Computer Ethics

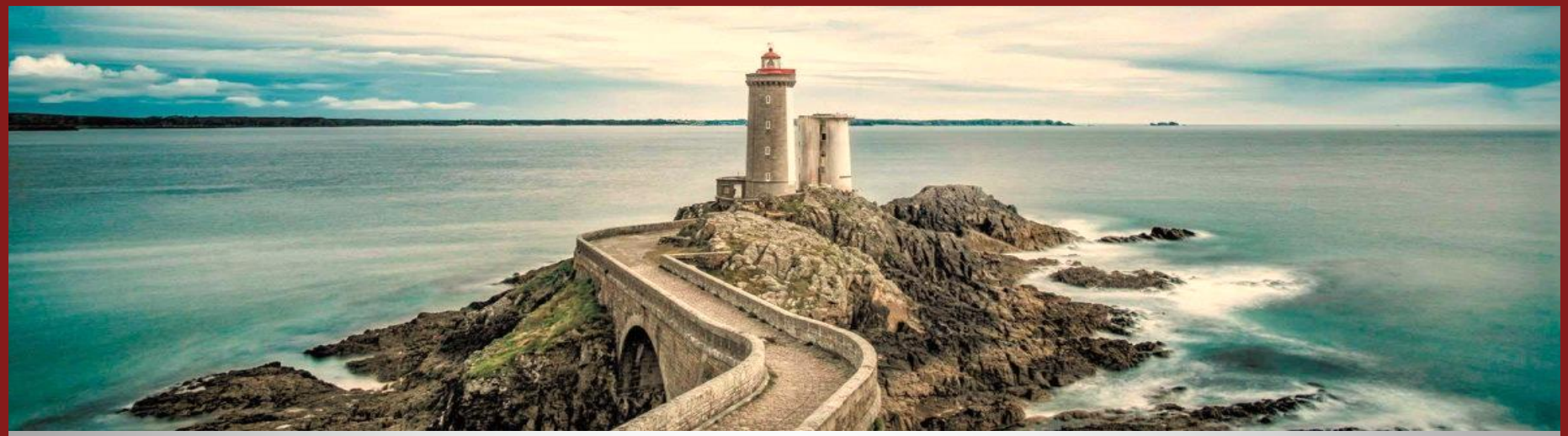
计算机伦理学

十-3、隐私保护

授课人: 李超 博士
chaol@sjtu.edu.cn

2020年 秋冬学期

上海交通大学计算机科学与工程系

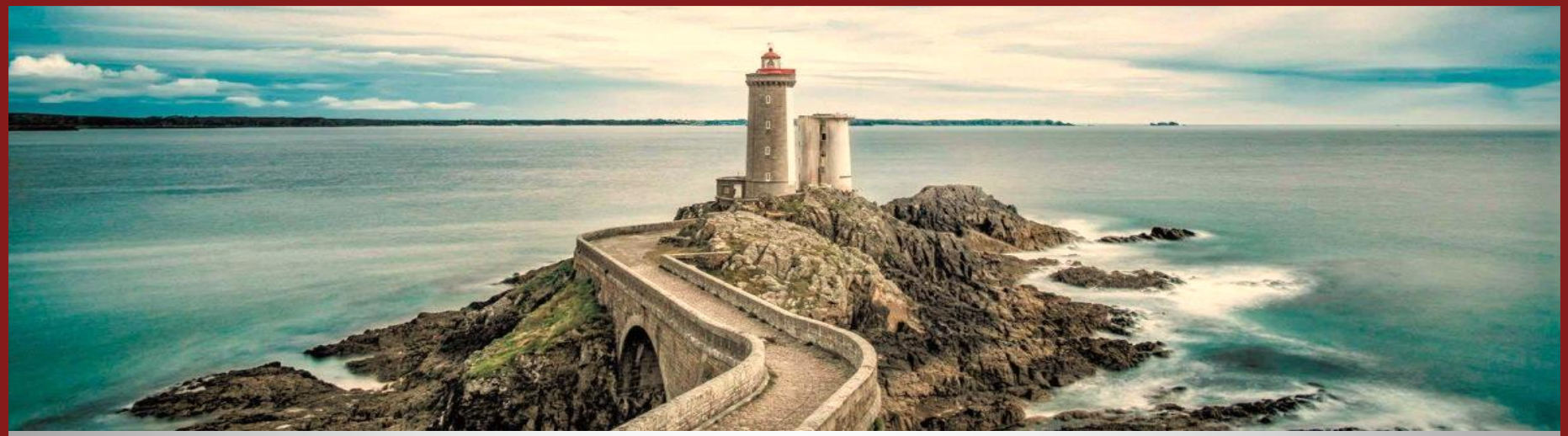


Course Review

上堂回顾

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 跨时空的交集: **人机和谐共存**
2. 言论自由思考: **冒犯是个问题**
3. 关于舆情分析: **关注民生民意**
4. 开放共享平台: **以己之力促进**



Course Outline

案例总览

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 谈计算机安全
2. 黑客伦理观察
3. 谈隐私的价值
4. 隐私问题观察

导言

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
WWW.CAC.GOV.CN

请输入检索关键词

首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题

当前位置：首页 > 正文

《国家网络空间安全战略》发布

2016年12月27日 12:11 来源：中国网信网 【打印】 【纠错】

如下词汇有什么区别?

