
看雪 2018 安全开发者峰会
Kanxue 2018 Security Developer Summit
2000-2018

从WPA2四次握手看KRACK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

什么是KRACK

- What：KRACK (Key Reinstallation Attack)，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……

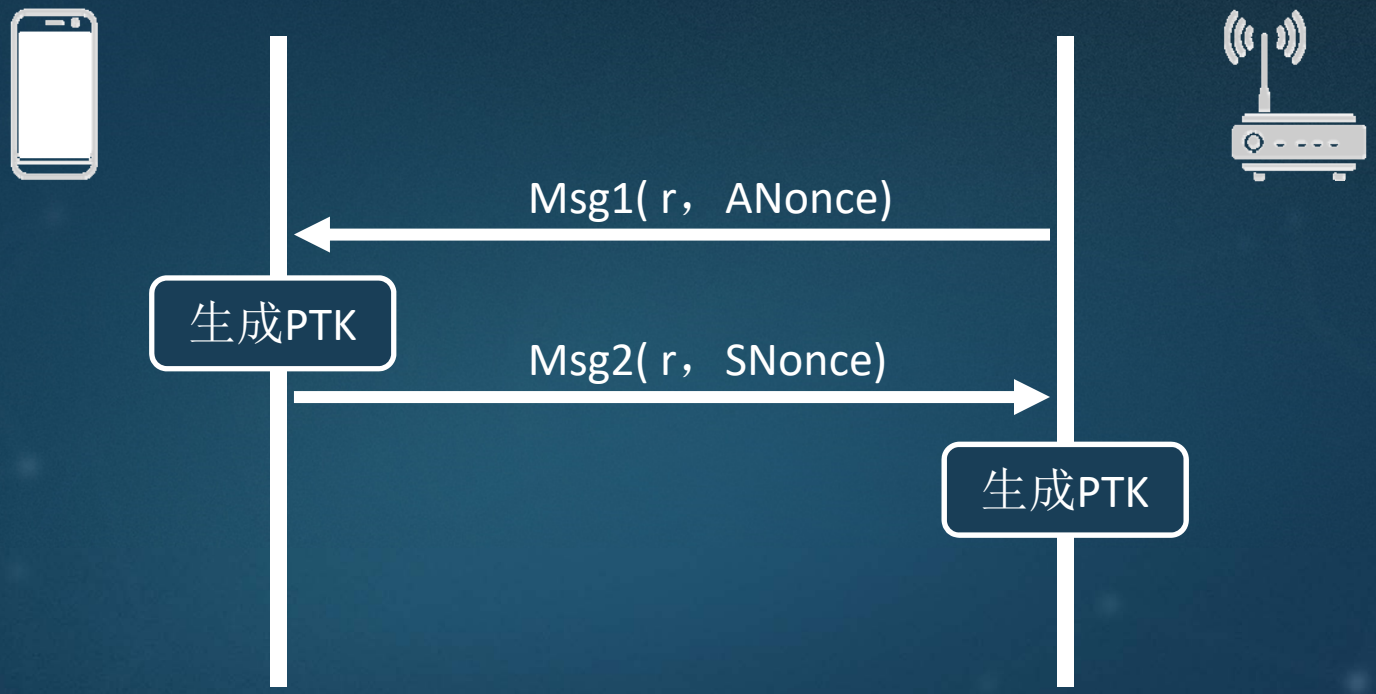
四次握手协议分析

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。

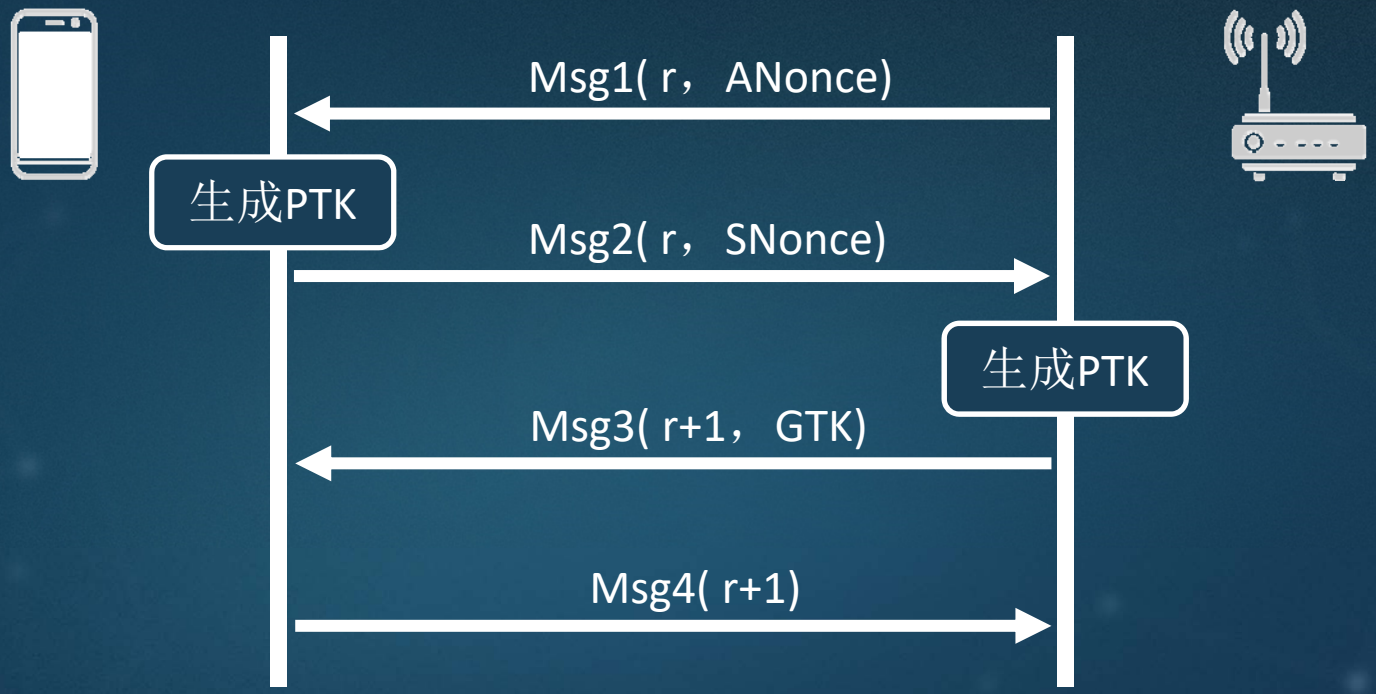
PTK的生成共包含5部分：

- Anonce
- Snonce
- Amac
- Smac
