
# 软件与系统安全（NIS7021）

李卷孺 博士 网络空间安全学院

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY


# 第一周：Thinking in Security

软件与系统安全

2020年9月9日

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

# 目录 Contents

# 目录 Contents

# 课程信息

- 网站：https://security.gossip.team/nis7021
- 课程主讲：李卷孺 博士
  - https://lijuanru.com
- 课程助教：G.O.S.S.I.P 成员
  - https://security.gossip.team
- 课程时间：秋季学期 1-16周
  - 每周三晚6点-8点20
  - 地点：陈瑞球楼 202

# 课程内容与要求

- **课程内容：软件与系统安全的基础概念和前沿研究**
  - 代码逆向工程
  - 内存安全问题
  - 系统安全防护
  - 网络（network & web）安全
  - 移动终端（Android & iOS）安全
  - 嵌入式系统与IoT安全
  - 现实世界中的密码软件安全
- **实验内容：7次实验**
  - 软件逆向、系统攻防、安全防护、web渗透测试、移动安全分析、IoT安全分析、密码系统分析

# 课程先修知识

- **前序课程**
  - 操作系统、计算机系统结构、计算机网络、编译原理
- **程序语言**
  - 系统编程语言（C/C++）
  - 快速开发语言（Python、Shell等）
- **软硬件环境**
  - Virtualbox 虚拟化环境
  - Windows/Linux/macOS 开发调试环境
  - 一个优秀的文本编辑器！！！
  - VPS 环境 one.gossip.team
  - （可选）：Android、iOS和IoT开发调试环境

# 考核方法

- **成绩评定**
  - 成绩分为出勤分（5 points）、实验分（70 points）和期末测试分（25 points）
- **出勤分**
  - 不点名，在整个课程期间内进行一次5分钟的技术分享即可
- **实验分**
  - 三部分内容：基础实验（25 points）、实验报告（35 points）、新成果扩展（10 points）
  - 实验报告需要使用在线latex完成 https://latex.sjtu.edu.cn
- **期末测试分**
  - Happy CTF

# 课程目标与原则

- **培养目标**
  - 面向**学术界**：培养良好的安全学术品味和学术研究能力（发现问题、解决问题、清晰表达）
  - 面向**工业界**：培养安全分析师的必备基础能力（安全设计原则、逆向分析、漏洞防御）
- **学习原则**
  - 掌握清晰的安全模型，针对**具体问题**的**实际分析**！！！
  - 充分了解前沿知识和技术（state-of-the-art）
  - 研究结论：少些，但要成熟
- **诚信原则**
  - 遵守学术道德规范，保证原创性，鼓励合作!

# 像攻击者一样思考！

- **站在攻击者（而不是设计者）的角度思考**
  - 当软件系统遇到非预期的行为，会发生什么问题?
  - 学习大量已有的攻击案例，会帮助你找到灵感
- **对系统的深刻理解，有助于发现问题**
  - 逆向分析能力来自于正向开发
- **基本要求**
  - 知道哪些地方可能发生问题
  - What goes wrong?

**After taking this class:** You might not know all answers, but you should know the questions!

# 推荐阅读

- 图书流动计划
  - 《 C和C++安全编码》(https://book.douban.com/subject/4136222/)
  - 《程序员的自我修养》(https://book.douban.com/subject/3652388/)
  - 《密码学实践》(https://book.douban.com/subject/1434818/)

- 选读
  - 《编程珠玑(第二版)》(https://book.douban.com/subject/1230206/)
  - 《虚拟机》(https://book.douban.com/subject/3611865/)
  - 《Serious Cryptography》(https://book.douban.com/subject/28549892/)

# 参考资料

- **论文**
  - 计算机安全学术会议
  - https://feysh.com/ranking/
- **在线课程和文档**
  - 国外著名大学的安全课程
  - Using Google！！！
- **线下交流**
  - E.g., 参与具体的科研项目

**G.O.S.S.I.P 安全学术会议排行榜（2019版）**

| Conference | Score |
|---|---|
| 1. ACM CCS | 1.0 |
| 2. IEEE S&P | 0.715 |
| 3. Usenix Sec | 0.561 |
| 4. NDSS | 0.500 |
| 5. PETS | 0.356 |
| 6. ACM AsiaCCS | 0.343 |
| 7. ACSAC | 0.297 |
| 8. ESORICS | 0.284 |
| 9. EuroS&P | 0.201 |
| 10. ICICS | 0.194 |
| 11. RAID | 0.173 |
| 12. DSN | 0.169 |
| 13. ACM WiSec | 0.151 |
| 14. DIMVA | 0.148 |
| 15. ACNS | 0.123 |
| 16. ISC | 0.115 |
| 17. ACM-CODASPY | 0.108 |
| 18. ACM-SACMAT | 0.078 |

# 参考课程

- MIT 6.858
  - http://css.csail.mit.edu/6.858/2020/
  - 非常硬核的system security课程!
- Stanford CS155
  - https://cs155.stanford.edu/
  - 大名鼎鼎的Dan Boneh主讲，网络安全和密码学课程
- OSU 系统安全与软件安全
  - http://web.cse.ohio-state.edu/~lin.3021/spring2012.html
  - http://web.cse.ohio-state.edu/~lin.3021/fall2013b.html

**Staff**

| Lecturers | | |
|---|---|---|
| **Name** | **E-Mail** | **Office** |
| Frans Kaashoek | kaashoek@mit.edu | 32-G992 |
| Nickolai Zeldovich | nickolai@csail.mit.edu | 32-G994 |

# 目录 Contents

# Security 基本原则

- 关注的是如何规范不同类型的操作行为
  - 例：NIS7021 课程管理系统
    - 教师：发布课程、安排测试、评定成绩
    - 助教：答疑、登记信息
    - 学生：查看课程、上传作业、参与测试
  - 系统控制不同角色的权限
- 安全风险（Security Risks）
  - 如果学生可以执行老师或者助教的行为？
    - 篡改成绩、删除其它同学信息
  - 根源
    - 系统控制逻辑不完备

# Security 基本原则

- 关注的是如何规范不同类型的操作行为
  - 例：NIS7021 课程管理系统
    - 教师：发布课程、安排测试、评定成绩
    - 助教：答疑、登记信息
    - 学生：查看课程、上传作业、参与测试
  - 系统控制不同角色的权限
- 安全风险（Security Risks）
  - 如果学生可以执行老师或者助教的行为？
    - 篡改成绩、删除其它同学信息
  - 根源
    - 系统控制逻辑不完备

# Security 基本要求

- 设计防御措施，减少（注意，不是杜绝！）安全风险
  - 安全防御由安全风险而定

- 经典的安全设计步骤：
  - 提出安全目标（Security Goal）
  - 建立安全策略（Security Policy）
  - 设计安全机制（Security mechanism）