Safety vs Security

不同类型的黑客

- **黑帽**：活动具有破坏性、不道德且通常非法的黑客
- **白帽**：利用技能演示系统漏洞，并帮助提高安全性
- **灰帽**：两者成分都有一些

黑客工具举例-1：

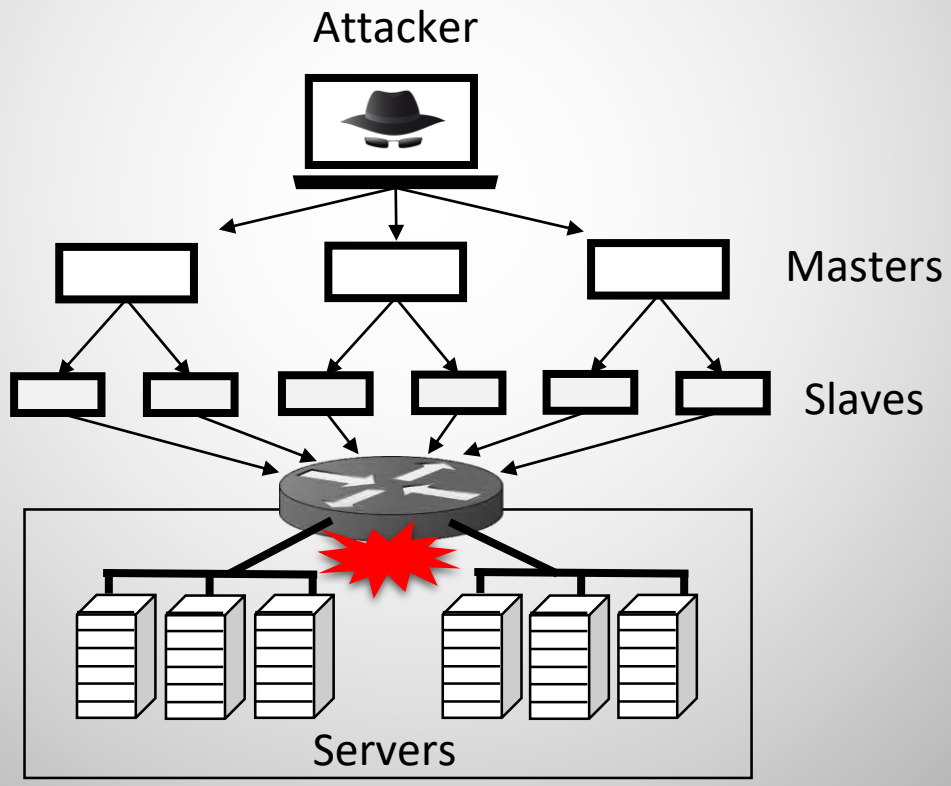
- **病毒**（virus）- 将自身附加到其他软件的代码，可以复制自身并执行其他功能
- **蠕虫**（worm）- 类似病毒，可以复制自身在电脑间传播，但不需要附着在某一程序上就可以运行
- **特洛伊木马**（Trojan horse）- 伪装成一个良性程序的软件应用程序，但携带着恶意构建的应用

黑客工具举例-2：

- **网络钓鱼**（phishing）- 发送海量信息，目的是套取一些有用的个人信息，如账户名密码等
- **勒索软件**（ransomware）- 对计算机或移动设备上的一些文件进行加密，然后索要解密的赎金
- **间谍软件**（spyware）- 可以监视和记录用户在计算机或移动设备上活动的软件，以达非法目的

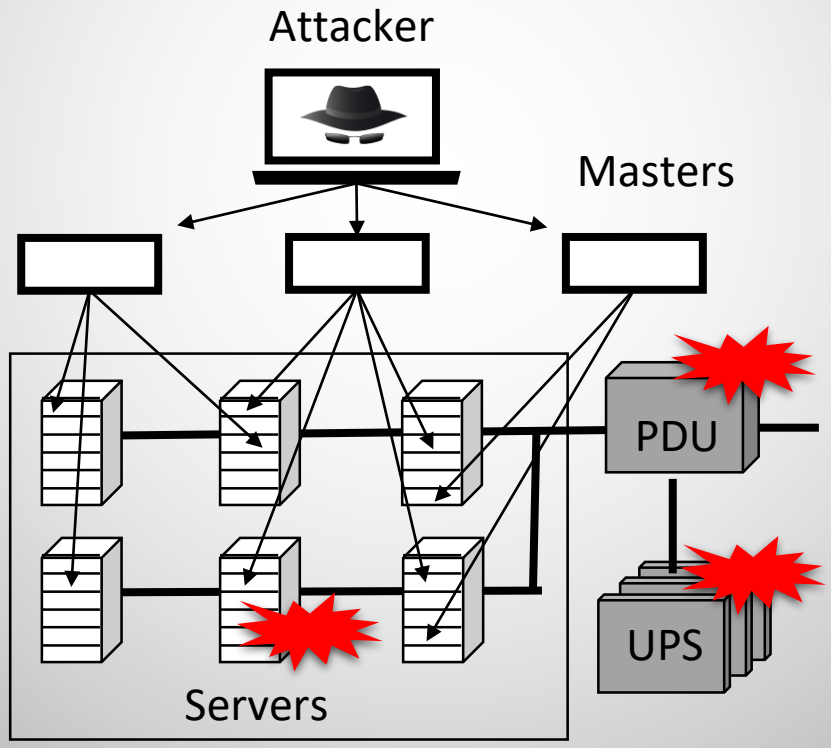
黑客工具举例-3：

- **拒绝服务**（Denial of Service, DoS）- 一些网络上的僵尸服务器利用大量请求把网站淹没



黑客工具举例-4：

- **性能攻击**（Performance Attack）- 通过对计算机关键资源施加恶意竞争，干扰用户正常应用性能。



零日攻击

- 若一漏洞发现的24小时内即被恶意利用，产生了攻击行为，则该漏洞是“Zero-Day Vulnerability”，该攻击被称为“Zero-Day Attack”。
- 零日漏洞除去会被白帽和灰帽黑客利用外，也会被黑帽黑客在地下黑市交易。
- 补救措施：软件补丁（Software Patch）