- PMK

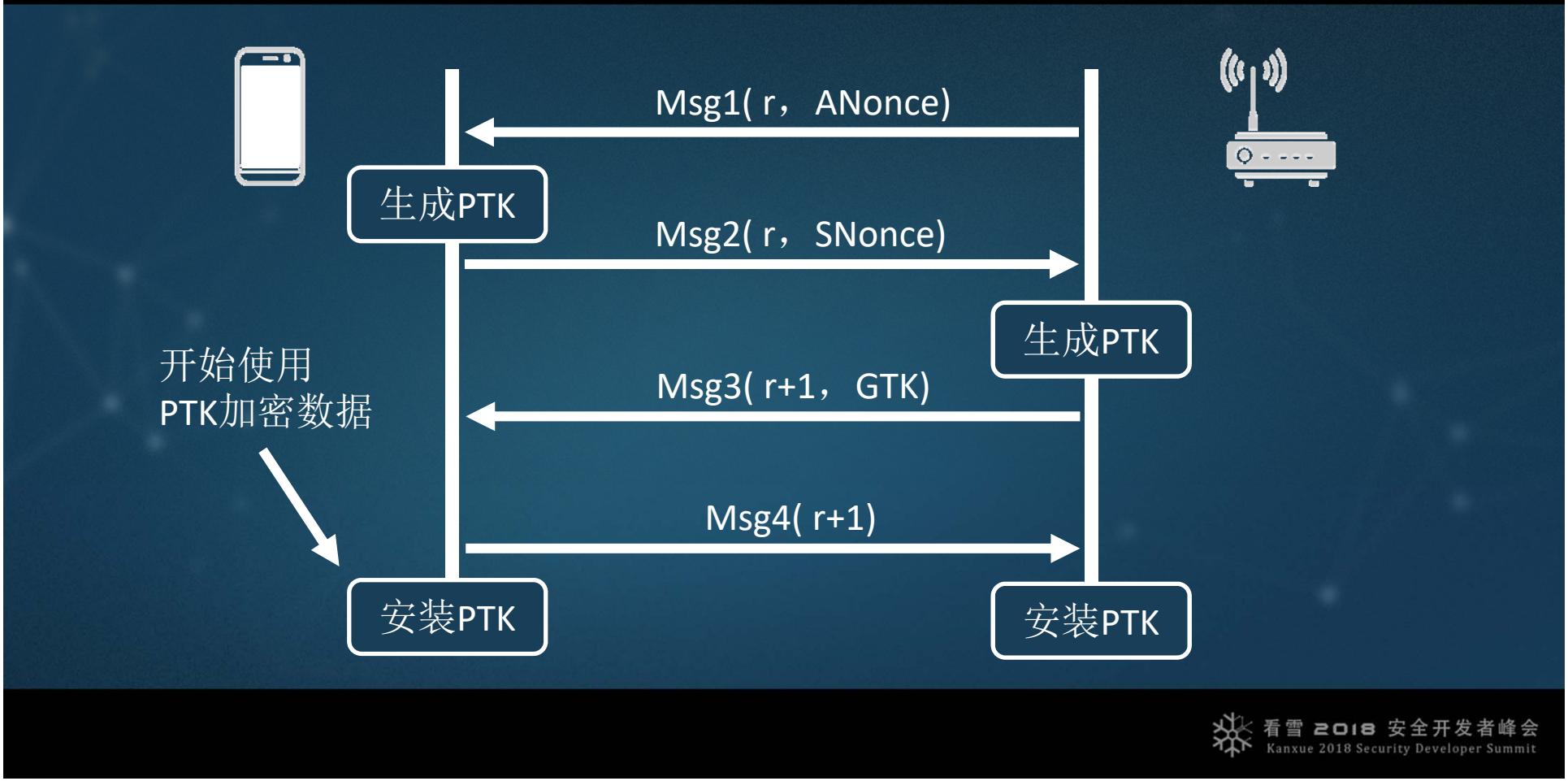
四次握手协议分析



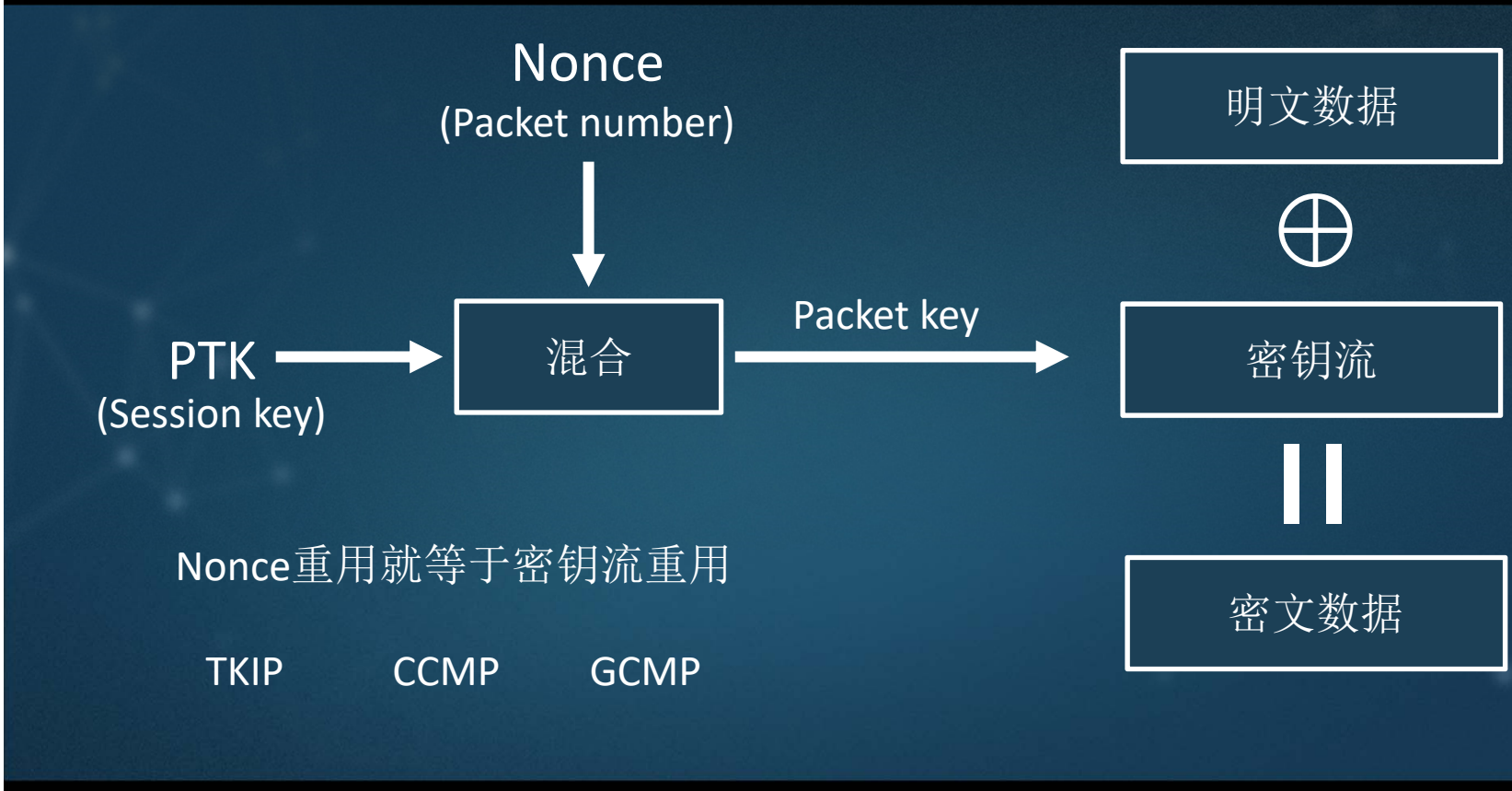
四次握手协议分析



四次握手协议分析


Msg1(r，ANonce)
生成PTK
Msg2(r，SNonce)
生成PTK
开始使用
PTK加密数据
Msg3(r+1，GTK)
Msg4(r+1)
安装PTK
安装PTK

