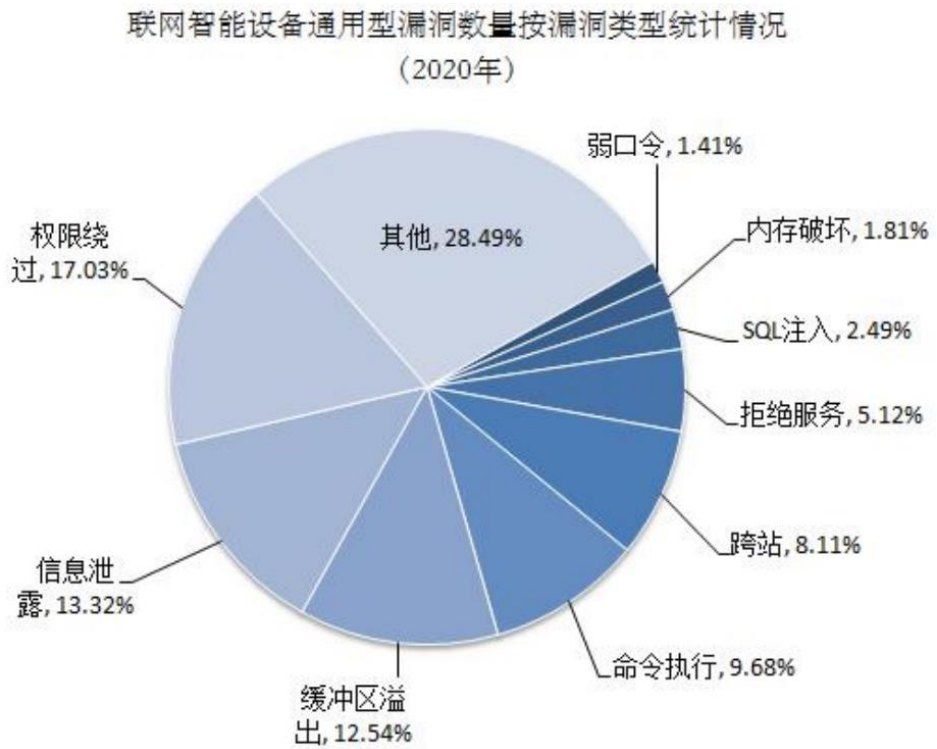
震网（Stuxnet）

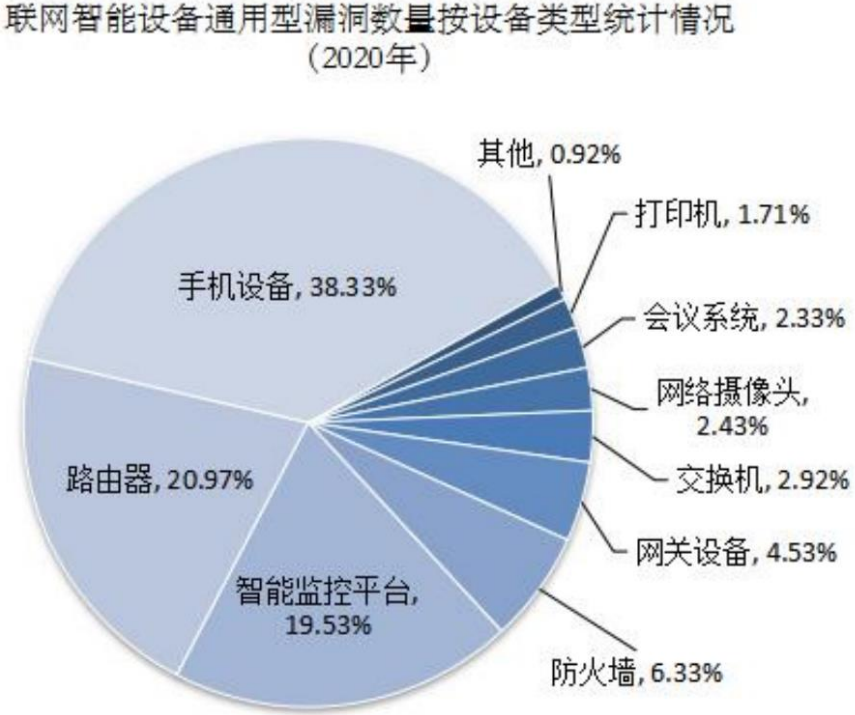
、施耐德等电气

网络空间泛在安全威胁

- 智能设备成为不法分子的目标
  - 成为攻击跳板
  - 存在功能缺陷

- 2020 年接入互联网的设备超过 380 亿台
- 2020 年，CNVD 收录通用型联网智能设备漏洞 3047 个（同比+28%）
- 2015年至今，CNVD已通报了多款联网摄像头存在





网络空间泛在安全威胁

- 数据泄露/数据暴露事件频发
  - 数据成为世界各国重要战略资源
  - 根据IBM最新的数据泄露年度成本研究，平均数据泄露成本高达392万美元
  - 2020年数据泄露呈现爆炸式增长，短短12个月内泄露的记录比过去15年的总和还多