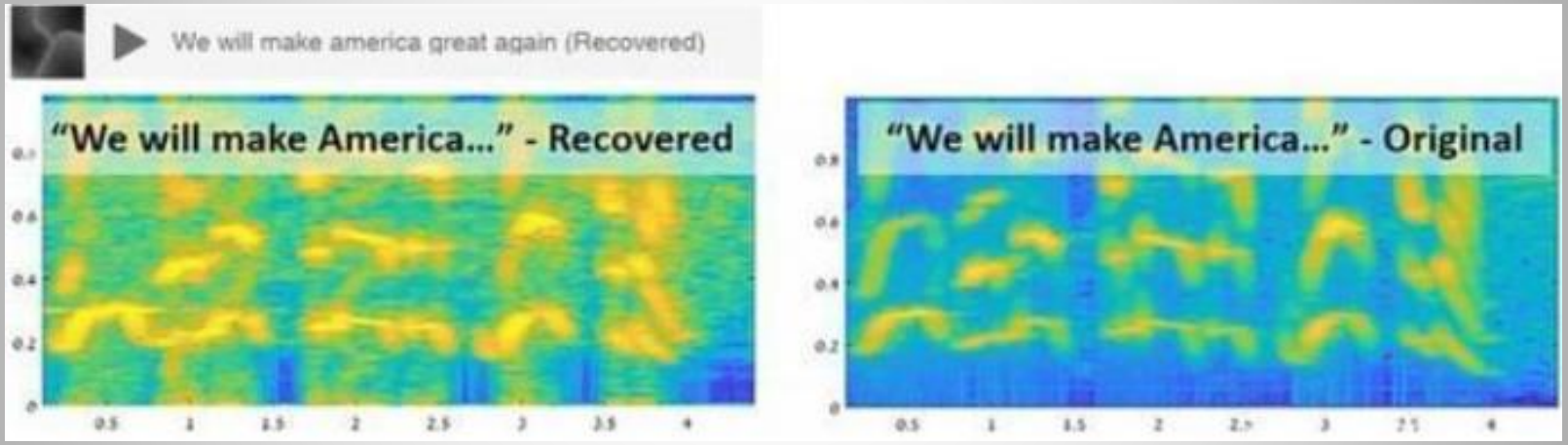
侧信道攻击

- 侧信道（side-channel）攻击也称旁路攻击
  - 基于事件引发的外部效果来加以推测的攻击方式

邮箱溢出反应出什么信息?