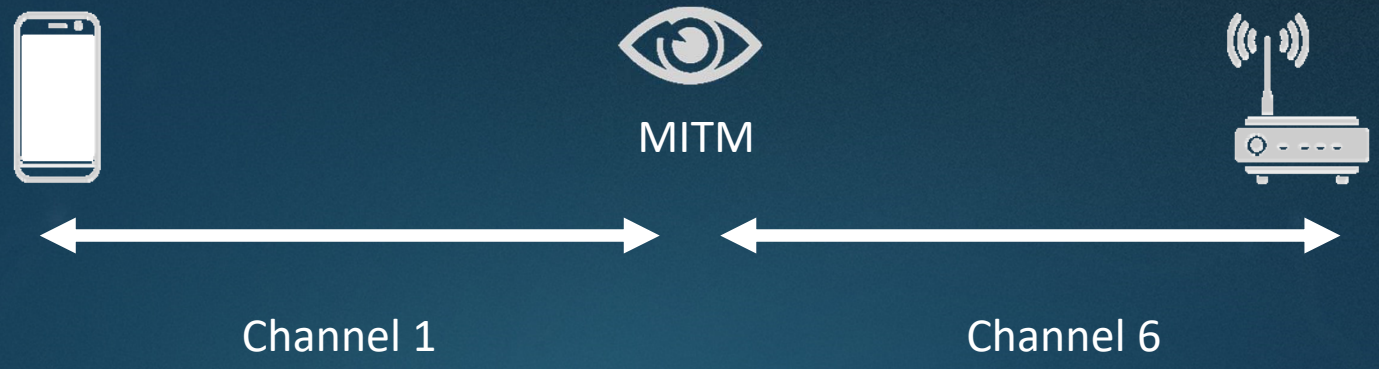
四次握手协议分析



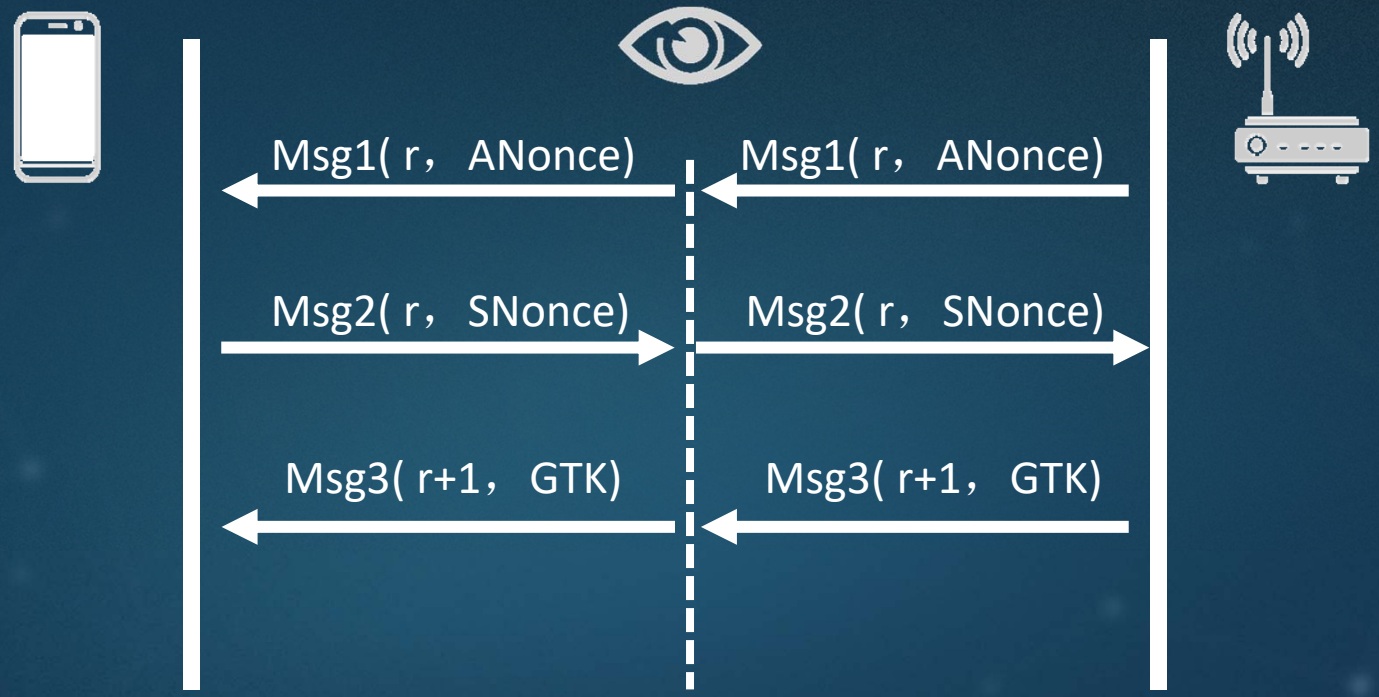
Nonce重用就等于密钥流重用

TKIP　　CCMP　　GCMP

