网络协议侧信道的漏洞简史

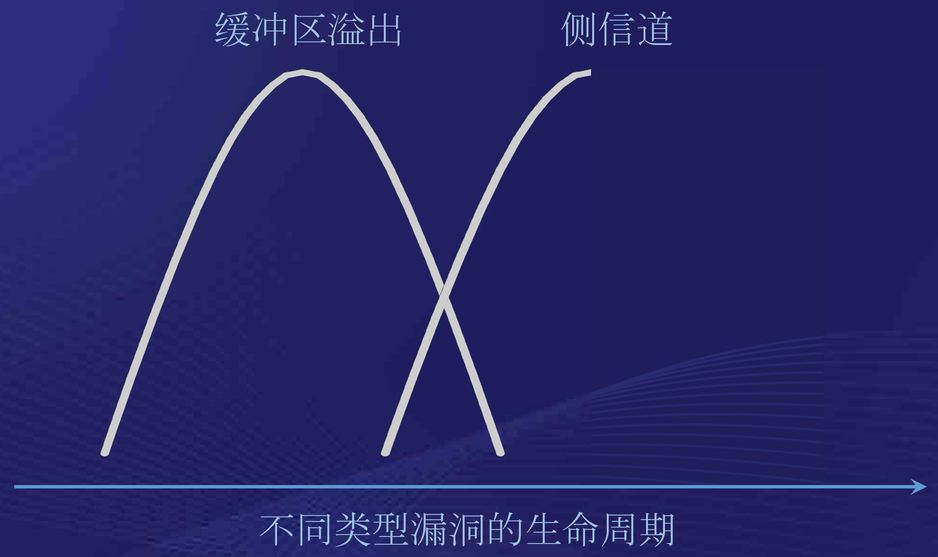
钱志云 加利福尼亚大学河滨分校

目录

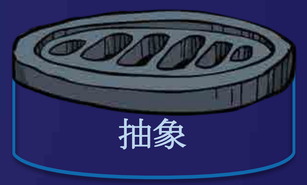
- 什么是侧信道？
- （网络）侧信道如何产生？
- 现实中的TCP/IP侧信道
- 如何系统地发现它们？

