



看雪 2018 安全开发者峰会

Kanxue 2018 Security Developer Summit

2000-2018

从 W P A 2 四 次 握 手 看 K R A C K 密 钥 重 装 攻 击

石冰

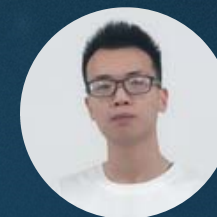


看雪 2018 安全开发者峰会
Kanxue 2018 Security Developer Summit

自我介绍

石冰

- 学生，大三在读。
- 安全爱好者，热衷于各类安全技术研究。
- CTF:RE/CRYPTO。
- Windows病毒狂热爱好者。



目录



KRACK

WPA2 Key Reinstallation Attack

- KRACK是什么
- 四次握手协议分析
- 如何攻击Msg3传输
- 这个攻击到底能做什么？？？
- 如何对抗KRACK



看雪 2018 安全开发者峰会
Kanshu 2018 Security Developer Summit

什么是KRACK

- What: KRACK (**K**ey **R**einstallation Att**ack**), 其本质是重放攻击。
- Where: 局域网环境
- Who: WPA/WPA2 WI-FI网络
- When: 当一个客户端试图连接一个受保护的WI-FI (触发四次握手)
- Why: 四次握手协议允许AP多次重传Msg3, 造成nouce被重置
- ◆ How: 说来话长.....