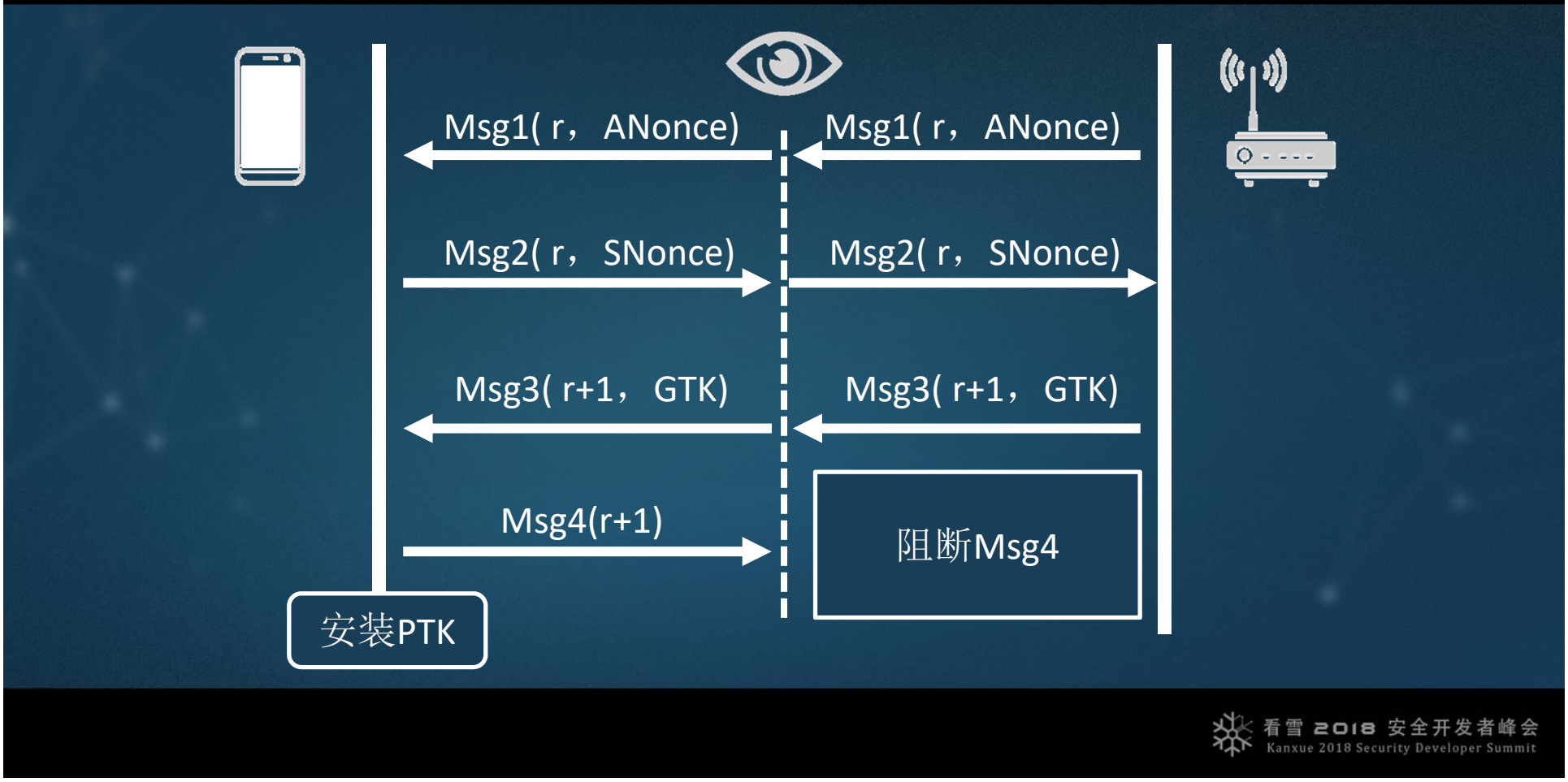
如何攻击Msg3传输



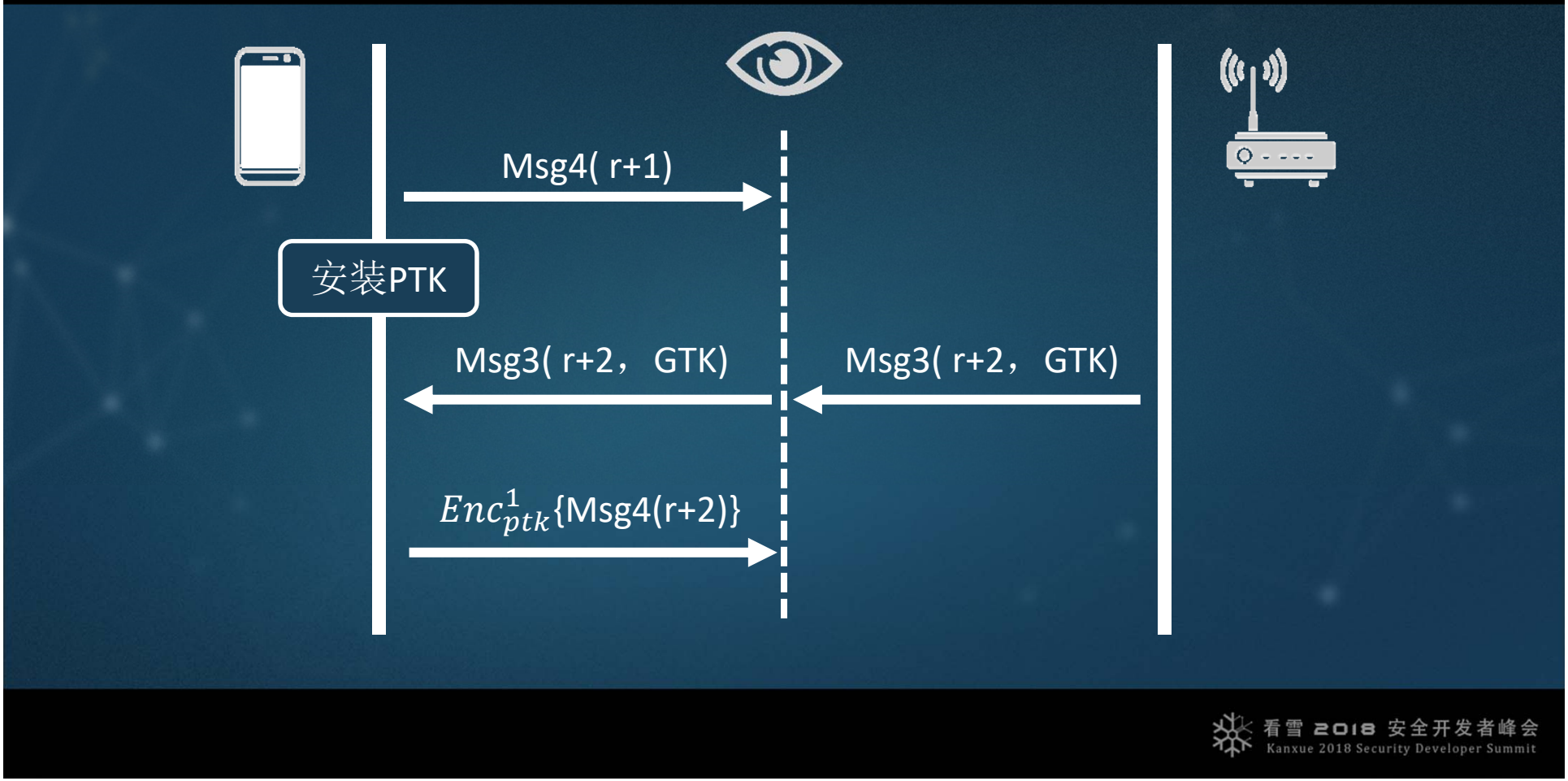
如何攻击Msg3传输


Msg1(r，ANonce)