# Security 基本要求

- 设计防御措施，减少（注意，不是杜绝！）安全风险
  - 安全防御由安全风险而定

- 经典的安全设计步骤：
  - 提出安全目标（Security Goal）
  - 建立安全策略（Security Policy）
  - 设计安全机制（Security mechanism）

# 让我们更生动一些

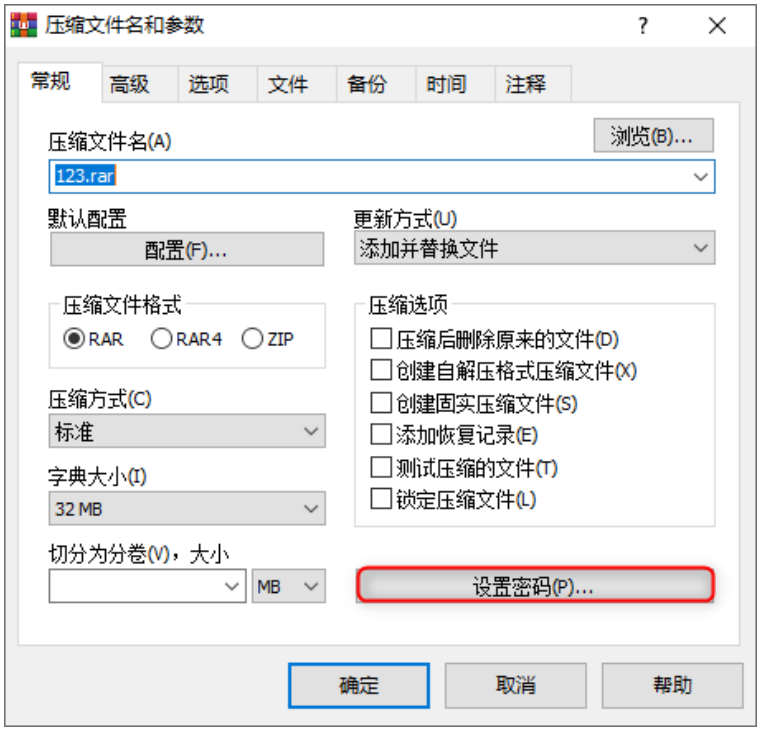
- 通过关于安全的问题与答案来学习

# Security vs Safety

- 此“安全”非彼“安全”


# 安全事件：加密RAR文件破解

- “我的rar文件密码忘记了，有没有快速破解恢复rar密码的办法，这份文件对我来说非常的重要”



# 安全事件：软件注册与软件破解

- 目前成熟的密码学算法可以保护软件不可破解？

第 25 卷第 9 期
2005 年 9 月

计算机应用
Computer Applications

Vol. 25 No. 9
Sept. 2005

文章编号:1001 - 9081(2005)09 - 2080 - 03

## 基于 RSA 算法的注册码软件加密保护

黄　俊,许　娟,左洪福
(南京航空航天大学 民航学院, 江苏 南京 210016)
(hj990411@126.com)

**摘　要**:提出了在注册码软件加密保护基础上的一套完整软件保护方案,方案中采用了"一机一码"制,运用密码学中成熟的非对称算法 RSA(Rivest Shamir Adelman)进行加密处理,并且以数据库的形式进行密钥管理,通过这一系列手段更好地防止了非法注册码的传播和非法注册机的制作。最后在基于VC++ 6.0 的开发平台上实现了该软件保护方案。

**关键词**:软件保护;注册码;RSA 算法;密钥管理
**中图分类号**: TP309.7　　**文献标识码**:A

# 安全名词：数据安全 vs 逻辑安全

- 数据安全
  - 依赖一小段保密的信息（密钥）保证很长一段信息的机密性
  - 关注的是数据信息的保密性
- 逻辑安全
  - 用代码来“定义”一段逻辑
  - 代码运行在CPU上，可被观察、修改
  - 关注的是逻辑的完整性

- Crypto is not the cause of these vulnerabilities, and could not solve/prevent these vulnerabilities
  - Protocol, implementation errors (e.g., WEP in WiFi)
  - Programming errors (buffer overflow)
  - Distribution errors (trojan)
- Bruce Schneier: “Currently encryption is the strongest link we have. Everything else is worse: software, networks, people. There's absolutely no value in taking the strongest link and making it even stronger”

# 安全事件：支付宝变身老赖?

保险

**余额宝遭窃，已购买账户保险，但支付宝耍赖不赔钱，我该怎么办?**

# 安全事件：支付宝变身老赖?

支付宝

谢邀。

**利益相关**：利益相关

还有种情况，家里的熊孩子记住了父母的支付密码，设法拿到了手机，进行了操作。家长一看，账户被盗了。问熊孩子，熊孩子也不认。家长就坚持说是被盗。报警后警方进行调查，发现是自家孩子的操作。这就比较尴尬了……

# 安全名词：Threat model

- 科学准确评估攻击者和防御者的能力边界
  - 为什么存在威胁?
  - 攻击者来自何处?
  - 攻击者拥有什么样的能力?
  - 防御者需要保护的对象?
  - 防御者拥有什么样的能力?
  - 防御者受到什么样的约束?

# 安全事件：黑客如何攻击Pony

- “终于在第七天早上，2006年8月7日，他成功攻破了腾讯后台的几十个系统，顺便还盗走了马化腾的五位数QQ账号”

# 安全名词：Attack Surface

- 系统暴露了哪些攻击者可以利用的输入输出接口
  - 远程输入输出：网络数据
  - 无线输入输出：红外、蓝牙、可见光、声音、电磁辐射
  - 本地输入输出：鼠标、键盘、打印机、显示器
- 系统的哪些功能/资源可能受到影响
  - 敏感信息：泄密、泄露、被篡改
  - 系统功能：异常、停止服务
  - 身份认证：未授权访问
  - 访问控制：提权

# 安全事件：芯片木马

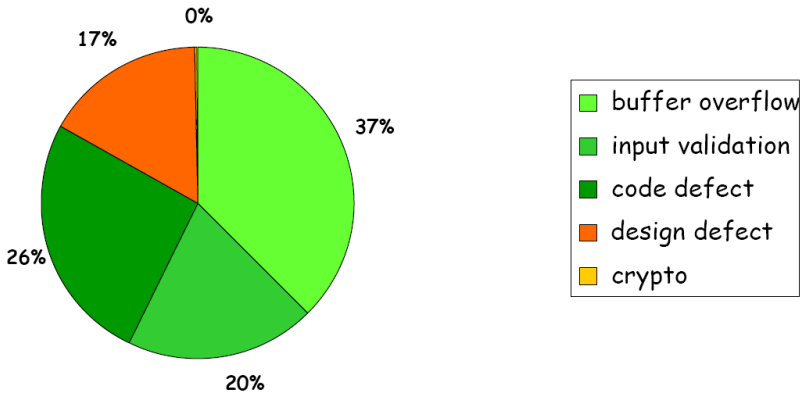
- Bloomberg：“中国用一个米粒大小的芯片，入侵了美国 30 多家公司”

# 安全事件：芯片木马

- Bloomberg：“中国用一个米粒大小的芯片，入侵了美国 30 多家公司”


# 安全名词：软件缺陷与漏洞

- Flaw
  - 设计层面的软件缺陷
- Bug
  - 实现层面的软件缺陷
- Vulnerability
  - 当软件问题可被用于执行非预期行为时，就称为漏洞
- Exploit
  - 利用漏洞完成攻击的行为

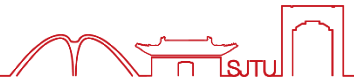



Security bugs found in Microsoft bug fix month (2002)

# 安全事件：2020抗疫

- 检疫隔离，击败新冠传播

# 安全名词：Access Control




- Isolation
  - 将系统划分为不同的区域（domain）
  - 可能是逻辑安全中最重要的机制
- Authentication
  - 用户是谁?
- Authorization
  - 用户可以访问哪些资源?