四次握手协议分析

所有安全的WI-FI网络，都会通过四次握手协议来生成一个会话密钥PTK。

PTK的生成共包含5部分：

- Anonce
- Snonce
- Amac
- Smac
- PMK

supplicant

客户端

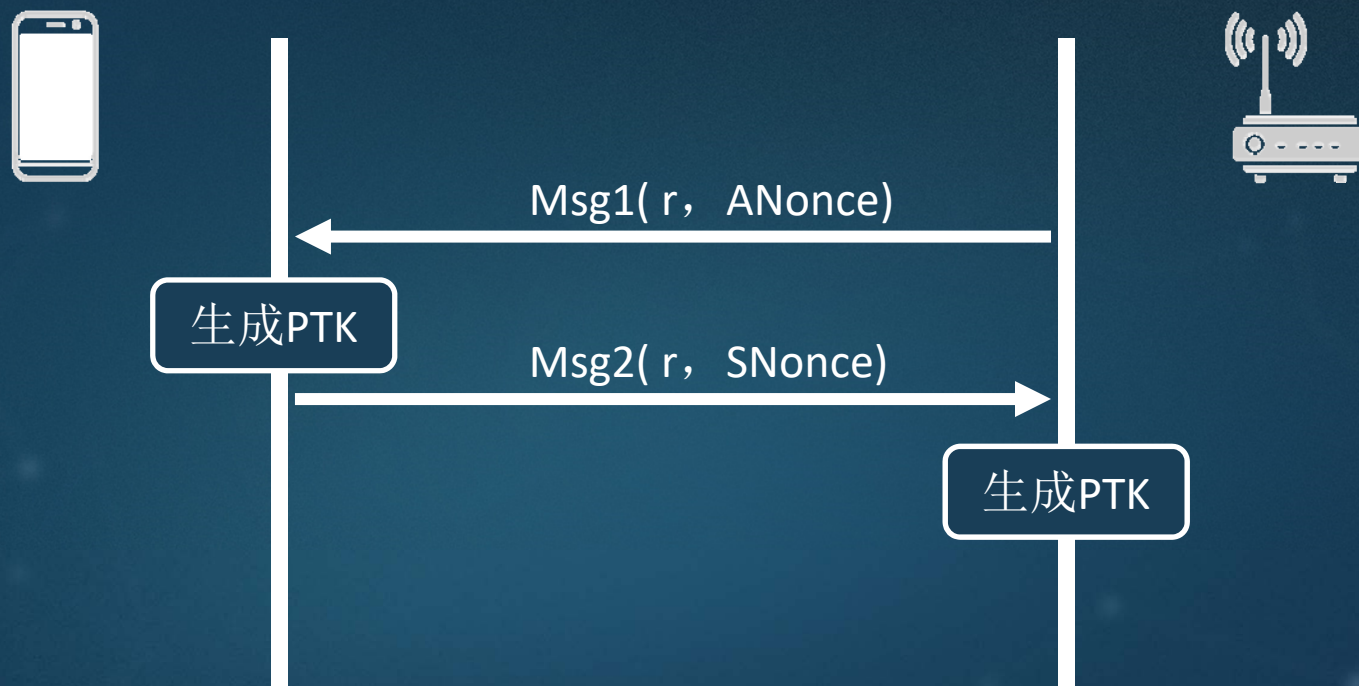


authenticator

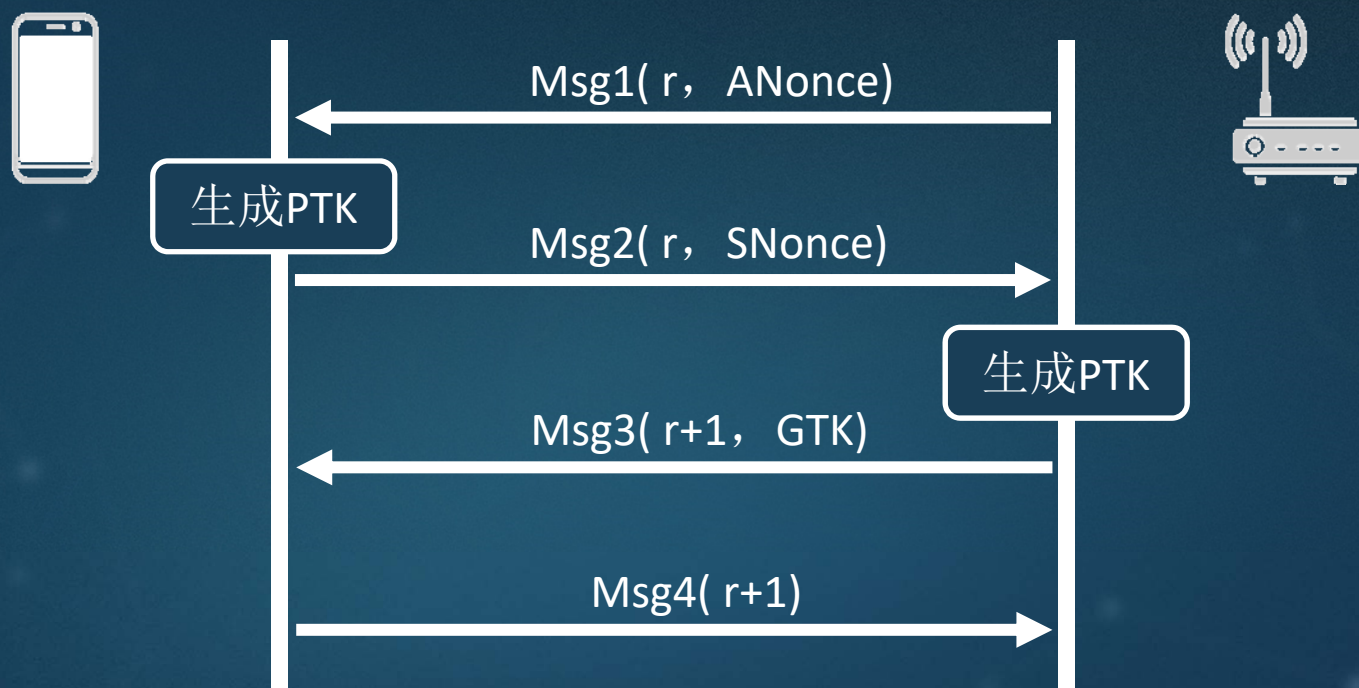
AP