计算机技术中的测信道一般指的是基于事件引发的功耗、电磁、时间等物理特性的攻击

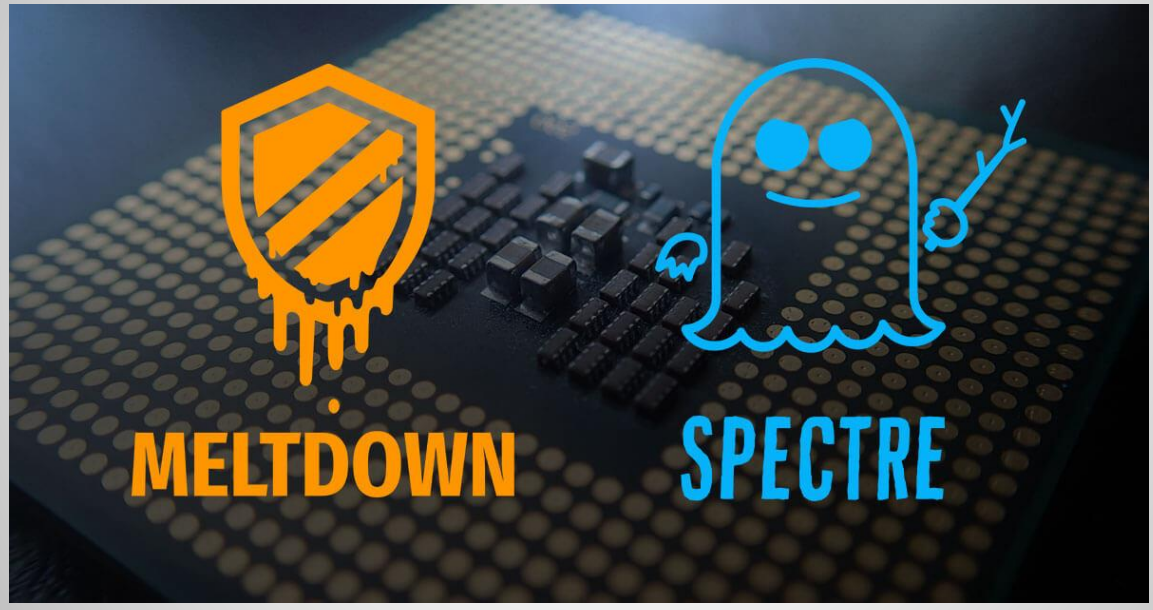
计算机技术中的测信道一般指的是基于事件引发的功耗、电磁、时间等物理特性的攻击



Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations, 2020

熔断和幽灵（2018年）

- 即便经典稳固的系统机制，也可能隐藏风险



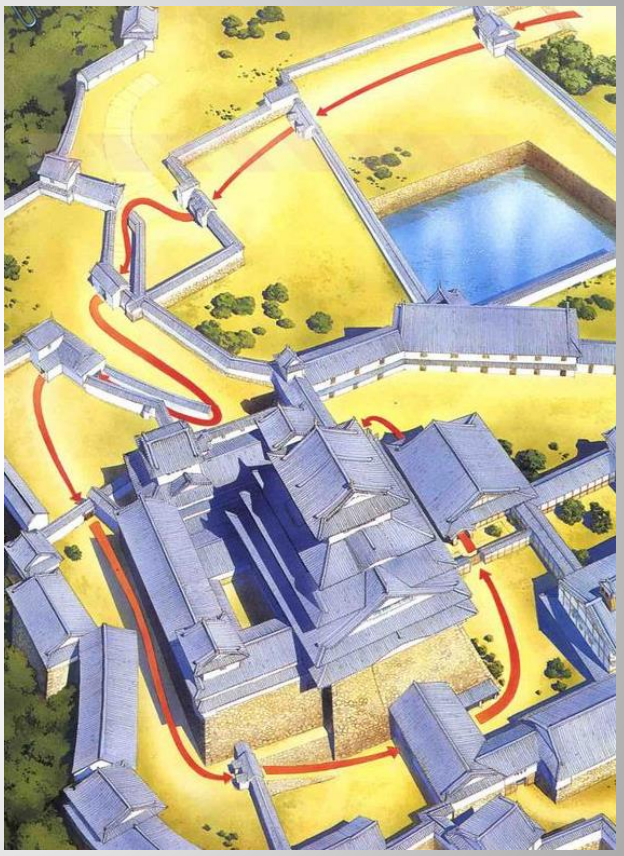
熔断：破坏了用户和操作系统间的隔离
幽灵：破坏了不同用户应用间的隔离性

存在许多问题和挑战

- 什么样的指标来衡量 Metrics?
- 是否有仿真环境 Simulators?
- 合适的测试环境 Testbeds?
- 测试集和工作负载 Benchmark/Workloads?
- 有相关轨迹数据吗 Traces?
- 对每类攻击都要重复思考上述问题Consider the above for each class of side-channels…

应考虑后退防守态势

- Need fallback positions (**defense-in-depth**)
  - City
  - Castile
  - Keep
  - Inner keep



从技术角度出发的努力：可信计算

A *trustworthy* computer is one that is designed to be dependable and to provide security properties, to do what it is supposed to do and nothing else that may harm itself or others

Trusted* vs *Trustworthy

网络空间安全的 CIA 原则

机密性
（Confidentiality）

完整性
（Integrity）

可用性
（Availability）

Course Outline

案例总览

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 谈计算机安全：日益严峻
2. 黑客伦理观察
3. 谈隐私的价值
4. 隐私问题观察

你认为黑客行为的正当性和不正当性有哪些?

黑客伦理

- 侵入计算机或编写恶意软件的黑客，会用一些（比简单盗窃/报复）更堂而皇之的理由为其行为辩解。

- **其中大多数人从未想要沿街行走，挨家挨户敲门以发现一个未锁牢的住户，然后进去搜寻一番**
- **但就是这批人，却会利用有关程序反复尝试，猜测部署于他们的账户密码，入侵系统阅览文件**

1. “无害攻击” 理由站得住脚吗?

许多情况下，激励黑客入侵计算机系统的原因是其带来的挑战和兴奋。有些黑客声称，若他们不拷贝数据也不修改文件，该入侵行为就是无害的。事实果真如此吗?

1）系统安全确认等方面的维护代价。
2）其它造成的计算机运行性能下降。
3）因网络入侵带来的公众形象问题。

2. “一切为了学习” 理由站得住脚吗?

学习型黑客：他们自称所作所为没有任何伤害，仅仅是为了弄明白计算机运作机制，并练习编写复杂程序。

1）上述观点首先和“无害攻击”论有相同之处。

2）编写破坏性程序和进入他人计算机与计算机学习几乎没有什么关系。正确的方法是掌握有关知识和技巧。

3）重要的是，如此“学习”计算机系统知识的人，是难以领会整个系统运行机制的，也无法预测其行为后果。

3. “表面侵入，实则贡献”理由站得住脚吗?

有一种普遍观点是，侵入系统的人通过暴露系统安全漏洞而服务于大家，因此，这些人应该受到鼓励，甚至得到奖赏。这种观点是正确的吗?