# 安全问题：三大IT巨头的失败

- 《震惊！美国一名IT杂志编辑的Gmail、Apple ID、Amazon账户竟被轻易攻破》

Meet Mat Honan. He just had his digital life dissolved by hackers.
PHOTO: ARIEL ZAMBELICH/WIRED. ILLUSTRATION: ROSS PATTON/WIRED

# 安全名词：Usability

- How Apple and Amazon Security Flaws Led to My Epic Hacking
  - https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- 攻击步骤
  - 攻击者试图重设Gmail密码，发现备用邮箱是Apple邮箱
  - 攻击者试图重设Apple密码，提示需要账单地址和信用卡号后4位
  - **攻击者联系Amazon客服，要求给受害账户增加一张信用卡**
  - 再次联系Amazon，重设邮箱地址，继而重设账户密码
  - 登陆Amazon账户，观察历史支付中的信用卡信息（只能看到后四位！）
  - 重设Apple密码，继而重设Gmail密码!

# 安全事件：神秘的百慕大三角


# 安全名词：Secrets

- 秘密：安全的基本要素
  - 密钥（crypto keys）
  - 令牌（token）
  - 指纹（fingerprints）

- 问题：哪些因素不应该保密？

- 穷搜索攻击 vs 信息论
  - Perfect Secrecy
  - Computational complexity

# 安全事件：DigiNotar

- 2011年8月，荷兰CA供应商DigiNotar的服务器被发现遭黑客入侵，疑似伊朗黑客在7月中旬入侵了DigiNotar服务器，签发531个伪造证书，包括Google、微软、雅虎、Twitter、Facebook、中情局、军情六处和摩萨德等；DigiNotar在7月19日发现了入侵，但直到8月份外界才知道入侵事件。DigiNotar因此次攻击而破产