美国选民数据库

新加坡艾滋病毒感染者敏感记录

网络空间泛在安全威胁

- 新型网络/应用带来新的安全威胁
  - 社交网络
    - 个人隐私泄露：地理位置、行动轨迹、日常活动、
    - 企业等的敏感信息泄露
    - 网络谣言
    - bot机器人账号
    - 不良文化
    - 。。。

网络空间泛在安全威胁

- 新型网络/应用带来新的安全威胁
  - 车联网
    - 车载信息娱乐服务、驾驶辅助系统和服务，如在线音乐、导航、路况和交通信息、应用软件实时更新、自动驾驶和基于司机驾驶情况的保险
    - 联网车辆正在产生越来越多的数据，其中大部分可以被视为个人数据

      车内摄像头、行车路径、驾驶习惯、发动机数据
    - 独立研究机构波莱蒙(Ponemon Institute) 曾预计[illegible]漏洞被召回

网络空间泛在安全威胁

- 有特殊目的、针对性更强的网络攻击越来越多
  - APT攻击
  - DDOS攻击
  - 国家支持
  - 。。。

- 2019年3月，委内瑞拉古里水电站遭反对派蓄意破坏，全国18个州断电
- 2020年5月，委内瑞拉国家电网的765千线遭到攻击，除首都加拉加斯外，全国11个州府均发生停电

网络空间泛在安全威胁

- 网络空间安全威胁泛在化和复杂化，网络攻击更有持续性和隐蔽性
- 网络空间安全最大的威胁是什么？
  - 是不确定威胁：未知漏洞、未知后门、未知攻击

AI & 网络安全

- AI伦理-百度李彦宏2018年
  - 第一，AI 的最高原则是**安全可控**；
  - 其次，AI 的创新愿景是促进人类更加平等地获得技术能力；
  - 第三，AI 存在的价值是教人学习，让人成长，而不是取代人、超越人；
  - 最后，AI的终极理想是为人类带来更多的自由和可能。

特斯拉一波未平一波又起。

4月17日晚间，广州增城一辆特斯拉撞上水泥墙上后自燃，事故造成副驾驶位乘客当场死亡。车祸发生时的视频最近在网上广为传播。**4月24日，车主左某的朋友冯先生代表车主接受红星资本局采访时称，事发前车辆向右变道后方向盘无法回正，AP（Autopilot，自动辅助驾驶）强制干预驾驶，以至于酿成惨剧。**

Stop Secret Surveillance Ordinance

AI & 网络安全

- 新挑战：
  - 人工智能？人工智障？

车主在斑马线前未“礼让狗”而被记违章？

AI & 网络安全

- **新挑战：**
  - **换脸：**Deepfake

AI & 网络安全

- 新挑战：
  - AI隐身术

图：一张贴纸“骗”过AI摄像头

图：远距离、近距离、稳定、动态拍摄下的“隐身”效果

- 新挑战：
  - AI障眼法

图：基于对抗样本生成的“眼镜”道具

AI & 网络安全

- 难点：
  - 安全事件往往出错成本高昂
    - 电商的推荐系统对出错的容忍度高
    - 工控系统、内容安全检测系统对出错的容忍度低
  - 数据要求高
    - 相关数据集难收集
    - 大量非结构化数据
    - 数据集处理的专业要求高，缺少自动化工具
  - 对抗环境的天然存在
    - 攻 vs 守

AI & 网络安全

- 难点：
  - 人工智能算法、架构或产品的不安全因素
    - 对AI模型的攻击
    - 对AI产品的攻击
    - 对AI数据（训练数据、测试数据）的获取

网络安全，以人为本

“三分技术,七分管理”

主要内容

01 何谓网络安全

02 网络空间安全挑战

03 网络安全演练与竞赛

网络安全演练

网络安全威胁堪比核武器
应搞"网上朱日和"