1） 上述观点假定存在强制性的因素迫使用户安装安全装置。而计算机的首要目的是工具性，而不是安全操练。

2）上述观点忽视了组织计算机用户升级或者纠正其软件错误带来的技术和经济因素，并不是所有用户有能力。

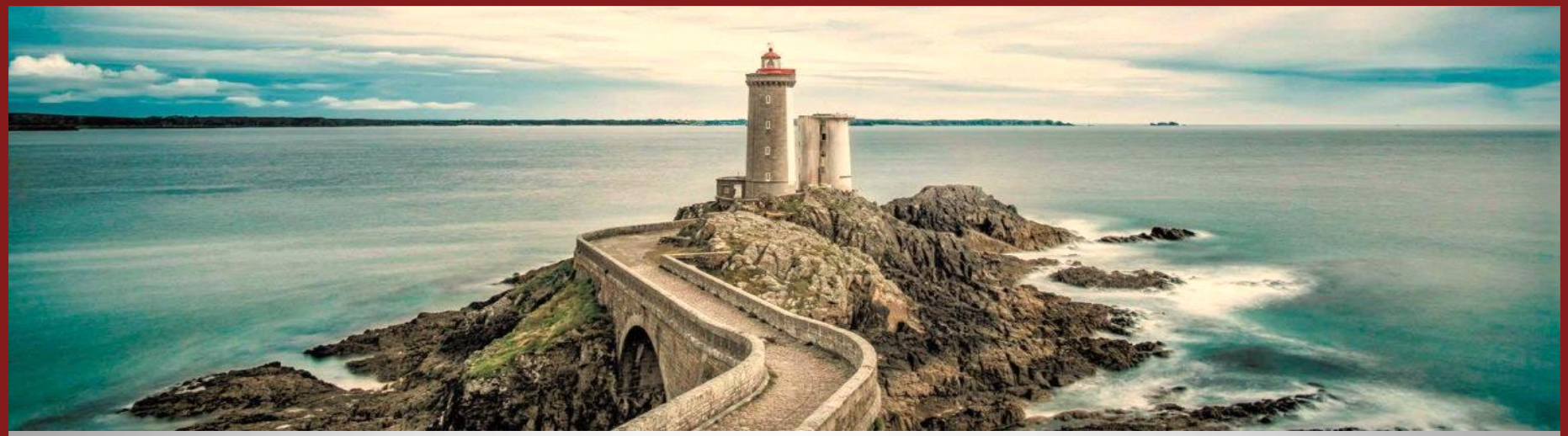
4. “社会监管者” 理由站得住脚吗?

在欧美另有一些观点是，黑客入侵系统是为了监控数据的滥用，有助于避开政府和公司对个人权力的侵犯

1）不可否认，存在数据滥用问题。但入侵系统是否可以改善这些问题，是非常不清晰的

2）我们无法知道，这些黑客是否是我们想要的“保护”我们的人，以及他们的真实目的

3）有关入侵反而促进了各类法律法规的出台，实际上造成了政府和公司权力的进一步加强



Course Outline

案例总览

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 谈计算机安全：日益严峻
2. 黑客伦理观察：严肃对待
3. 谈隐私的价值
4. 隐私问题观察

全国人大常委会法工委：个人信息保护法草案即将亮相

2020年10月12日 10:57:32

来源：新华视点

123人参与 3评论

全国人大常委会法工委发言人臧铁伟在12日举行的记者会上介绍，十三届全国人大常委会第二十二次会议将于10月13日至17日在北京举行。个人信息保护法草案将提请本次会议审议。随着信息化与经济社会持续深入融合，个人信息的收集、使用更为广泛。虽然近年来我国个人信息保护力度不断加大，但在现实生活中，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。为及时回应广大人民群众的呼声和期待，制定个人信息保护法，将进一步明确个人信息处理活动应遵循的原则，完善个人信息处理规则，保障个人在个人信息处理活动中的各项权利，强化个人信息处理者的义务，明确个人信息保护的监管职责，并设置严格的法律责任。个人信息保护法的制定，将进一步增强法律规范的系统性、针对性和可操作性，在个人信息保护方面形成更加完备的制度、提供更加有力的法律保障。

导言

什么是隐私

- “隐私”这个词有是用来指称一种状态，在这种状态中，人们受到免遭自然的或身体的侵犯或观察的保护。

对于他人而言，一个人或一个集体处于一种规范性的隐私状态，当且仅当在这个状态中，这个人或这个集体能够受到免遭他人侵犯、干扰和信息访问的规范性的保护

Cluver et al. 1994

人物 · 观点

朱迪斯·汤姆森【美】(1929 -2020)
-美国哲学家、伦理学家

> 首先确定该行为是否违反了任何其他权利，如果没有的话，那么应该确定它是否针对违反了任何权力

汤姆森建议处理隐私权侵权行为时，采用上述启发式观点

逐渐发展的隐私观念

- “**不侵入**” （美国宪法第四次修正案）
- “**不可侵犯的人格**” （大法官布兰代斯，1890年）
- “**不干涉**” （赋予妇女选择人流的权力的判例）
- “**有限制的信息访问**” （1974年隐私法）

逐渐发展的隐私观念

- **隐私控制观**
  - 1984年，美国法学家Charles Fried写道：隐私并不只是指他人不知道关于我们的信息，相反，它是指我们能够控制关于我们自己的信息。

- **限制访问观**
  - 1990年，美国计算机伦理学家James Moor提出，在高度计算机化的时代，控制关于我们自己的信息犹如天方夜谭，限制访问才更实际。

思考

你有没有思考过，隐私的价值/意义是什么?

人物 · 观点

詹姆斯·瑞切尔斯【美】(1941 -2003)
-美国著名道德哲学家

> 隐私具有价值，因为它能使我们与他人形成各色的人际关系

瑞切尔斯在探索隐私内在价值上做了较为深入尝试

人物 · 观点

黛博拉·约翰逊 (D. Johnson)【美】

- 1985出版第一部计算机伦理教科书

> **应当把隐私看作自主的一个内在方面**

约翰逊认为没有隐私的话，自主是不可思议的

关于隐私的价值的思考

关于隐私的一些观点

- 为我们提供免受伤害的保护（工具善）
- 促成各式各样的人际关系（不简单的工具善）
- 个人自主性的必要条件（接近于内在善）

- **隐私仿佛具有特殊的价值**
  - 一方面它似乎是需要捍卫的，至关重要的东西
  - 另一方面，它似乎只是个人偏好或与文化相关

信息时代隐私问题简述

- 如今，以破坏电脑软硬件为目标的病毒攻击逐渐减少，盗窃数据和窥探隐私的攻击日益增多。

若干风险来源

1. 我们在网络空间中的所有事情都会被（至少短暂的）记录下来，并进行关联。
2. 放在公共场合的数据对所有人都是公开的，而且任何人在任何时候访问都很容易
3. 与个人相关的信息数量激增且数据检索工具日益强大，识别个人身份不再困难
4. 一旦敏感信息发布在互联网上，想把它从流通中彻底删除是几乎难以完成的任务
5. 软件日益复杂，系统漏洞难以避免，即便公司和组织也无法掌握其拥有的所有数据去向