DigiNotar
Internet Trust Services

# 安全名词：Trust

- 不可信原则
  - 在没有进行认证之前，一切对象和外部输入都不得信任
- 信任根
  - 一生二，二生三，三生万物
- 信任链
  - 如何证明我是我？

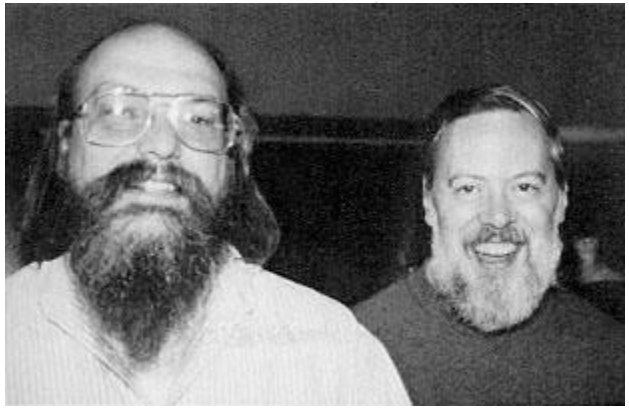
- 问题：两个陌生人初次见面，如何认证（authenticate）对方

# 安全事件：Ken的编译器后门

*TURING AWARD LECTURE*

## Reflections on Trusting Trust

*To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.*

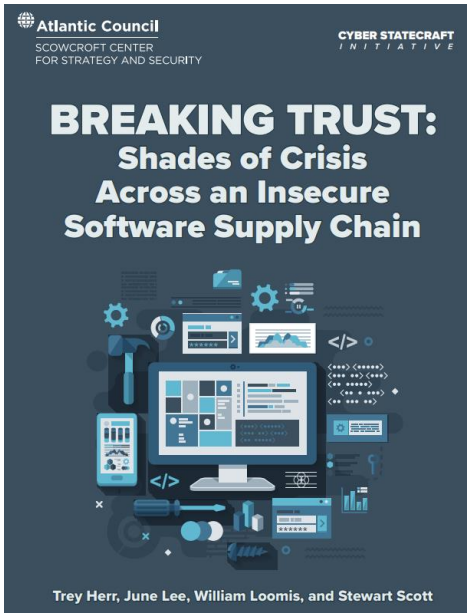


```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

**FIGURE 3.3.**

# 安全名词：供应链安全

- 供应链上的软件和硬件
  - 编译系统
  - 三方库
  - 执行环境
  - Sample code
  - 芯片模组




- BREAKING TRUST
  - https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

# 安全事件：人工智能的诞生

- 给一岁小朋友的人工智能教材

# 安全事件：人工智能的诞生

- 一岁小朋友亲测

# 安全名词：Similarity & Diversity

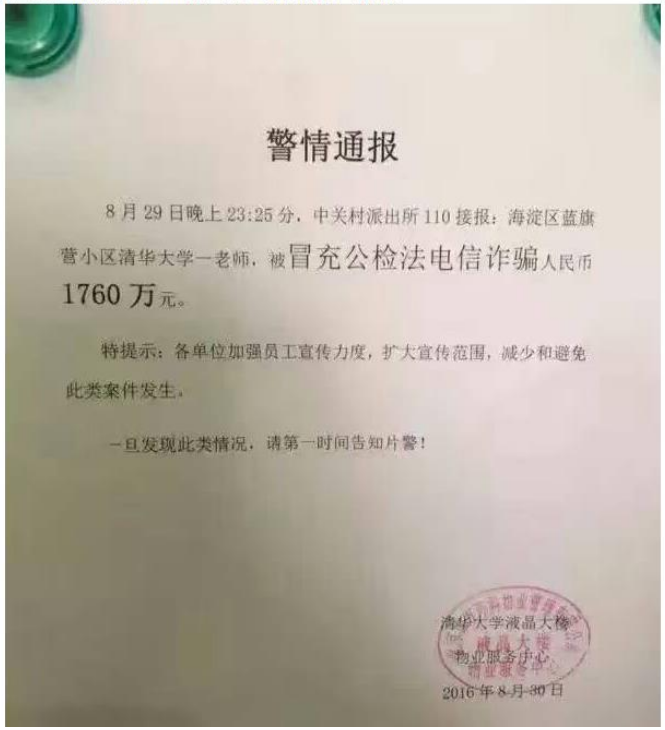
- Anomaly detection
- Differential analysis
- Moving target defense
- Indistinguishability

# 安全问题：电信诈骗谁之过？

- 真的是因为受害者无知或贪婪吗？

**如何看待清华大学教授被骗 1760 万元?**

今日清华大学某教授被骗1760万。关于金额和案情，都有点



警情通报

8 月 29 日晚上 23:25 分，中关村派出所 110 接报：海淀区蓝旗营小区清华大学一老师，被冒充公检法电信诈骗人民币 1760 万元。

特提示：各单位加强员工宣传力度，扩大宣传范围，减少和避免此类案件发生。

一旦发现此类情况，请第一时间告知片警！

清华大学液晶大楼
物业服务中心
2016 年 8 月 30 日

# 安全名词：Privacy

- 为什么隐私关乎安全
  - 数据特征==身份
  - 身份==认证
- 差分隐私技术 Differential Privacy
- 问题：人脸识别是否应该在小区普及？

# 安全事件：俄罗斯vs特斯拉

- 安全不仅包括代码的因素，也包括人的因素

**安全: 俄罗斯人试图贿赂特斯拉雇员安装恶意程序**

WinterIsComing(31822) 发表于2020年08月28日 14时57分 星期五
来自

一名俄罗斯人试图贿赂特斯拉雇员百万美元，目的是将恶意程序安装到公司内网。根据美国媒体和检方的起诉书，被告是 27 岁的俄罗斯公民 Egor Igorevich Kriuchkov，他从俄罗斯旅行到美国内华达州，多次与一名未公布名字的特斯拉内华达工厂雇员碰面，一开始他的出价是 50 万美元，之后提高到一百万美元。特斯拉雇员将此事报告给了公司，之后与 FBI 合作记录了两人会面的细节。Kriuchkov 的目的是将恶意程序安装到特斯拉的内部网络，窃取数据，然后威胁公开数据向特斯拉勒索赎金。安全研究人员认为 Kriuchkov 亲自跑去美国实施阴谋简直疯狂，网络犯罪分子几乎没人会这么做。

阅读更多... | 发表评论

# 安全名词：Human Factors

- 社会工程学 Social Engineering
  - 《欺骗的艺术》凯文·米特尼克
  - （不了解安全原理的）人往往是安全系统中最薄弱的环节

- 内部威胁 Inside Threats
  - 伊朗核电站Stuxnet攻击事件
  - 解决方案
    - 零信任模型
    - 最小访问权限

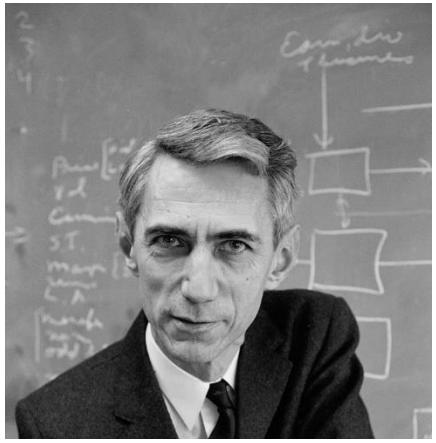
# 安全事件：复杂系统的失败

- 《模仿游戏》： 图灵vs德国Enigma密码机

# 安全名词：公开系统设计

- The Kerckhoffs's Principle
  - *The design of a system should not require secrecy*

- 香农（Claude Shannon）版本
  - *The enemy knows the system*



# 安全名词：K.I.S.S

- “我相信有两种设计软件的方式：一种是使软件足够简单而明显没有缺陷；另一种是使它如此的复杂，以至于没有明显的（可被轻易发现的）缺陷。”

  —— Tony Hoare（英国计算机科学家、图灵奖得主、快速排序算法发明人、哲学家就餐问题的提出者）


* [为什么“简单”如此复杂](http://bird-frank.github.io/2018/11/08/why-simple-is-so-complex)

# 最后一个安全要素：用户

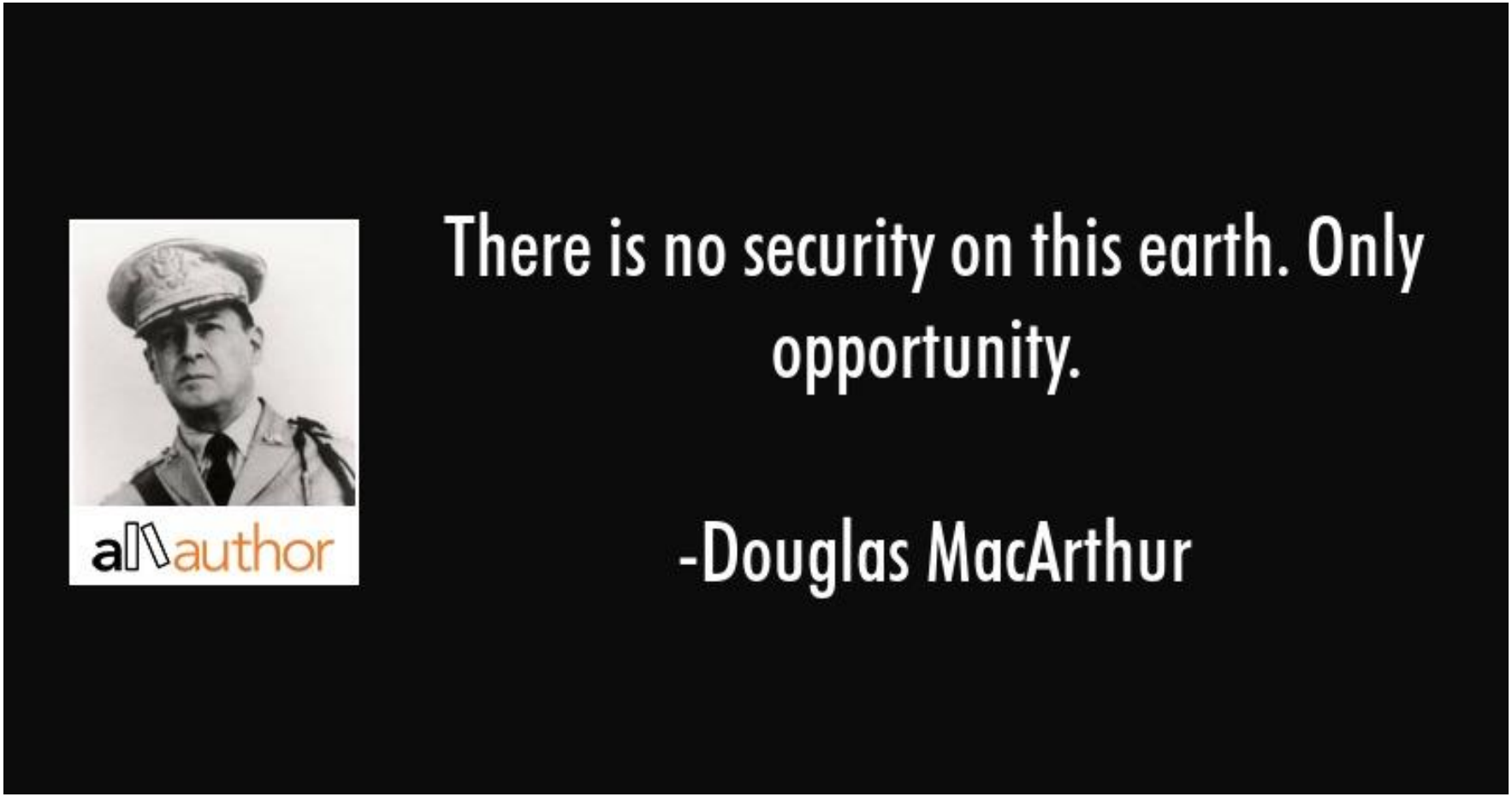
- “不懂网络安全的人是幸福的，而我们的责任就是要守护他们这种幸福。”
  -- 李柏松，安天科技



* https://www.tust.edu.cn/temp/zssc.pdf

# 目录 Contents

# 安全的绝对性?




图片来源：https://allauthor.com/quotes/4297/

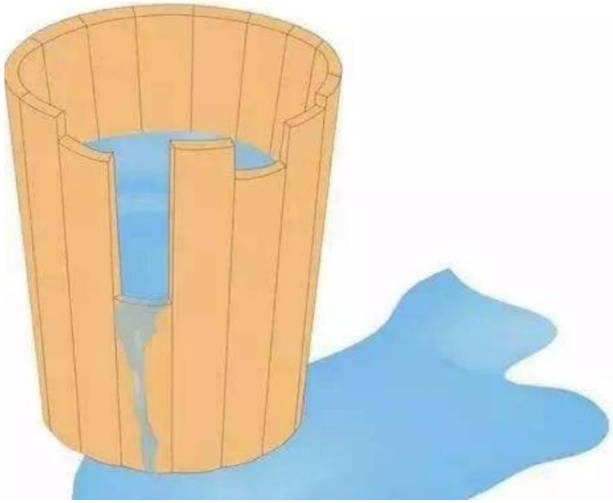
# 安全的绝对性?

- 安全和功能的trade-off
  - 软件功能的正常执行是第一要素
  - Security永远是第二考虑
  - 功能保证>风险控制
- 绝对的安全带来绝对的低效
  - 当安全影响了可用性时，用户往往会破坏安全措施