网络安全演练

美国

Cyber Storm
每两年举行一次

欧盟

Cyber Europe
每两年举办一次

网络安全演练

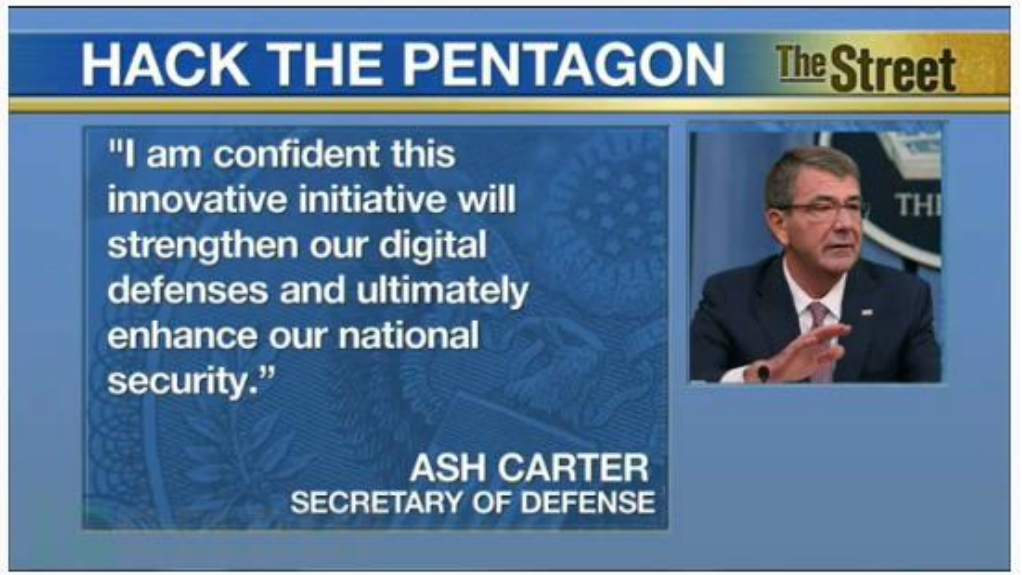
- 北约
  - 网络联盟演习（Cyber Coalition）
    - 2008年开始，每年一次

Locked Shields

Crossed Swords

网络安全演练

- 美国
  - 2016年3月，美国国防部宣布：邀请数千名经过审核的黑客参与五角大楼漏洞奖励计划
    - 18 April 2016，ran for 24 days.
    - 约250人参加，确认138个漏洞，58个黑客获得了超过8万美元的赏金
    - 最年轻的获奖者14岁



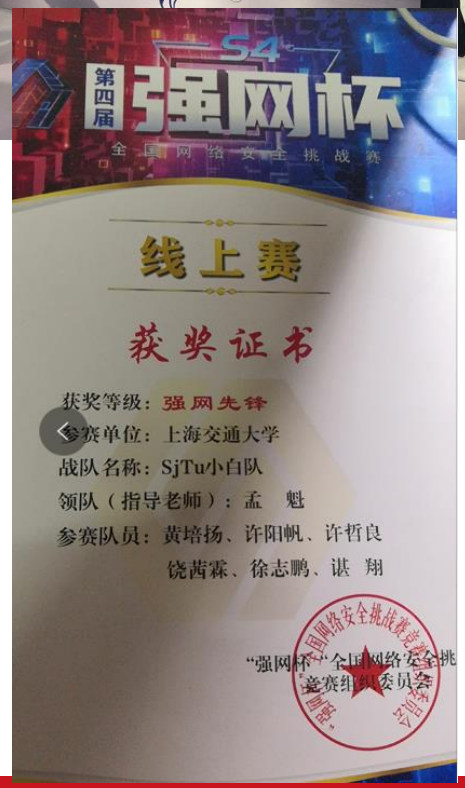
网络安全演练

- 美国
  - 陆续发起“黑进五角大楼”、“黑掉海军陆战队”、“黑掉陆军”、“黑掉空军”等
  - 发现了超过5000个各类漏洞，送出了超过30万美元的奖励。

美国网络司令部赞助

网络安全竞赛

- 国内CTF
  - 网鼎杯
  - 强网杯
  - 护网杯
  - 各类企业、高校的CTF赛事



全国大学生信息安全竞赛

- 2008年起，每年举办一次，由教育部高校信息安全专业教学指导委员会主办
- 2020月，该竞赛**正式入围**中国高等教育学会《高校竞赛评估与管理体系研究》专家工作组发布的**高校学科竞赛排行榜**
- 竞赛官网（http://www.ciscn.cn）
- 目前包括作品赛和技能赛两类竞赛，组队参赛。
  - 作品赛：分初赛（在线提交）、决赛（现场答辩）两阶段，自主命题、自主设计，3月报名，6月初赛，7-8月复赛（决赛）
  - 技能赛：分线上初赛、分区赛和全国总决赛三阶段，采用线上解题、线下攻防的方式。4月报名，5-6月 初/复赛，7-8月决赛

近年赛况

交大近五年赛绩

年份	报名数	作品赛			技能赛
		一等奖	二等奖	三等奖	
2016	8				等奖1
2017	1(				
2018	18				等奖1项
2019	13				等奖1项
2020	19（17/2）	7	1		一等奖1项

五次蝉联优秀组织奖

近五年获一等奖22项

网安创新人才训练营

- 网安创新人才训练营CITtrip项目
  - 面向所有对网络安全有兴趣的本科生，不限专业，不限年级
  - 定期发布，可参加发布的项目，也可以自行申报项目
  - 兴趣项目、培养项目、成长项目
    - 全国大学生信息安全竞赛
    - 第四届“强网杯”全国网络安全挑战赛--创新作品赛
    - 大创国家级项目
    - 全国高校计算机大赛网络技术挑战赛二等奖
    - 专利申请、论文撰写（发表）

联系方式： mengkui@sjtu.edu.cn

上海交通大學

网络空间安全学院

Q & A