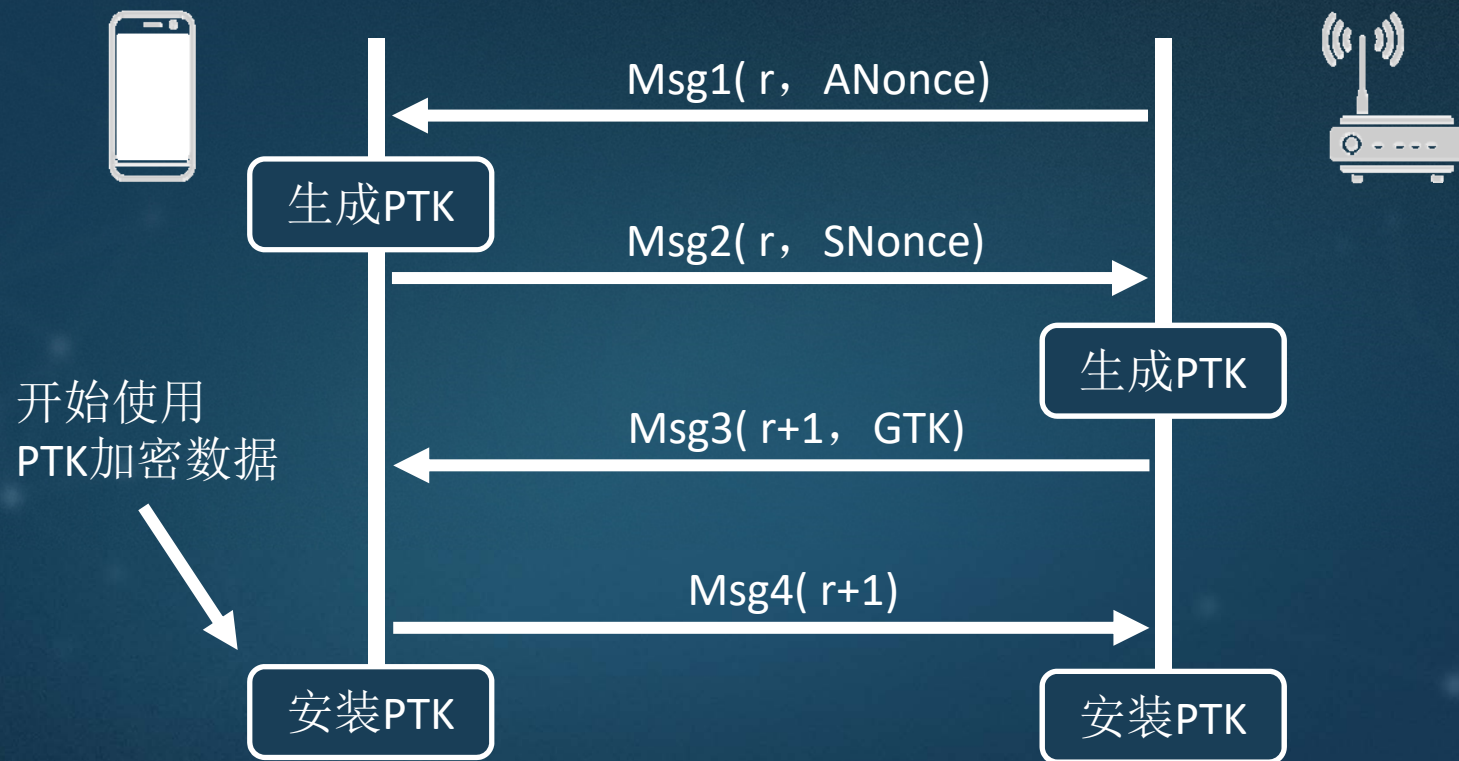
四次握手协议分析



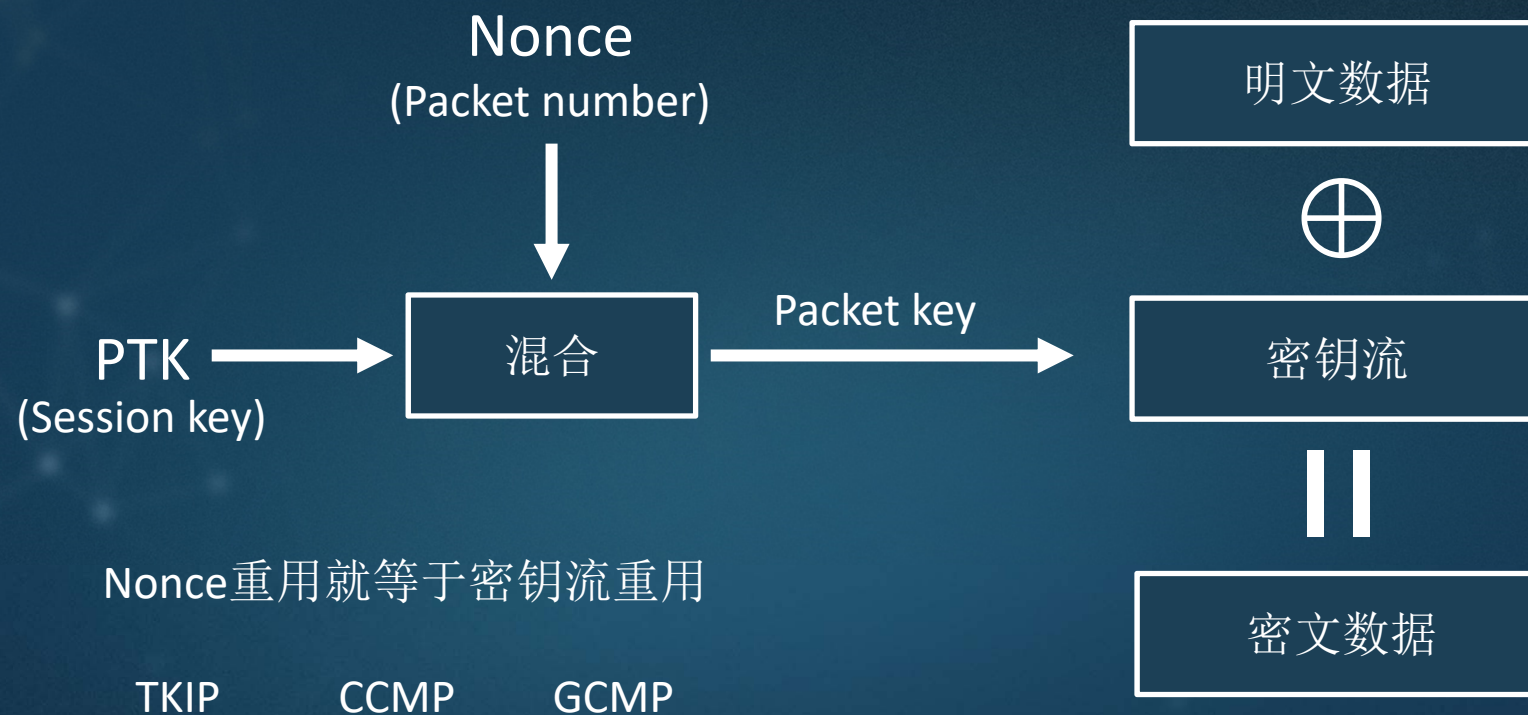
四次握手协议分析



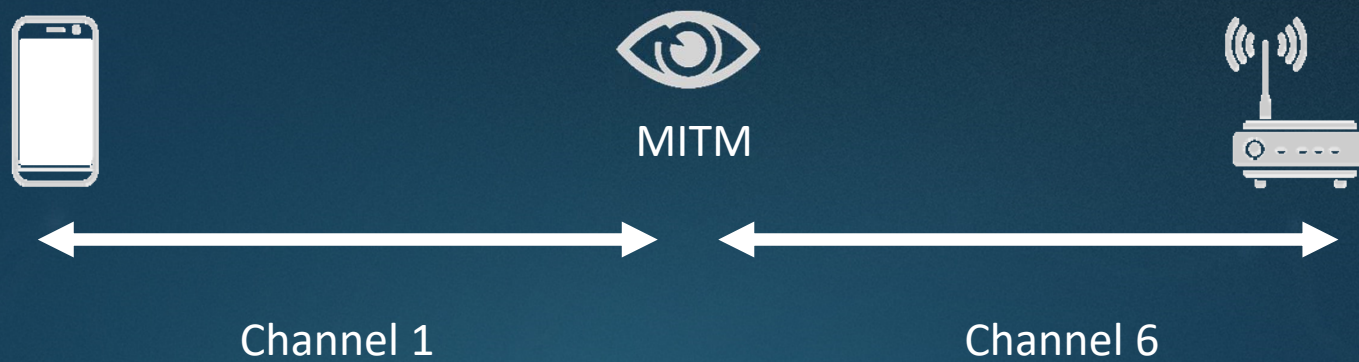
四次握手协议分析



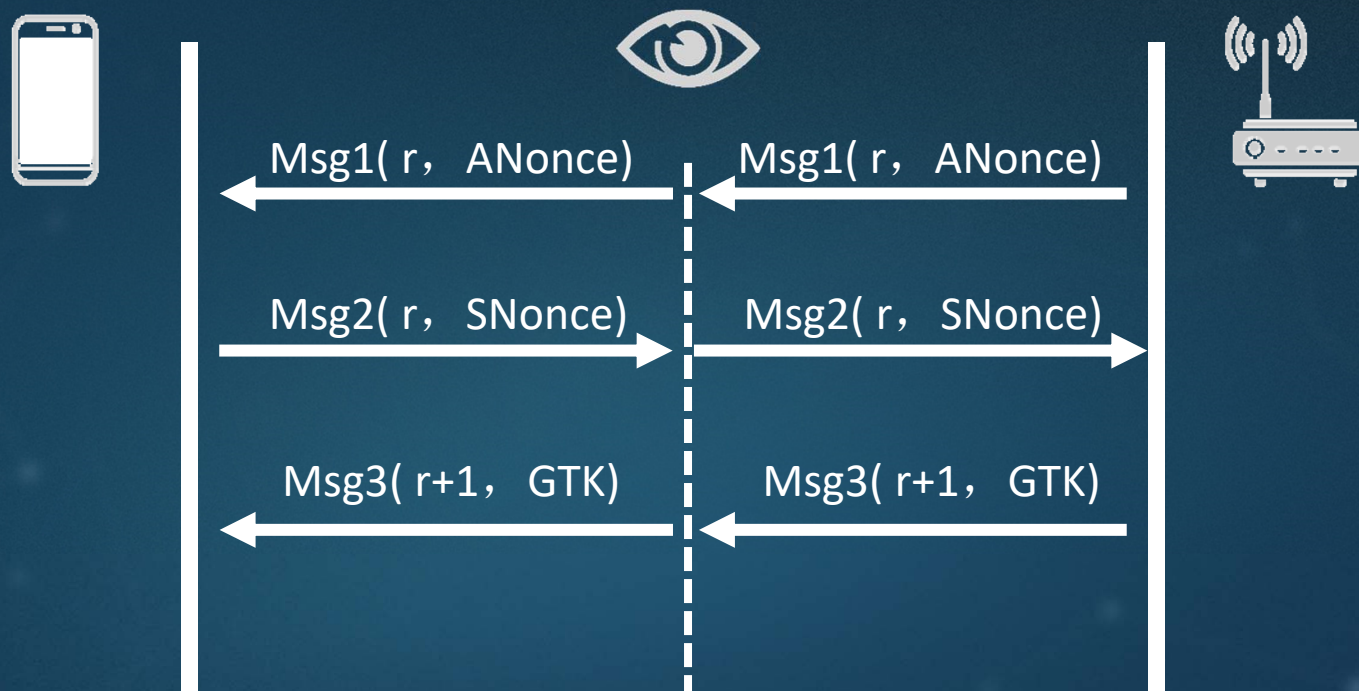
四次握手协议分析



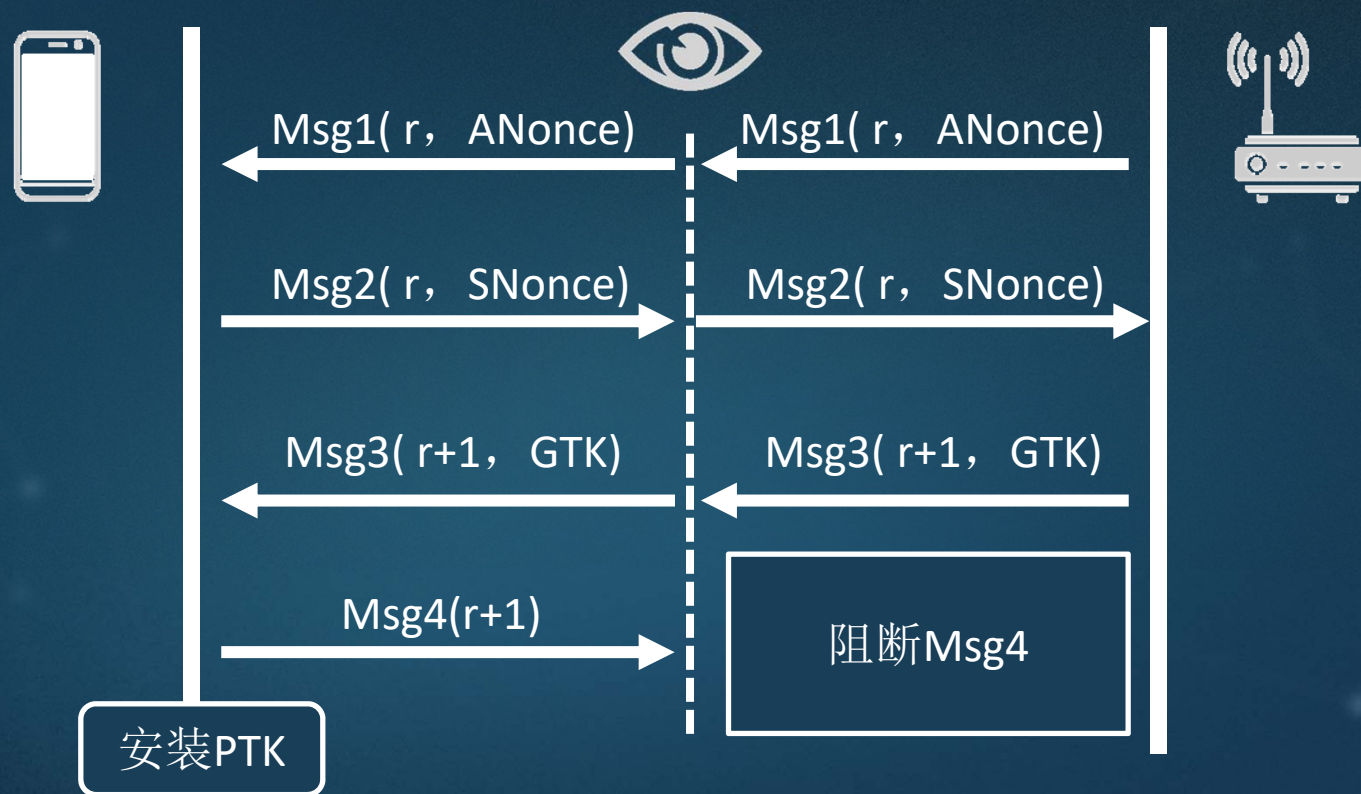