  - Password
    - 5b2fdd18babc280084a85a891916a810
    - 123456

# 安全的木桶效应

- 一个系统的安全性，取决于其最薄弱环节

- 攻击者总是寻找最容易攻击的点



# 安全实例：地铁安检系统

- 可用性问题
  - 高峰时段的效率和安全
- 安全问题：是否检查了所有路径


# 安全的经济学

- 《三无图书馆》
  - 浙江鄞州高级中学的图书馆堪称“三无”图书馆：无墙、无门、无岗。10万册图书统统躺在完全开放的书架上，在没有任何监控设施的宽松环境里，任由师生自助借阅。


从图书馆到读书馆

□ 邵颖华

《人民日报海外版》（2019年02月22日 第07版）

- 成本分析原则
  - 防御成本 < 攻击成本

- 如何评估攻击成本和防御成本?

# 攻击者代价

- 1980年代：脚本小子
  - 时间成本：0
  - 经济成本：计算机购置费用
- 2000年代：黑产团伙
  - 时间成本：和公司赛跑
  - 经济成本：犯罪成本+雇佣研究人员
- 2020年代：国家级黑客
  - 时间成本：对抗中占据先机
  - 经济成本：不计投入

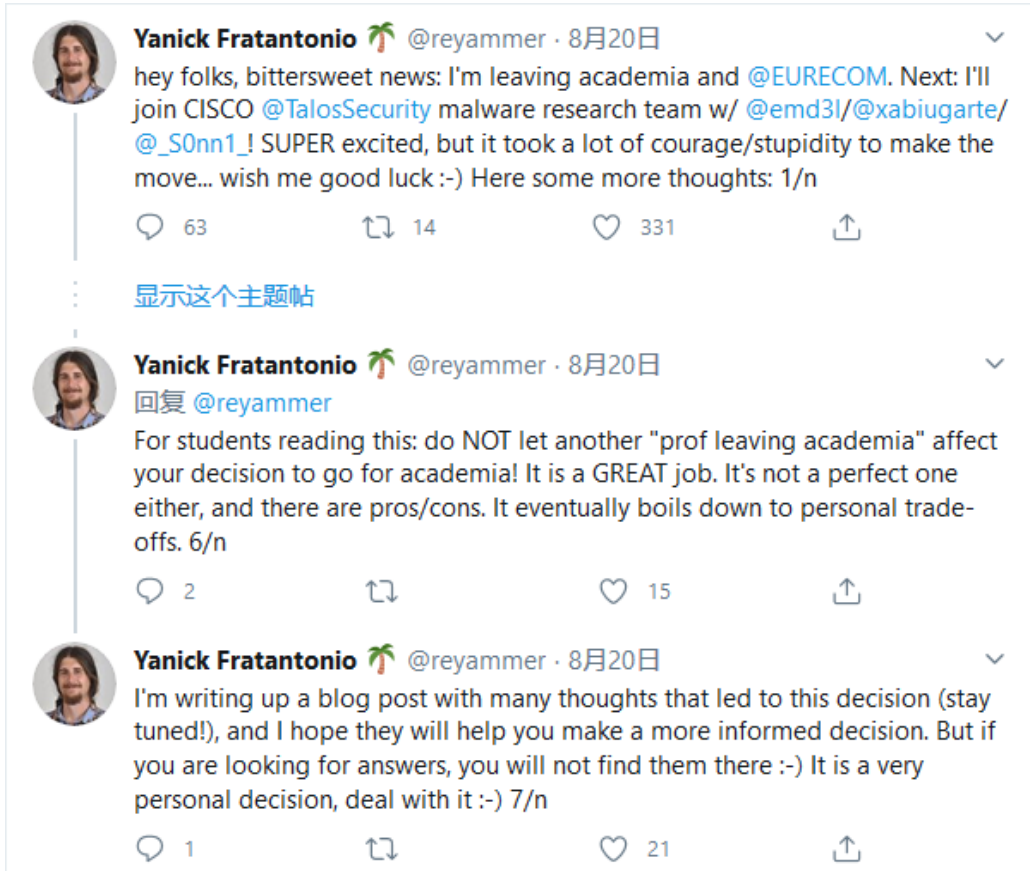
# 防御者代价

- 1980年代：
  - 软件防护：依赖少数安全专家
  - 高昂的计算机和网络费用：阻止普通用户使用
- 2000年代：
  - 软件防护：软件开发人员（non-expert）
  - 网络普及程度不高：阻止攻击的蔓延
- 2020年代：
  - 软件防护：安全研究人员（学术界和工业界）提出的各种方案
  - 软件和网络极度普及：攻击随处可见

# 目录 Contents

# 安全从业指南

- 学术界：影响力导向
  - 安全研究
  - 企业合作
  - 人才培养
- 工业界：经济效益导向
  - 安全防护
  - 攻防对抗
  - 安全产品输出



**Yanick Fratantonio** 🌴 @reyammer · 8月20日

hey folks, bittersweet news: I'm leaving academia and @EURECOM. Next: I'll join CISCO @TalosSecurity malware research team w/ @emd3l/@xabiugarte/@_S0nn1_! SUPER excited, but it took a lot of courage/stupidity to make the move... wish me good luck :-) Here some more thoughts: 1/n

63 14 331

显示这个主题帖

**Yanick Fratantonio** 🌴 @reyammer · 8月20日

回复 @reyammer

For students reading this: do NOT let another "prof leaving academia" affect your decision to go for academia! It is a GREAT job. It's not a perfect one either, and there are pros/cons. It eventually boils down to personal trade-offs. 6/n

2 15

**Yanick Fratantonio** 🌴 @reyammer · 8月20日

I'm writing up a blog post with many thoughts that led to this decision (stay tuned!), and I hope they will help you make a more informed decision. But if you are looking for answers, you will not find them there :-) It is a very personal decision, deal with it :-) 7/n

1 21

# 学术界进阶之路

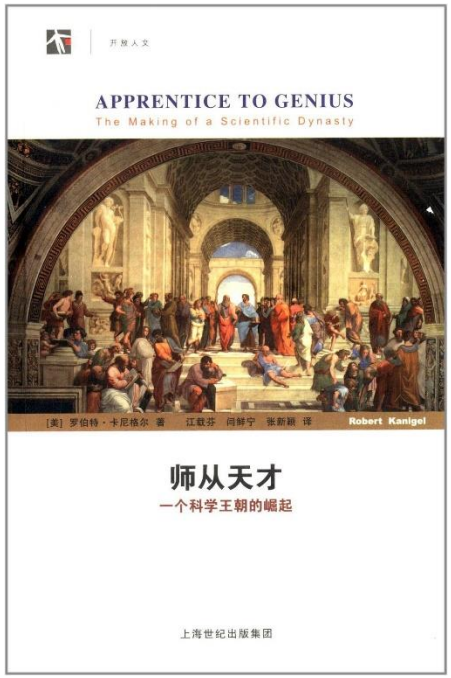
- 麻省理工学院(MIT)研究生学习指导-- 怎样做研究生
  - 快速广泛阅读
  - 了解研究现状（state-of-the-art）
  - 选择问题

- 了解安全研究社区
  - 安全研究人员
  - 安全学术会议

# 安全研究人员 排行榜

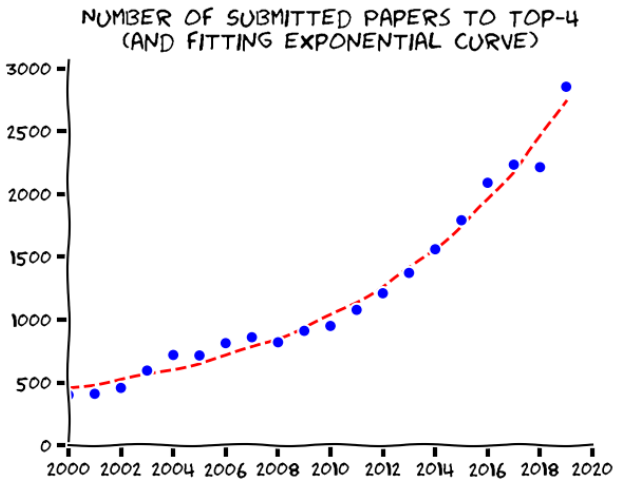
- Top 1000 Authors
  - http://s3.eurecom.fr/~balzarot/notes/top4_2019/authors_all_conf.html

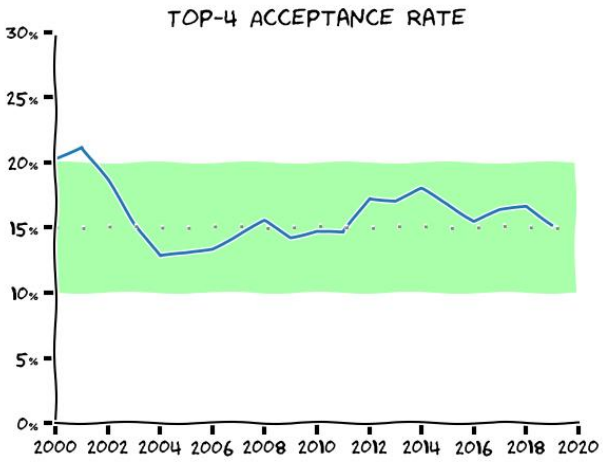
| Rank | Name | Total | Top4 | Tier2 | Oakland | CCS | Usenix | NDSS | RAID | ACSAC | Last Affiliations |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Christopher Kruegel | 112 | 75 | 37 | 13 | 17 | 22 | 23 | 15 | 22 | University of California - Santa Barbara |
| 2 | Giovanni Vigna | 106 | 67 | 39 | 9 | 18 | 22 | 18 | 14 | 25 | University of California - Santa Barbara |
| 3 | Wenke Lee | 87 | 66 | 21 | 11 | 19 | 16 | 20 | 10 | 11 | Georgia Institute of Technology |