什么是侧信道？

- “意外”泄露敏感信息的信道
- 下一代缓冲区溢出漏洞



（网络）侧信道如何产生？



（网络）侧信道如何产生？

- 需要打破抽象

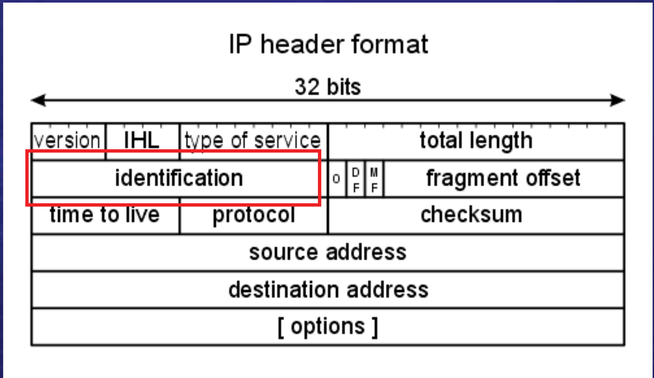
什么是侧信道？

什么是侧信道？

什么是侧信道？

首个著名的网络侧信道（于1998年报道）

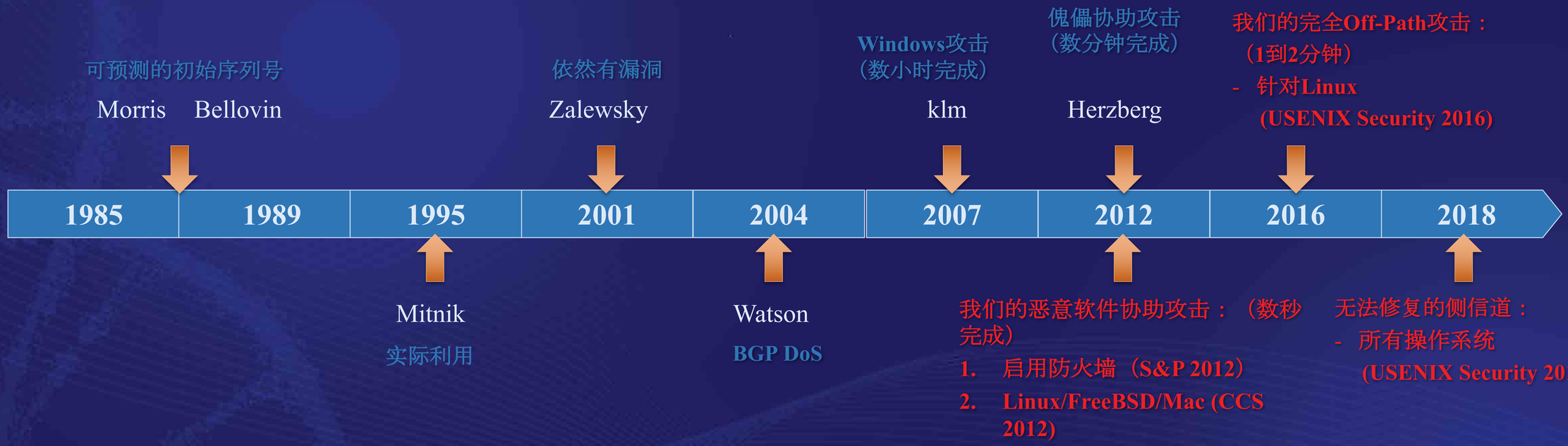
- 共享资源： **Windows操作系统上的全局IPID计数器**



TCP侧信道攻击

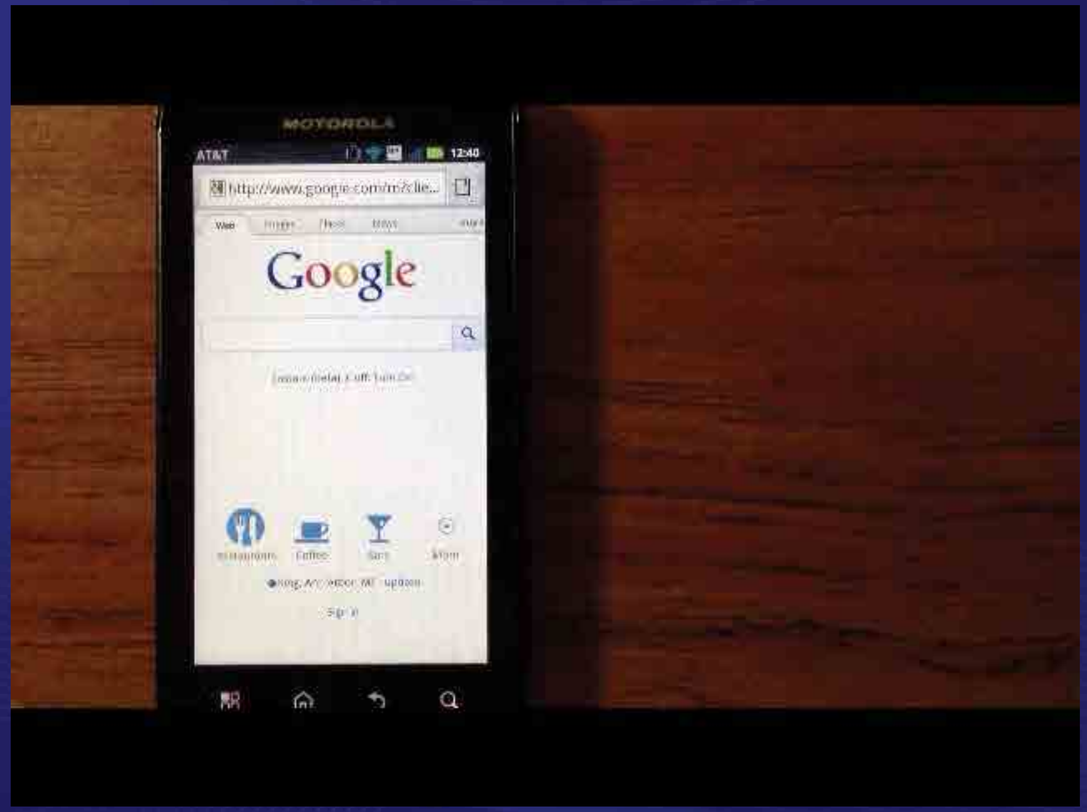
- 威胁模型：Off-Path (非中间人) 攻击者，能发送伪造IP源地址的数据包
- 目的：推断任意两台主机之间的连接状态
  - 它们是否有TCP连接？序列号是多少？