如何攻击Msg3传输



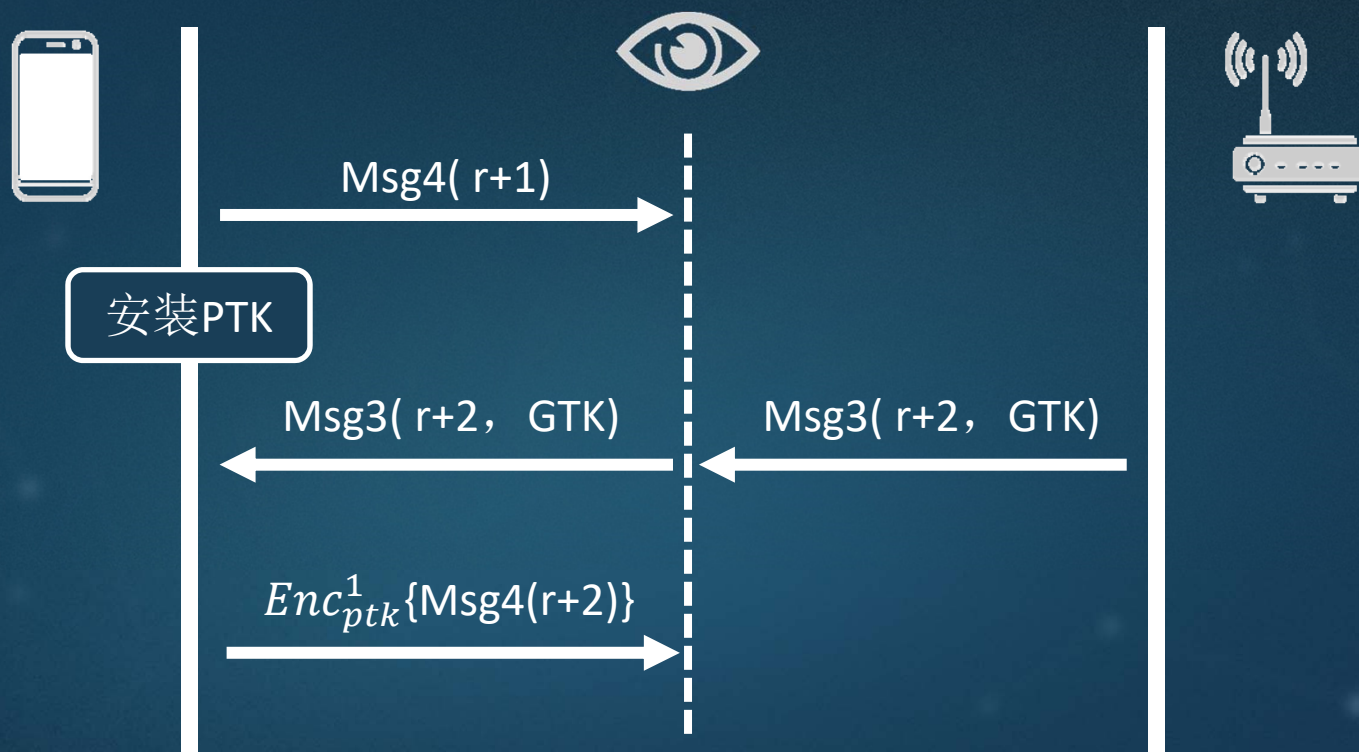
如何攻击Msg3传输



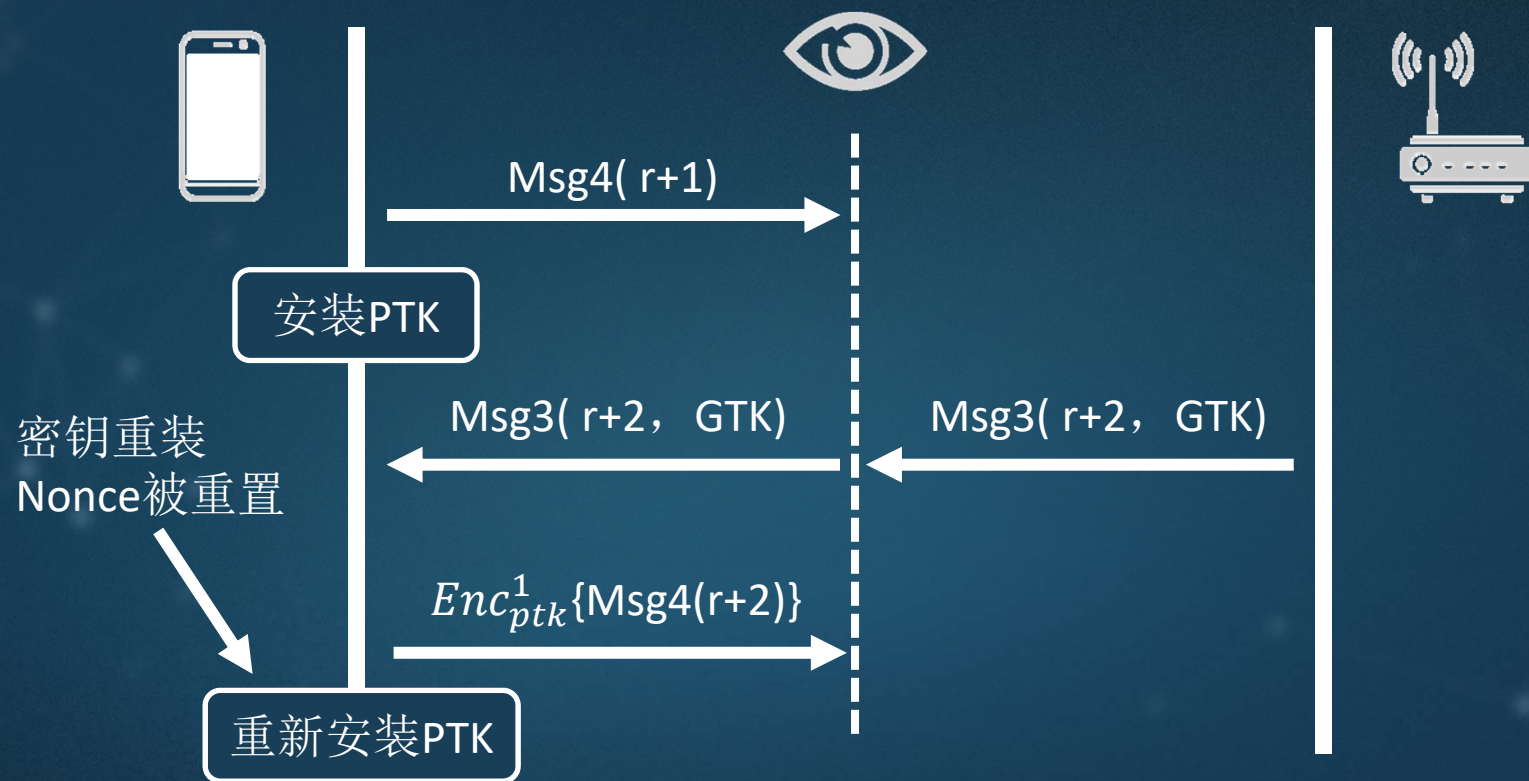
如何攻击Msg3传输



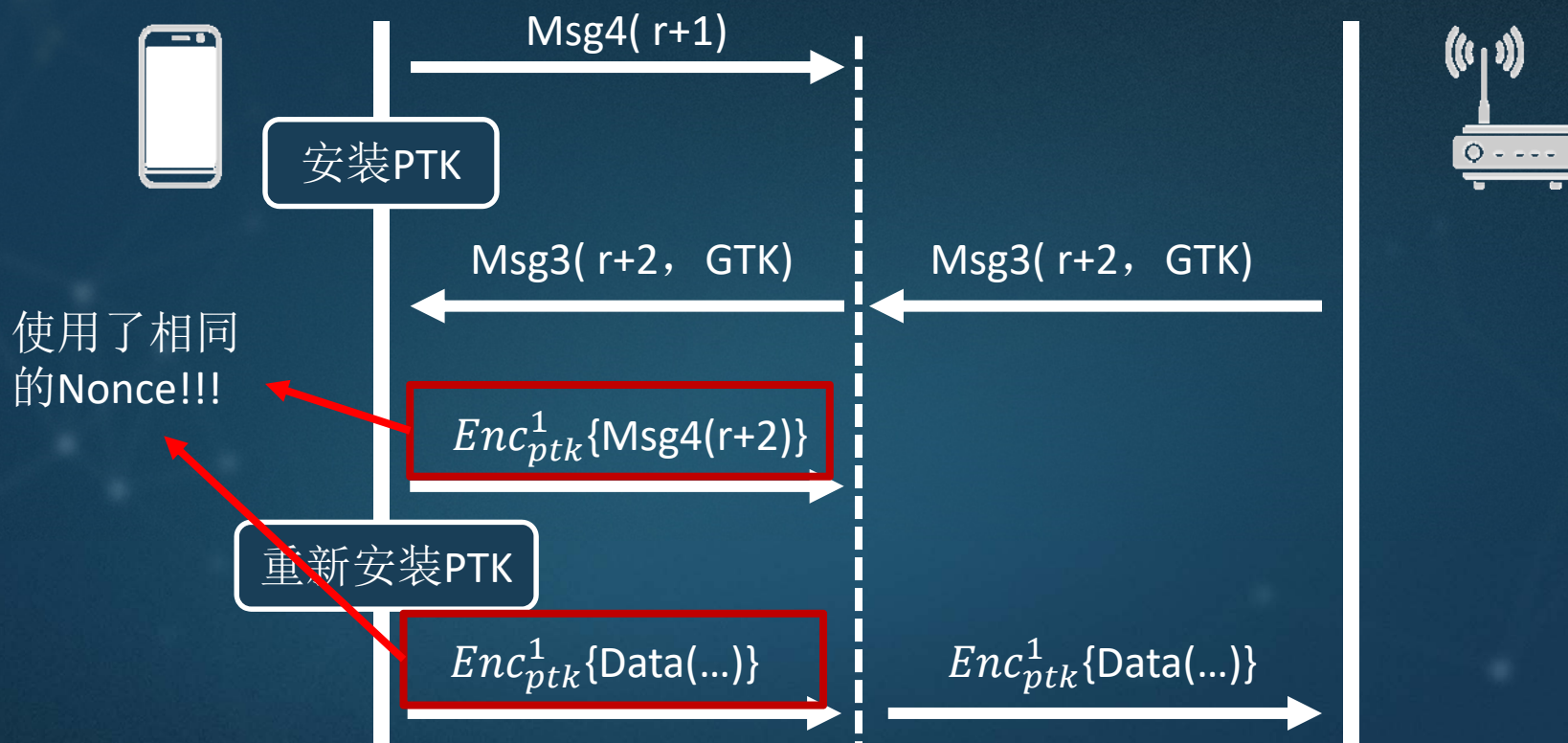
如何攻击Msg3传输



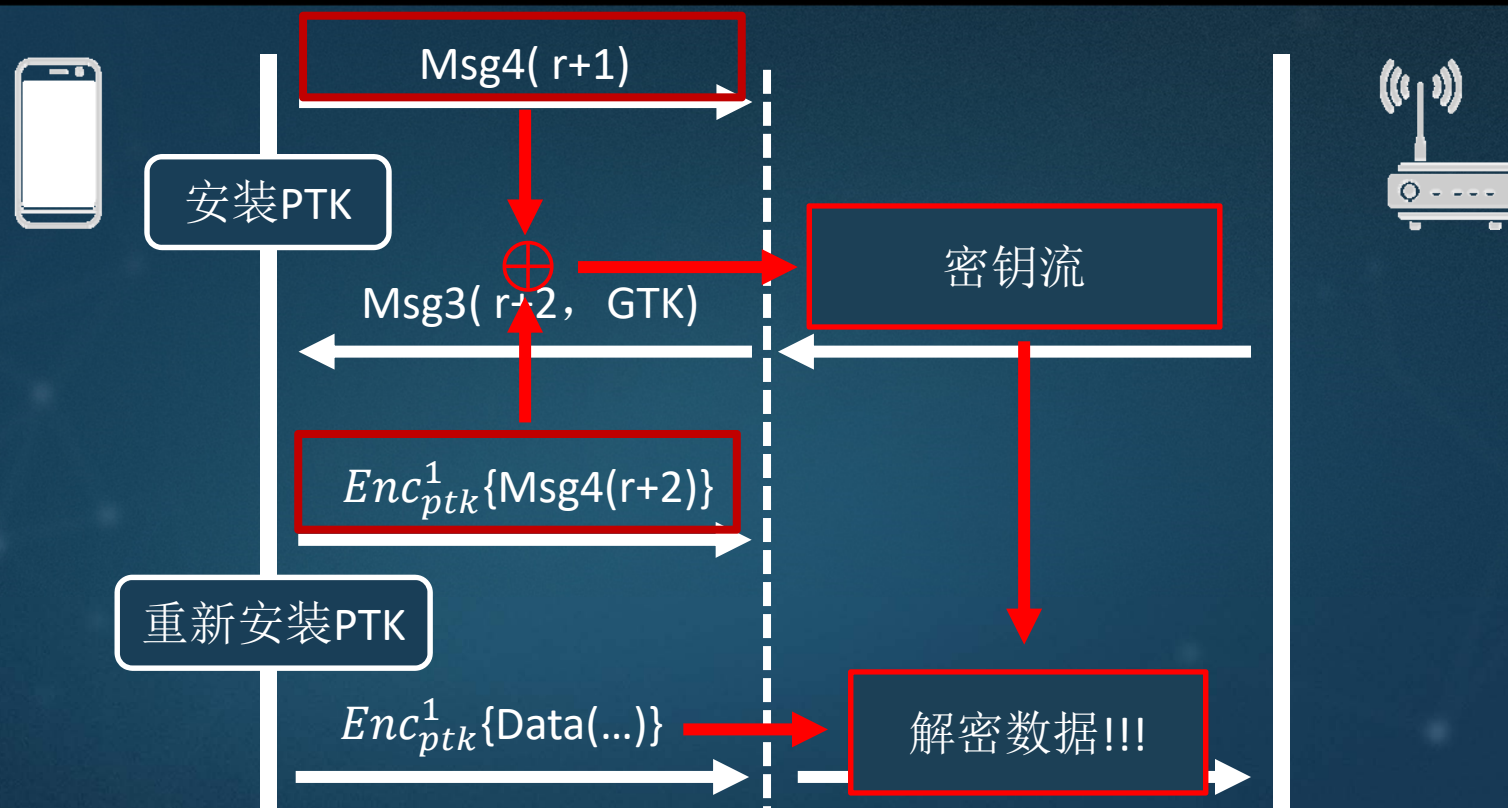
如何攻击Msg3传输