| 4 | Dawn Song | 80 | 75 | 5 | 22 | 19 | 13 | 21 | 5 | 0 | University of California - Berkeley |
| 5 | XiaoFeng Wang | 76 | 69 | 7 | 20 | 24 | 13 | 12 | 4 | 3 | Indiana University - Bloomington |
| 6 | Michael Backes | 65 | 59 | 6 | 18 | 22 | 9 | 10 | 3 | 3 | CISPA Helmholtz Center for Information Security |
| 6 | Thorsten Holz | 65 | 41 | 24 | 10 | 9 | 12 | 10 | 10 | 14 | Ruhr-University Bochum |
| 8 | Michael K. Reiter | 56 | 48 | 8 | 12 | 19 | 7 | 10 | 7 | 1 | University of North Carolina - Chapel Hill |
| 9 | Engin Kirda | 53 | 34 | 19 | 12 | 3 | 7 | 12 | 8 | 11 | Northeastern University |
| 9 | Vern Paxson | 53 | 48 | 5 | 11 | 14 | 18 | 5 | 4 | 1 | University of California - Berkeley<br>International Computer Science Institute (ICSI) |
| 11 | Angelos D. Keromytis | 50 | 35 | 15 | 8 | 16 | 5 | 6 | 6 | 9 | Columbia University |
| 12 | Ari Juels | 47 | 44 | 3 | 6 | 25 | 12 | 1 | 1 | 2 | Cornell Tech |
| 13 | Ahmad-Reza Sadeghi | 46 | 39 | 7 | 5 | 13 | 8 | 13 | 3 | 4 | Technical University - Darmstadt |
| 13 | Dan Boneh | 46 | 45 | 1 | 7 | 20 | 11 | 7 | 0 | 1 | Stanford University |
| 15 | Adrian Perrig | 43 | 41 | 2 | 21 | 12 | 1 | 7 | 0 | 2 | ETH Zurich |
| 15 | Somesh Jha | 43 | 34 | 9 | 13 | 8 | 10 | 3 | 4 | 5 | University of Wisconsin - Madison |
| 17 | Zhiqiang Lin | 42 | 29 | 13 | 2 | 8 | 8 | 11 | 7 | 6 | Ohio State University |
| 18 | Patrick McDaniel | 40 | 27 | 13 | 4 | 11 | 6 | 6 | 0 | 13 | Pennsylvania State University |
| 19 | David Wagner | 39 | 37 | 2 | 7 | 9 | 17 | 4 | 0 | 2 | University of California - Berkeley |
| 19 | Guofei Gu | 39 | 25 | 14 | 3 | 7 | 7 | 8 | 8 | 6 | Texas A&M University |
| 19 | Herbert Bos | 39 | 26 | 13 | 9 | 5 | 8 | 4 | 5 | 8 | Vrije University - Amsterdam |
| 19 | Peng Liu | 39 | 17 | 22 | 0 | 8 | 6 | 3 | 6 | 16 | Pennsylvania State University |
| 19 | Srdjan Capkun | 39 | 30 | 9 | 6 | 8 | 11 | 5 | 0 | 9 | ETH Zurich |



# 安全学术会议

- Top 4 + 2
  - http://s3.eurecom.fr/~balzarot/notes/top4_2019/
  - IEEE S&P (a.k.a Oakland)
  - USENIX Security
  - ACM CCS
  - NDSS
  - RAID
  - ACSAC



# 安全学术活动

- 工业界主导的安全会议
- 国际活动
  - Blackhat、DEF CON
  - RSA大会
- 国内活动
  - 360安全大会
  - 奇安信安全大会
  - DEF CON 神州安全大会
  - 腾讯互联网安全领袖峰会
  - XDef


# 工业界进阶之路

- 产品安全
  - 安全开发
  - 应急响应
  - 安全合作
- 安全分析对抗
  - 漏洞挖掘
  - 安全事件分析
- 独立安全服务
  - 安全工具
  - 安全咨询、安全审计

Gold Supporters

avast　CISCO

facebook　Google

Silver Supporters

Baidu 百度　CERT Software Engineering Institute Carnegie Mellon

IBM Research　intel

# 企业安全防护

- 安全开发
  - DevSecOps vs. SecDevOps vs. DevOpsSec
- 应急响应
  - SRC：漏洞处理
  - 运维部门：24小时事故处理
- 安全合作
  - 联合研究项目
  - 企业-高校联合研究中心