Msg1(r，ANonce)
Msg2(r，SNonce)
Msg2(r，SNonce)
Msg3(r+1，GTK)
Msg3(r+1，GTK)

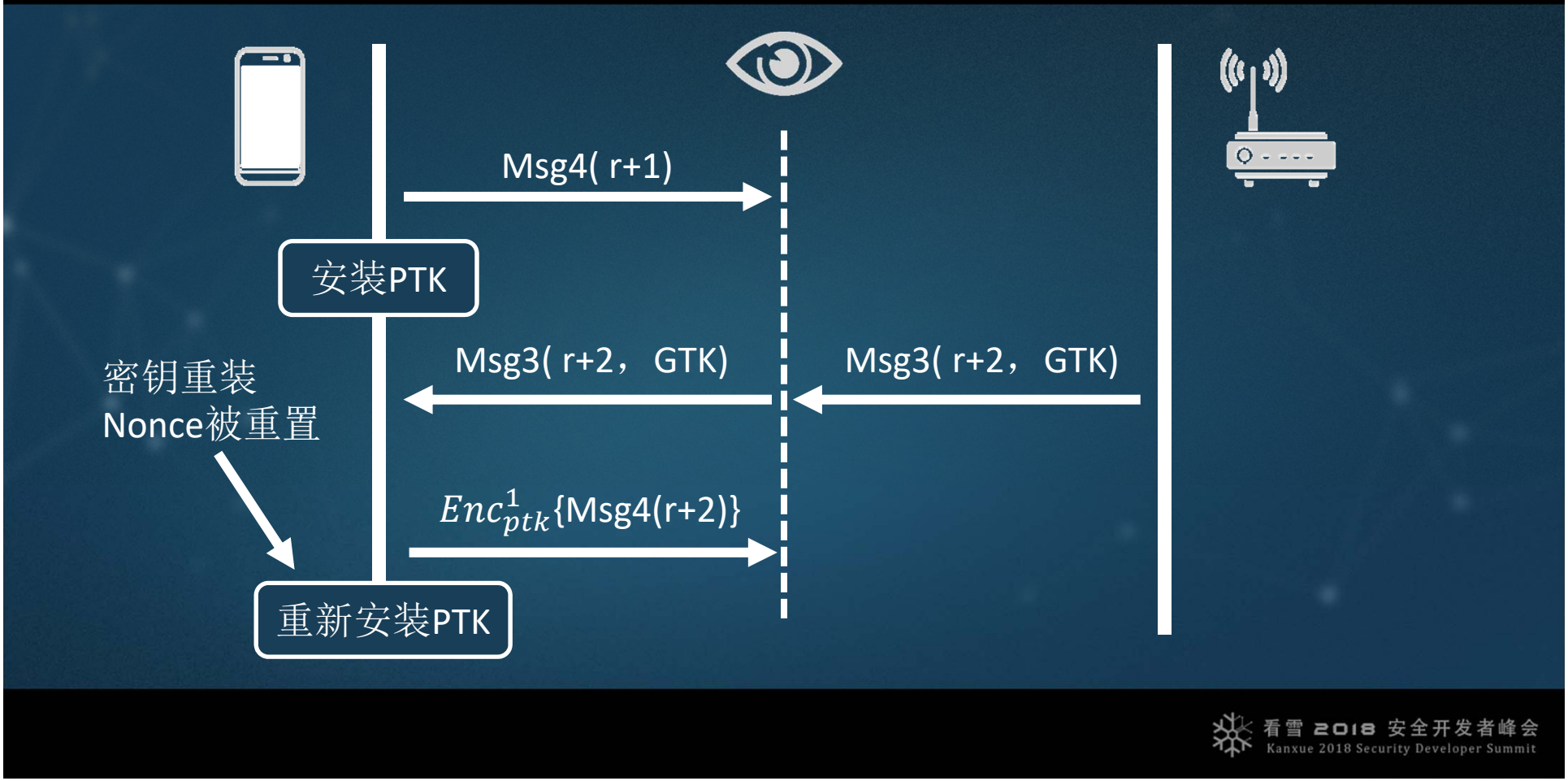
如何攻击Msg3传输


Msg1(r，ANonce)
Msg1(r，ANonce)
Msg2(r，SNonce)
Msg2(r，SNonce)
Msg3(r+1，GTK)
Msg3(r+1，GTK)
Msg4(r+1)
阻断Msg4
安装PTK