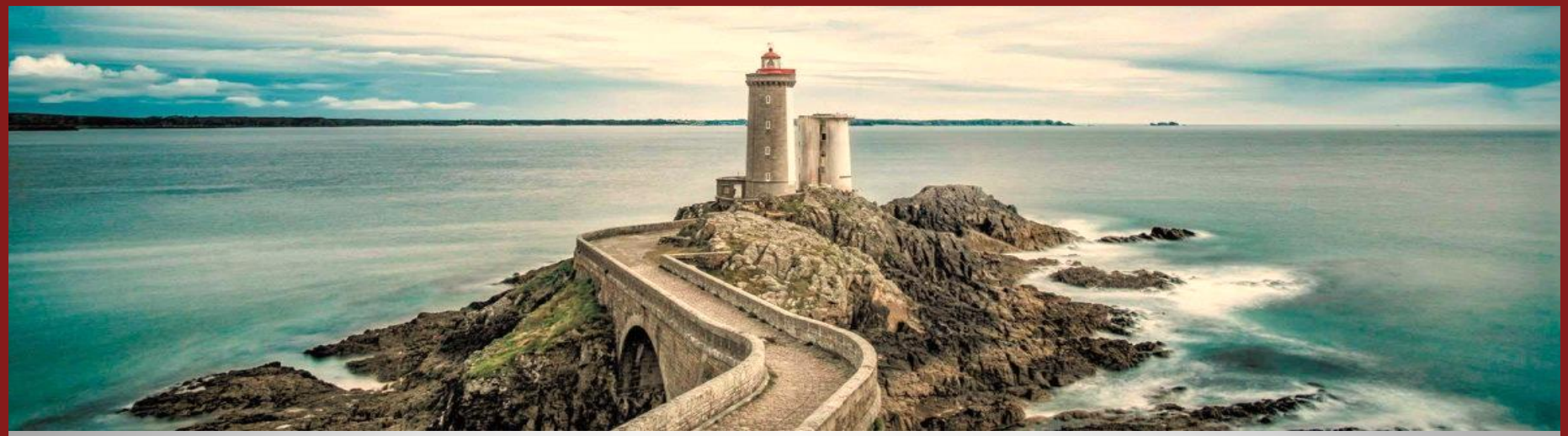
人物 · 观点

詹姆斯·摩尔 (J. Moor)【美】

- 1985年给出CE最具影响力的宽泛定义

> 在日益计算机化的文化中，作为安全的表达，隐私就是我们价值系统中一个至关重要的纽带。

摩尔认为，在一个人口密集、高度计算机化的社会中，隐私是安全这一核心价值的内在表达，是内在价值的合适候选者。



Course Outline

案例总览

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 谈计算机安全：日益严峻
2. 黑客伦理观察：严肃对待
3. 谈隐私的价值：特殊价值
4. 隐私问题观察

隐私问题：无处不在的监听

- **普适计算** Ubiquitous computing makes issues of privacy more readily apparent to users

正方	反方
	
必要的监控工具	谁来防止技术滥用

隐私问题：无处不在的监听

《爱国者法案》

(USA Patriot Act of 2001)

美国911事件后不久出台的法律，给予了美国政府前所未有的权利来向任何总部在美国的公司（不管公司数据中心位于哪里）提出数据请求。

隐私问题：无处不在的监听

2013年斯诺登事件

一份文档揭示NSA从Verizon、Facebook、谷歌、微软等多家公司提取大量数据。事实上Verizon的电话通讯元数据等都不在公有云中。其它大公司也有自己的私有云。

是否允许第三方从云服务提供商处拿走数据?

反方观点

不能让云服务商代替自己存储数据，否则会把数据暴露于风险之中

正方观点

不管数据在不在云中，政府都能向任何公司提出数据请求

云计算服务中的强制要求

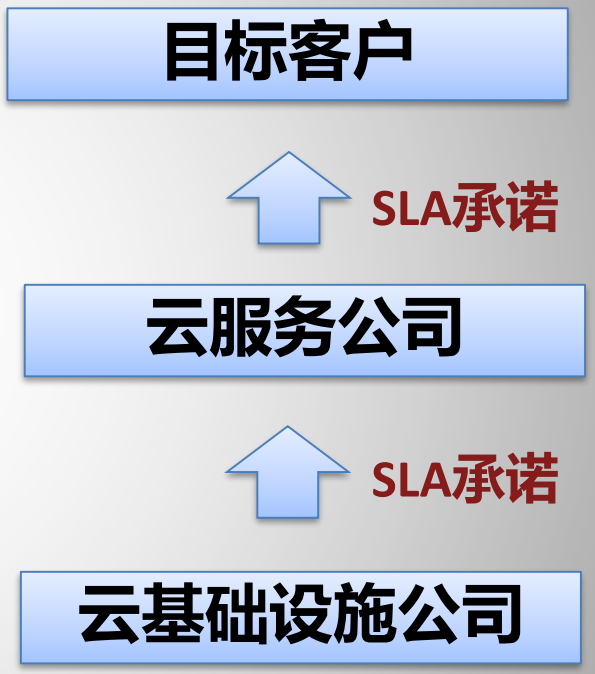
- **服务等级协议（Service-Level Agreement)**
  - 云服务提供商与云服务消费者间的一份协议
  - 协议设定了承诺提供的云服务等级的期望值