**姓名** 黄颖

**职位** 上海交通大学-蚂蚁金服安全科技联合研究中心运营管理组长

**介绍** 支撑联合创新中心，项目管理、人才引进、预算管理和会议组织等工作

**姓名** 王俊瑛

**职位** 上海交通大学-蚂蚁金服安全科技联合研究中心运营管小组成员

**介绍** 支撑联合创新中心，项目管理、人才引进、预算管理和会议组织等工作

**姓名** 陈泽元

**职位** 上海交通大学-蚂蚁金服安全科技联合研究中心运营管小组成员

**介绍** 支撑联合创新中心，项目管理、人才引进、预算管理和会议组织等工作

·丰厚大奖·

重磅大奖

36万元

单个漏洞最高奖励

年度大奖

海外知名公司 高校游学

年度前8名

季度大奖

周大福纯金勋章

季度金币数第一

# 安全分析对抗

- 漏洞挖掘
  - Google Project Zero
  - 腾讯科恩实验室
  - 360

Project Zero

News and updates from the Project Zero team at Google

- 安全事件分析
  - Cisco Talos Intelligence Group
  - Symantec @ Accenture

TALOS

BROADCOM. Symantec

# 独立安全服务

- 安全工具
  - 程序分析工具
  - 程序保护工具
  - 网络防护系统
- 安全咨询、安全审计
  - 产品安全测试
  - 渗透测试
  - 安全设计

FireEye™
Next Generation Threat Protection

长亭科技
CHAITIN.CN

paloalto networks®
the enterprise security company™

lastline™

Hex-Rays

nccgroup

# 安全竞赛

- 攻防竞赛
  - CTF
  - Pwn2Own、GeekPwn
- 分析竞赛
  - Datacon
- 作品赛
  - 信安大赛


Folks,
Frank, Mahmud, Azizan and Matt have judged all submissions and results have been posted on the challenge web site. The winners are:

1. Emilien Girault
2. Yuhao Luo, Wenbo Yang and Juanru Li
3. José Lopes Esteves

Really congratulations to the winners and thanks to the other partecipants.

Stay tuned because a new challenge is going to start in the next hours!

Angelo Dell'Aera
The Honeynet Project

| TOTAL | | Attack | | | | | |
|---|---|---|---|---|---|---|---|
| 970 | A*0*E | 2317.5 | A*0*E | 88 | Shellphish | 542 | CyKor |
| 968 | PPP | 2227.0 | PPP | 79 | NorseCode | 484 | koreanbadass |
| ▲841 | HITCON × Balsn | 1831.0 | Tea Deliverers | 73 | CyKor | 438 | Star-Bugs |
| ▼750 | Tea Deliverers | 1679.5 | HITCON × Balsn | 62 | mhackeroni | 428 | RPISEC |
| ▲635 | More Bush Smoked Whackers | 1563.0 | 侍 | 62 | r3kapig | 385 | r3kapig |
| ▲570 | 侍 | 1138.5 | More Bush Smoked Whackers | 57 | Star-Bugs | 349 | mhackeroni |
| ▼495 | Shellphish | 1130.5 | Shellphish | 48 | koreanbadass | 314 | 侍 |
| ▲435 | CyKor | 1125.5 | NorseCode | 46 | RPISEC | 205 | NorseCode |
| ▼409 | /bin/tw | 1053.0 | CyKor | 22 | pasten | 130 | pasten |
| ▲394 | NorseCode | 885.5 | Star-Bugs | | | | |
| ▼352 | Star-Bugs | 645.0 | koreanbadass | | | | |
| ▼303 | koreanbadass | 416.0 | /bin/tw | | | | |
| ▲273 | mhackeroni | 403.5 | mhackeroni | | | | |
| ▼260 | r3kapig | 268.5 | r3kapig | | | | |
| 211 | RPISEC | 134.5 | RPISEC | | | | |
| 77 | pasten | 0.0 | pasten | | | | |

$350\,{}^{a}/_{M_a} + 350\,{}^{d}/_{M_d} + 300\,{}^{k}/_{M_k}$

$\Sigma$ tick (1 per non-stealth flag)

$M_a = \max(\uparrow, 100) = 2317.5$

$\Sigma$ tick (1 if non-exploited AND there were exploits)

$M_d = \max(\uparrow, 100) = 150$

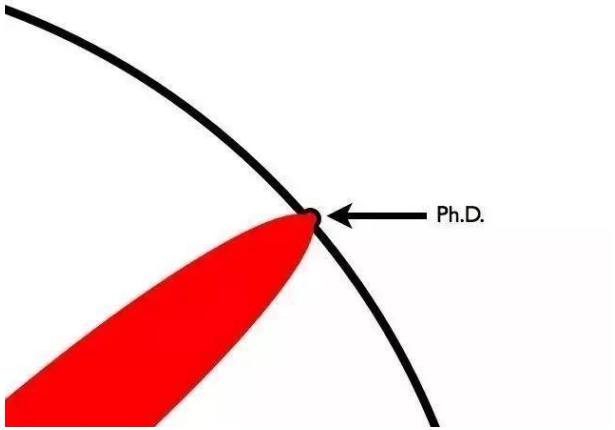
$\Sigma$ tick (10 if first-ranked down to 1 for fifth)

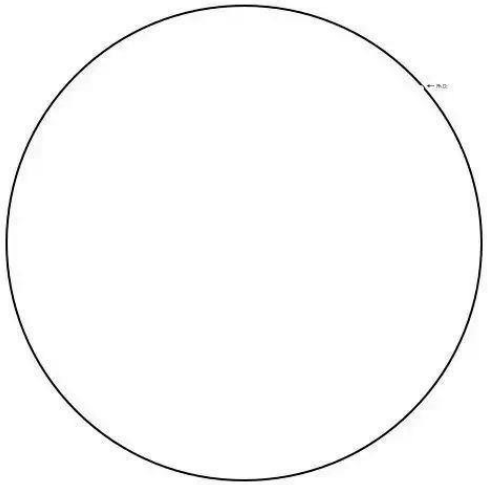
$M_k = \max(\uparrow, 100) = 1545$