TCP序列号之争时间轴



演示：TCP侧信道攻击（2012）

要求：在设备上与远程费中间人攻击者协作的低权限恶意软件。



TCP侧信道攻击（2016 Linux）

- 无恶意软件需求！
- 全局速率限制 Challenge ACK 类型的网络包 (Rate limit)， 共享资源
  - 所有连接共享
  - 默认值：100（每秒重置）

漏洞？如何利用？

- 例如：猜测正确的客户端端口号
  - 如猜对：

漏洞？如何利用？

- 例如：猜测正确的客户端端口号
  - 如猜错：

客户端

服务器

无 challenge ACK

带客户端IP和猜测的src端口的欺骗 SYN

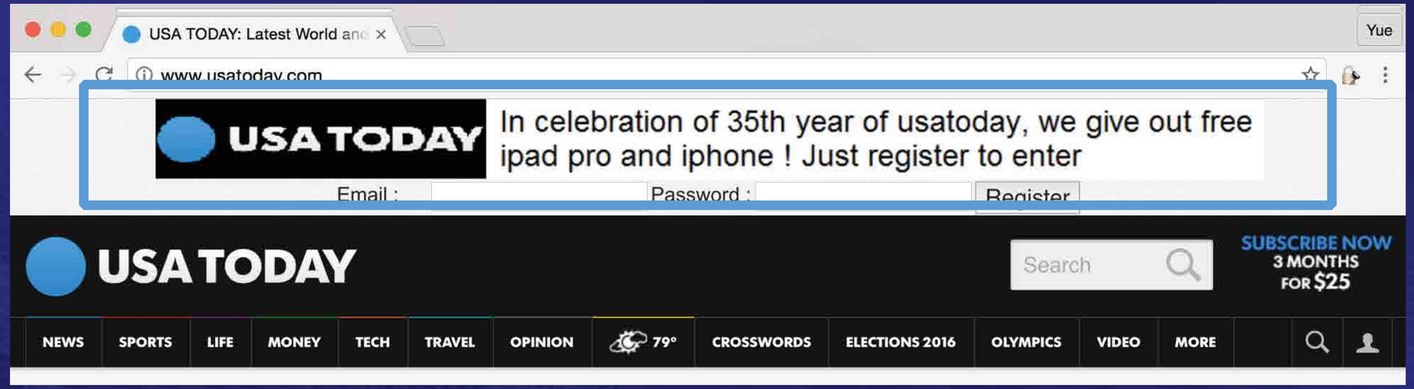
100 RST

100 challenge ACK

攻击者

攻击影响

- 连接存在：小于10 秒
- 序列号：　30 秒
- ACK 号：　小于10 秒



经验教训

- 不能忽略任何小型共享资源
- 上报Linux

打补丁，并包修订了TCP规范（RFC 5961）

Status: Held for Document Update (1)

RFC 5961, "Improving TCP's Robustness to Blind In-Window Attacks", August 2010

Source of RFC: tcpm (tsv)

Errata ID: 4772
Status: Held for Document Update
Type: Technical

Reported By: Stéphane Bortzmeyer
Date Reported: 2016-08-10
Held for Document Update by: Mirja Kühlewind
Date Held: 2016-09-12

Section 7 says:

```
[The entire section]
```

It should say:

```
No suggested text because it requires a much more serious analysis.
May be adding that the rate-limit counter SHOULD be per-connection,
in the spirit of RFC 6528?
```

Notes:

It appears the section does not specify that the counter for ACK throttling SHOULD be per-connection. In Linux, it is apparently global, which allowed its use as a side channel enabling nasty attacks (CVE-2016-5696 and the paper "Off-Path TCP Exploits: Global Rate Limit Considered Dangerous" <http://www.cs.ucr.edu/~zhiyunq/pub/sec16_TCP_pure_offpath.pdf>).
Also see discussion on tcpm list about this reported errata!