- 常见服务等级协议内容：
  - 页面加载时间
  - 事务处理时间
  - 事件解决时间
  - 安全隐私保障
  - 突发事件响应计划
  - 数据所有权申明
  - 标准，价格，责任等

云计算服务中的强制要求

- 云的SLA可能会非常复杂，尤其在牵涉到多个云服务提供商的情况下。

- **许多客户特征会影响到SLA**
  - 消费者对比企业客户
  - 付费用户对比非付费用户
  - 受监管行业对比不受监管行业
  - 匿名对比身份认证



隐私问题：个人数据滥用问题

塔吉特的“读心术”

怎么看社交媒体对你的绘像?


人民日报评大数据滥用:不欢迎"读心术"更不想成"透明人"

人民日报

发布时间：18-03-26 10:00 人民日报社

“people willingly surrender data all the time… because they receive something of value in return” --- **Michael Stonebraker**

讨论

匿名就够吗？数据加密就够吗？

Twitter明文存储用户登录密码！泄密几时休?

2018-05-08 14:22

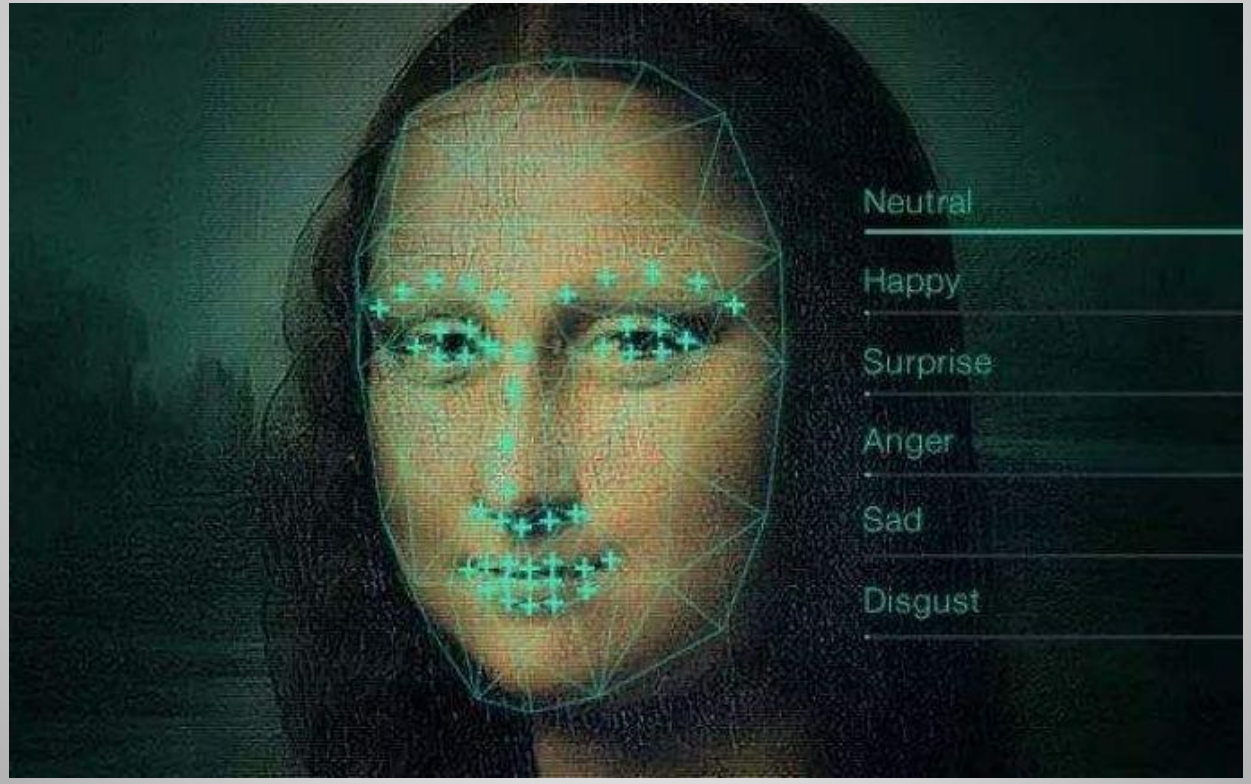
谷歌发现了G Suite漏洞：部分密码明文存储长达十四年

2019-05-23 11:37

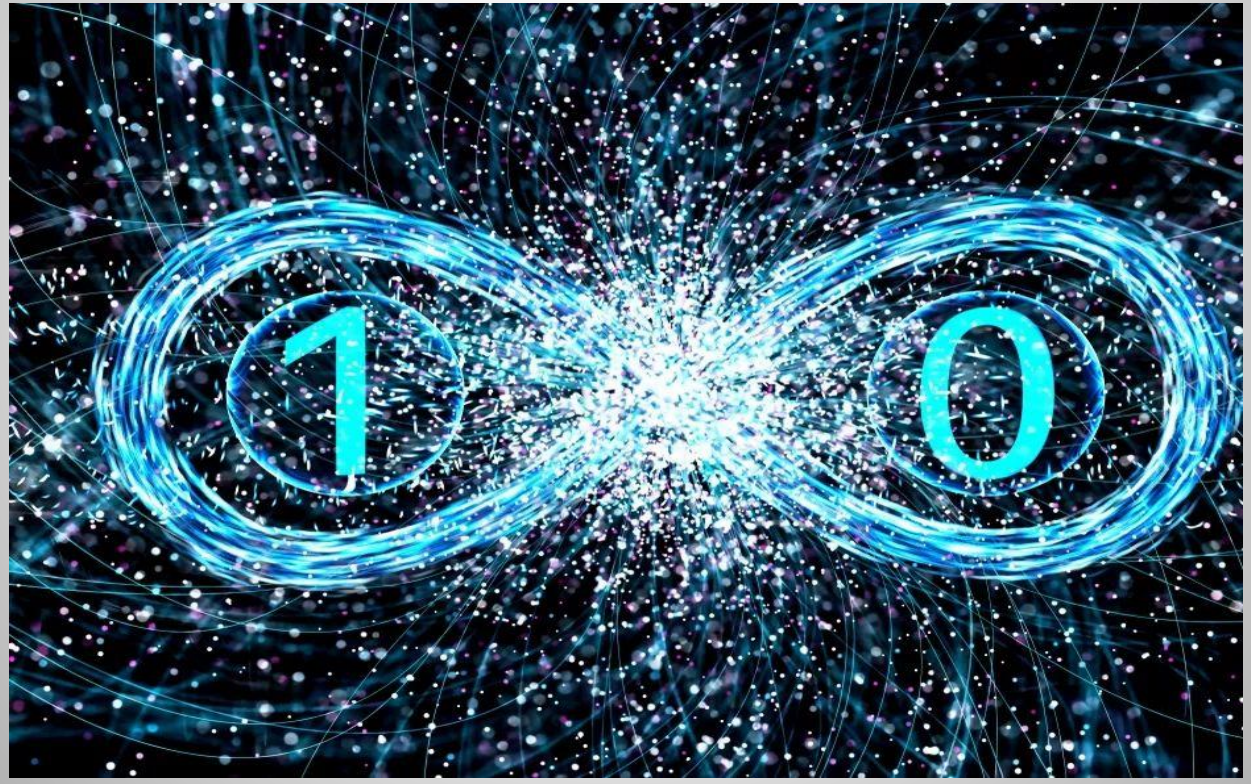
谷歌街景和隐私保护

数字现金的匿名问题

反人脸识别的伦理问题



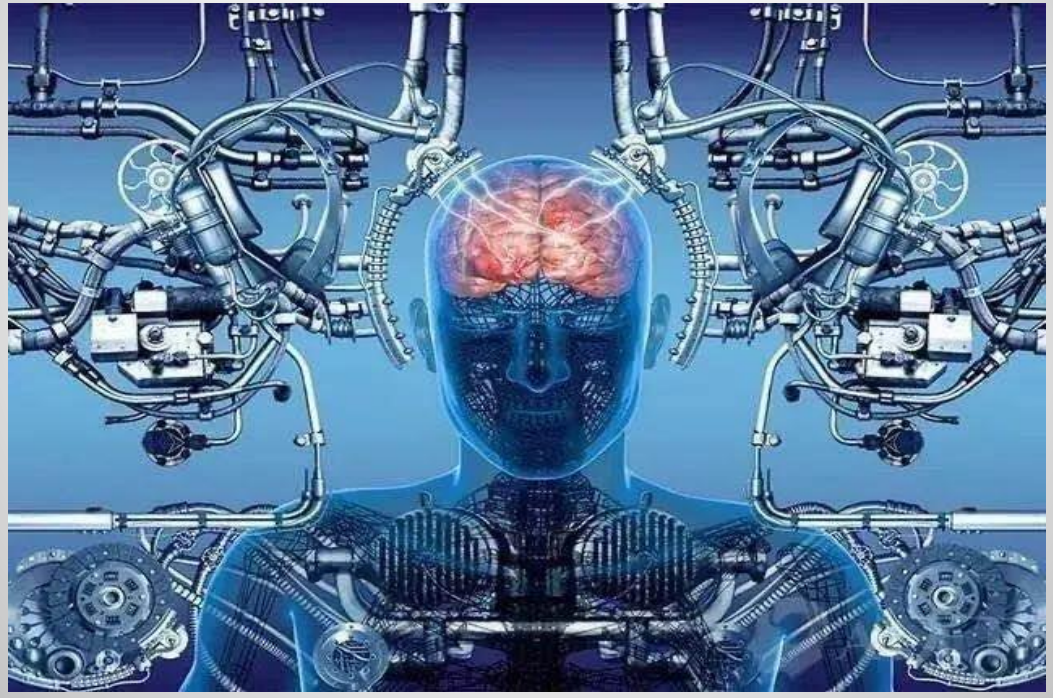
量子计算对密码保护的影响?



案例：人人都是“透明人”

什么是应该/不应该捕捉的信息

如果未来人机融合，计算机安全漏洞可能面临那些难以接受的后果?



从规则角度出发的努力

制定和修正隐私状态的原则

公开原则： 有关隐私状态的规定和条件应当明确，并且为受其影响的人所知晓。

- 公开原则提倡知情同意以及理性决策
- 更好的信息公开=>更好的隐私保护

Course Outline

案例总览

- 4.6 产权利益
- 4.5 真实可信
- 4.4 公平公正
- 4.3 隐私保护
- 4.2 自由尊重
- 4.1 健康安全

1. 谈计算机安全：日益严峻
2. 黑客伦理观察：严肃对待
3. 谈隐私的价值：特殊价值
4. 隐私问题观察：全面审视