# 安全竞赛vs科研?

- How to address well defined problems
  - 已知答案 vs 未知答案


- How to define a problem well
  - https://new.qq.com/omn/20181219/20181219B082GV.html



# 科研的精神

- 批判性思维
  - 科学是关于“不知道”，而不是“知道”
- 站在巨人肩膀上
  - 永远从已有成果出发
- 解决问题，而不是提出想法、技术
  - “我想登月”
  - “我登上了月球”

# 目录 Contents

# 安全人员的威胁模型^_^

- 网络安全法规
  - 《中华人民共和国网络安全法》
  - ~~乌云~~
- 道德标准
  - 白帽黑客vs灰帽黑客vs黑帽黑客
- 犯罪分子
  - 威逼or利诱?
- 国家机器
  - FBI


乌云及相关服务升级公告

尊敬的各位用户：

为了更好地向大家提供服务，乌云及相关服务将进行升级。我们将在最短的时间内，以最好的姿态回归。

一直以来，乌云致力于让安全性作为用户选择产品的重要考量之一，促进企业更重视安全，让更多人了解安全关注安全，从而营造出更好的安全生态。

不管从前，现在，还是未来，我们都将坚持这么做下去。

**与其听信谣言，不如相信乌云。**

共勉。

乌云全体成员 敬上
2016年7月20日

# 漏洞通报流程

- Policy and Disclosure: 2020 Edition
  - https://googleprojectzero.blogspot.com/2020/01/policy-and-disclosure-2020-edition.html
  - For vulnerabilities reported starting January 1, 2020, we are changing our Disclosure Policy: **Full 90 days by default, regardless of when the bug is fixed**.

  - “安全研究员 Allison Husain 在 2020年4月向 Google 报告了一个漏洞，该漏洞允许攻击者模仿任何 Gmail 或 G Suite 客户发送欺骗性邮件。但 Google 没有在 90 天时间内修复漏洞，它计划的修复时间是在 9 月份，也就是在漏洞报告 5 个月之后。8 月 19 日，Husain 在其个人博客上披露了漏洞细节，包括 POC 漏洞利用代码。Google 开发者在漏洞公开 7 个小时后给 Gmail 打了补丁阻止漏洞被利用，但完整补丁将在 9 月份部署。”

# 漏洞提交引发的故事

- Tesla 案例
  - https://vshare.sjtu.edu.cn/play/f619602c654e95ac0b43c4ce50594c94
  - 我们在今年5月向Tesla提交了漏洞报告
    - 然而……

**Security Vulnerabilities of Fingerprint Authentication in Tesla Apps (Android and iOS versions)**

**Issues of Tesla Android App**

**APP Info**

package Name: *com.teslamotors.tesla*
Version: *3.10.4 (f5597473b)*
MD5: bfe7bdd7eda1bab56213b6819edeb768

- Libsodium案例
  - https://github.com/jedisct1/libsodium/issues/617

**jedisct1** commented on Oct 22, 2017

Unfortunately, this is tricky to do reliably, if possible at all.

**jedisct1** added a commit that referenced this issue on Nov 6, 2017

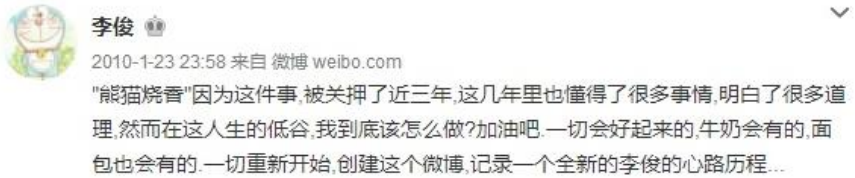
`Symbolically clear the round keys after aes256gcm_(en|de)crypt()` ...

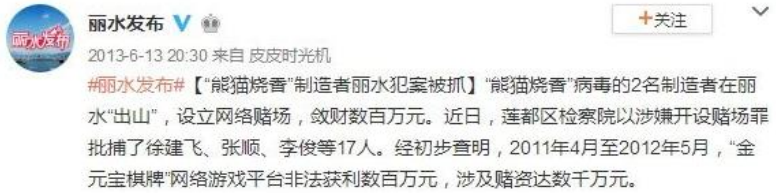
# 安全论文道德规范

- From USENIX Security 2021 Submission Policies and Instructions
  - If the submission deals with **vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system)**, the authors need to **discuss in detail the steps they have already taken or plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors)**. The same applies if the submission deals with **personally identifiable information (PII) or other kinds of sensitive data**.
  - If a paper raises significant ethical and legal concerns, it might be **rejected based on these concerns**.

# 如何保护自身

- 法律意识
  - 远离网络犯罪事件
  - 远离涉黑人员，洁身自好
  - 渗透测试需要取得授权！！！
- 金钱
  - 漏洞奖励 – OK!
  - 安全研究项目津贴 – OK!
  - 黑产攻击代码、游戏外挂 -- ☹ ☹ ☹
    - 即使是以bitcoin方式支付!



# 谢 谢!