其他侧信道？

- 后续思考
  - 是否可以穷举所有共享资源?
  - 答案是肯定的, 至少在软件层面

其他侧信道？

- 后续思考
  - 是否可以穷举所有共享资源?
  - 答案是肯定的, 至少在软件层面

- 5个新的侧信道 FreeBSD 4.9.3
- 7个新的侧信道 Linux 4.8.0

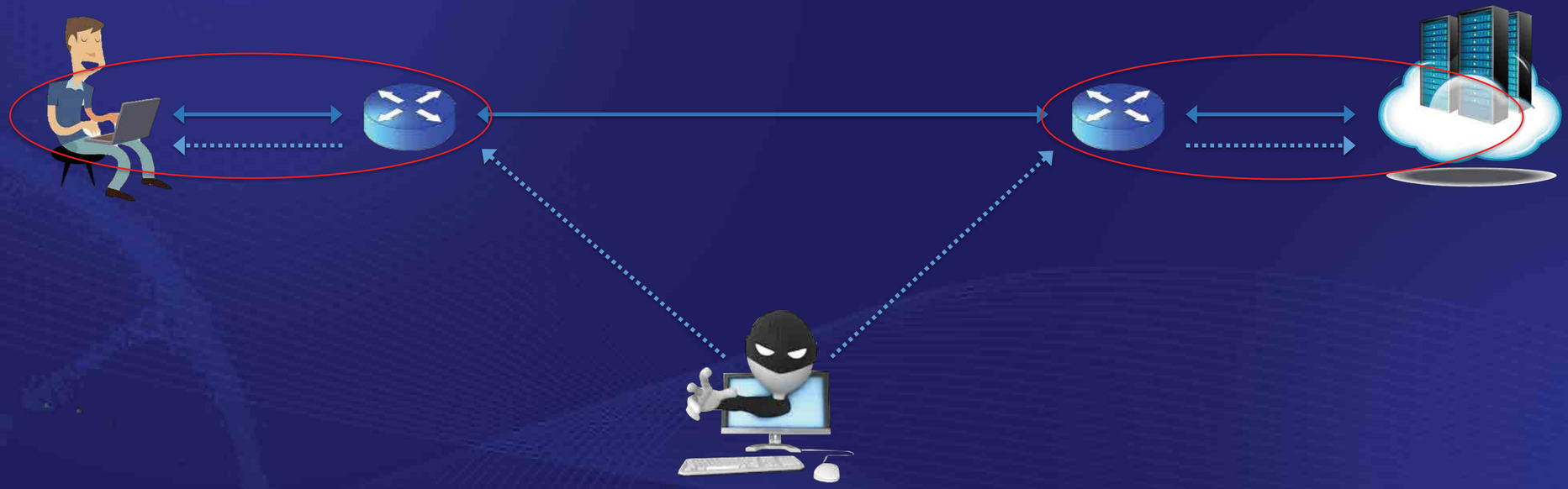
(ACM CCS 2019)