如何攻击Msg3传输



如何攻击Msg3传输



这个攻击到底能做什么???

简而言之，KRACK实现的攻击效果可以分为三类：



~~蹭网?~~

这个攻击到底能做什么???

Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 ^c	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓ ^a	✓ ^a	✓
wpa_supplicant v2.6	✓	✓	✓	✓ ^b	✓ ^b	✓
Android 6.0.1	✓	✗	✓	✓ ^a	✓ ^a	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 ^c	✗	N/A	N/A	N/A	✗	✓
Windows 10 ^c	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

WPA_Supplicant : WI-FI客户端加密认证工具

开源项目，后被谷歌修改后加入Android移动平台。

Linux、Android 6.0、Android Wear 2.0

直接全0密钥代替重装密钥

Windows : 😭 ???



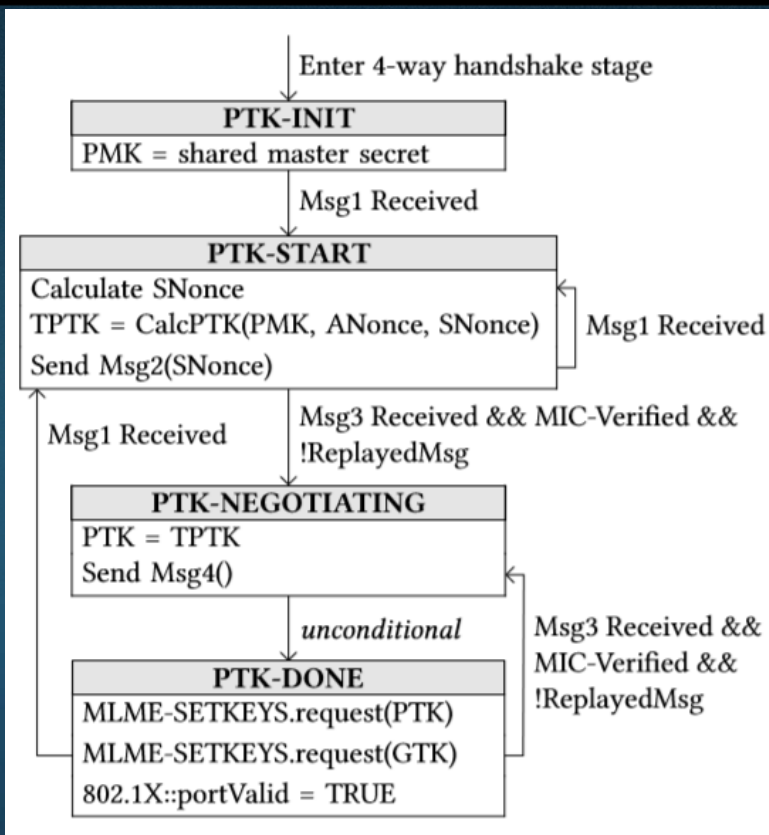
如何对抗KRACK

问题的核心: **nonce重用**

对抗思路:

- 取消nonces和replay counters的重用
- 确保密钥仅被安装一次, 当收到重传的Msg3时给出回应, 但不安装PTK

布尔型变量+状态机



如何对抗KRACK

- 个人用户：

对接入无线的客户端或AP进行更新升级或安装对应补丁，避免Msg3重传，确保密钥仅被安装一次。

- 企业用户：

除了更新设备、加强监管和排查之外，还可以考虑WIPS

对抗KRACK —————> 对抗中间人



思维方式



THANK YOU

欢迎和我一起探讨安全技术
alfredshi@outlook.com



看雪 2018 安全开发者峰会
Kansue 2018 Security Developer Summit