TCP侧信道攻击（2018 wifi）

- 是否存在任何其他非软件的共享资源？

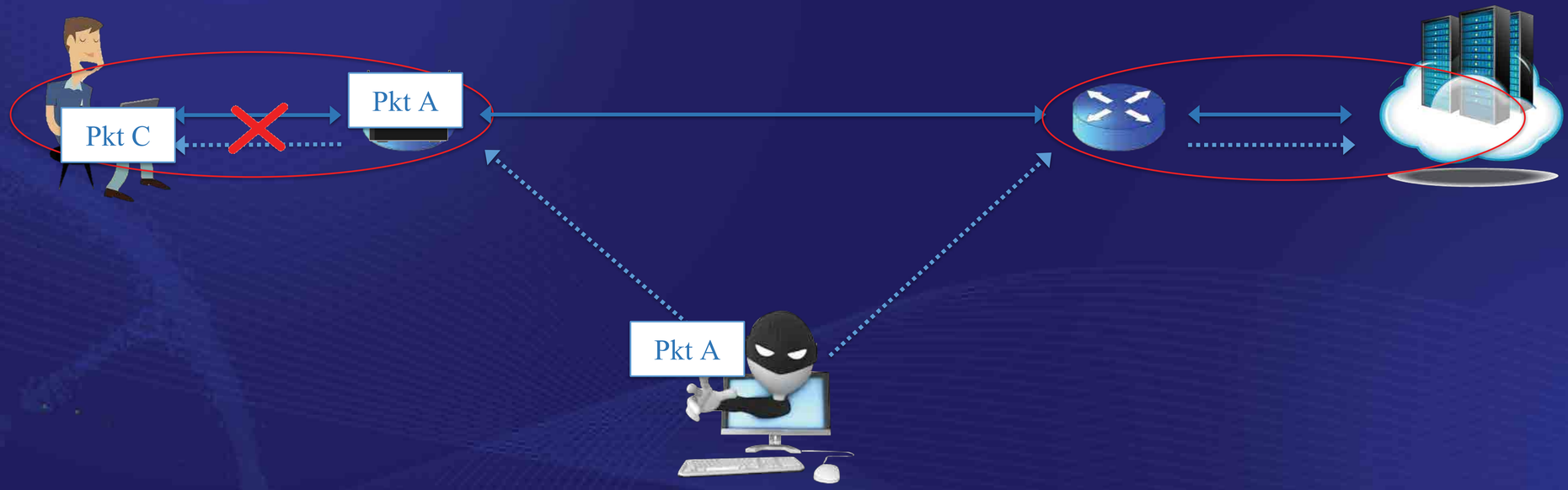
TCP侧信道攻击（2018 wifi）

- 是否存在任何其他非软件的共享资源？
  - 答案：共享物理网络链路！



TCP侧信道攻击（2018 wifi）

- 共享链路有什么问题？
  - 全双工链路->半双工链路！

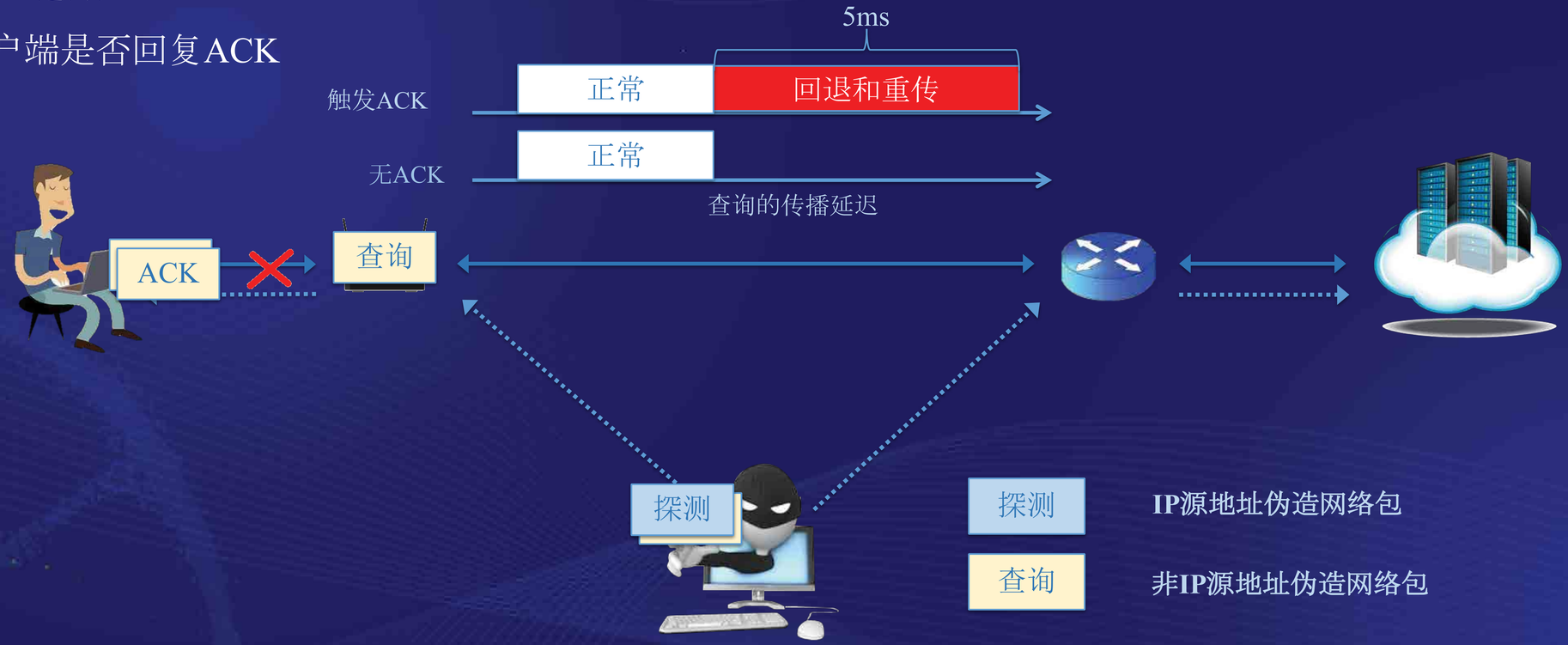


TCP连接劫持——所有 WiFi 都不安全

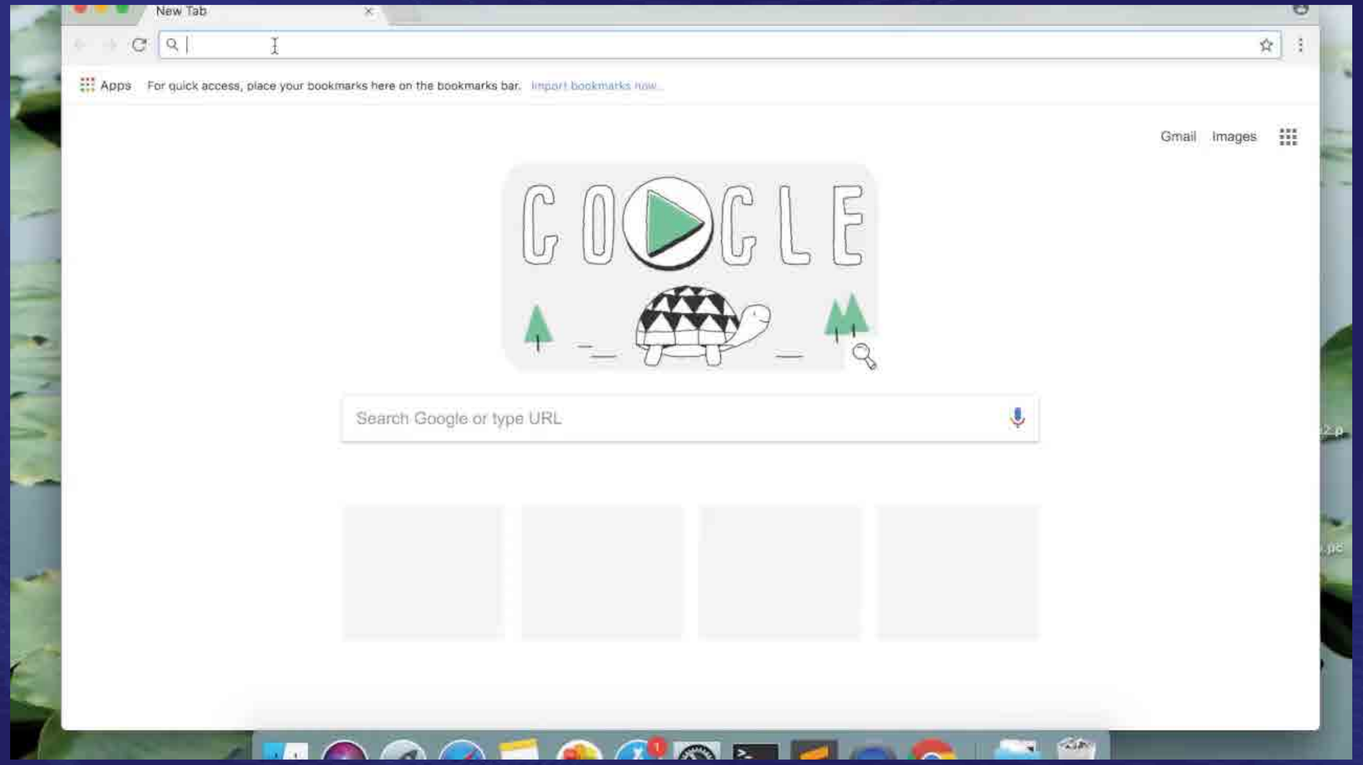
- 利用半双工链路
  - 推断客户端是否回复ACK

TCP连接劫持——所有 WiFi 都不安全

- 利用半双工链路
  - 推断客户端是否回复ACK

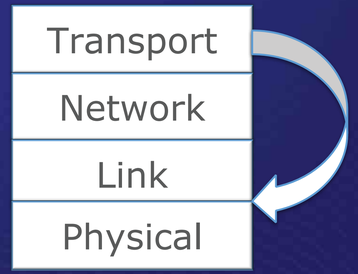


演示：浏览器缓存污染攻击 (2018)



经验教训

- 非软件的共享资源：半双工链路
- 相同原则：打破网络层抽象
- 上报IEEE 802.11工作组
  - 无解决方案



谢谢

钱志云
zhiyunq@cs.ucr.edu

发现网络侧信道的关键

- 存在哪些共享资源？
- 攻击者可以探测到什么？
- 受害者的密码如何“影响”共享资源的状态？