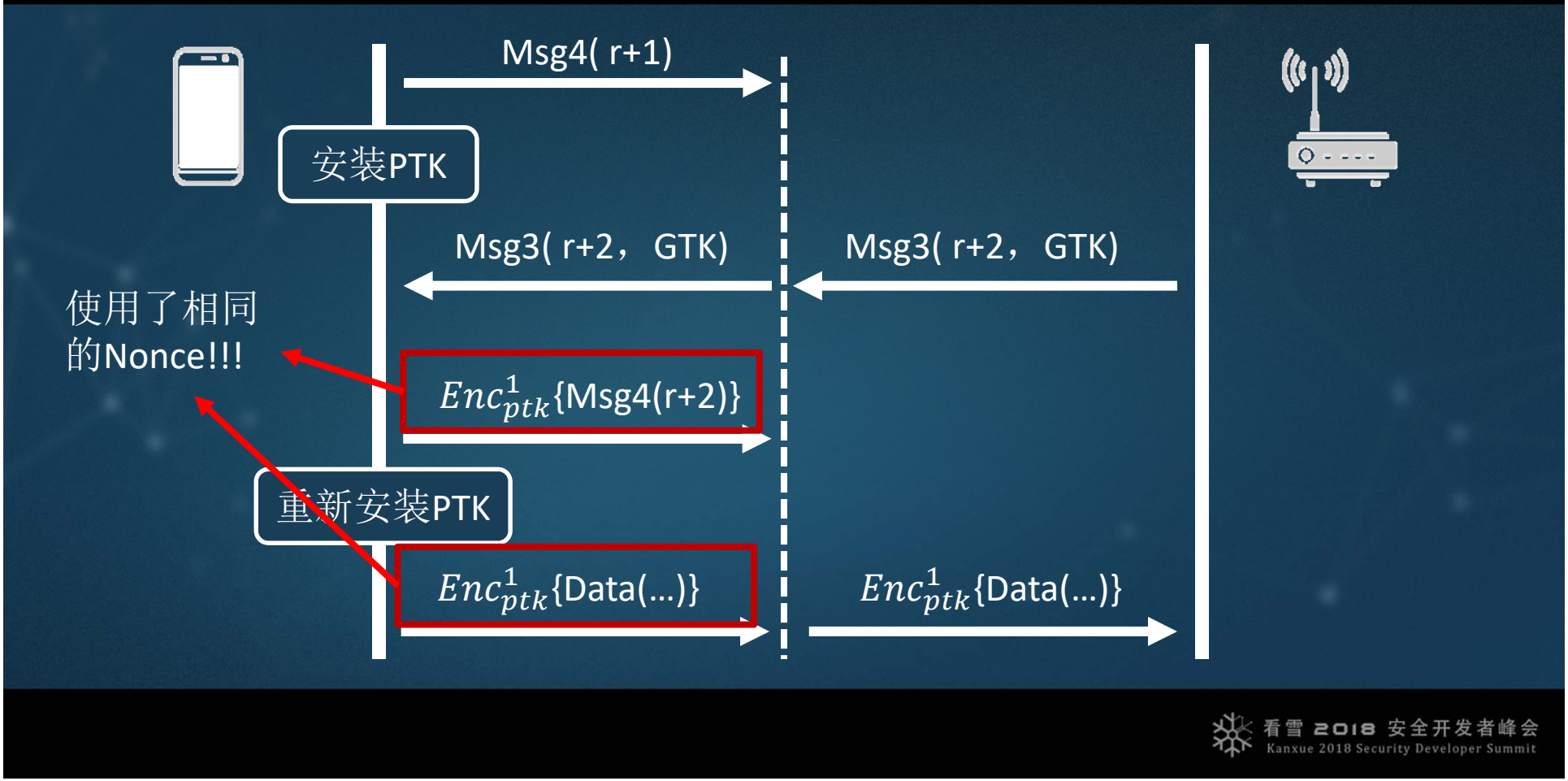
如何攻击Msg3传输



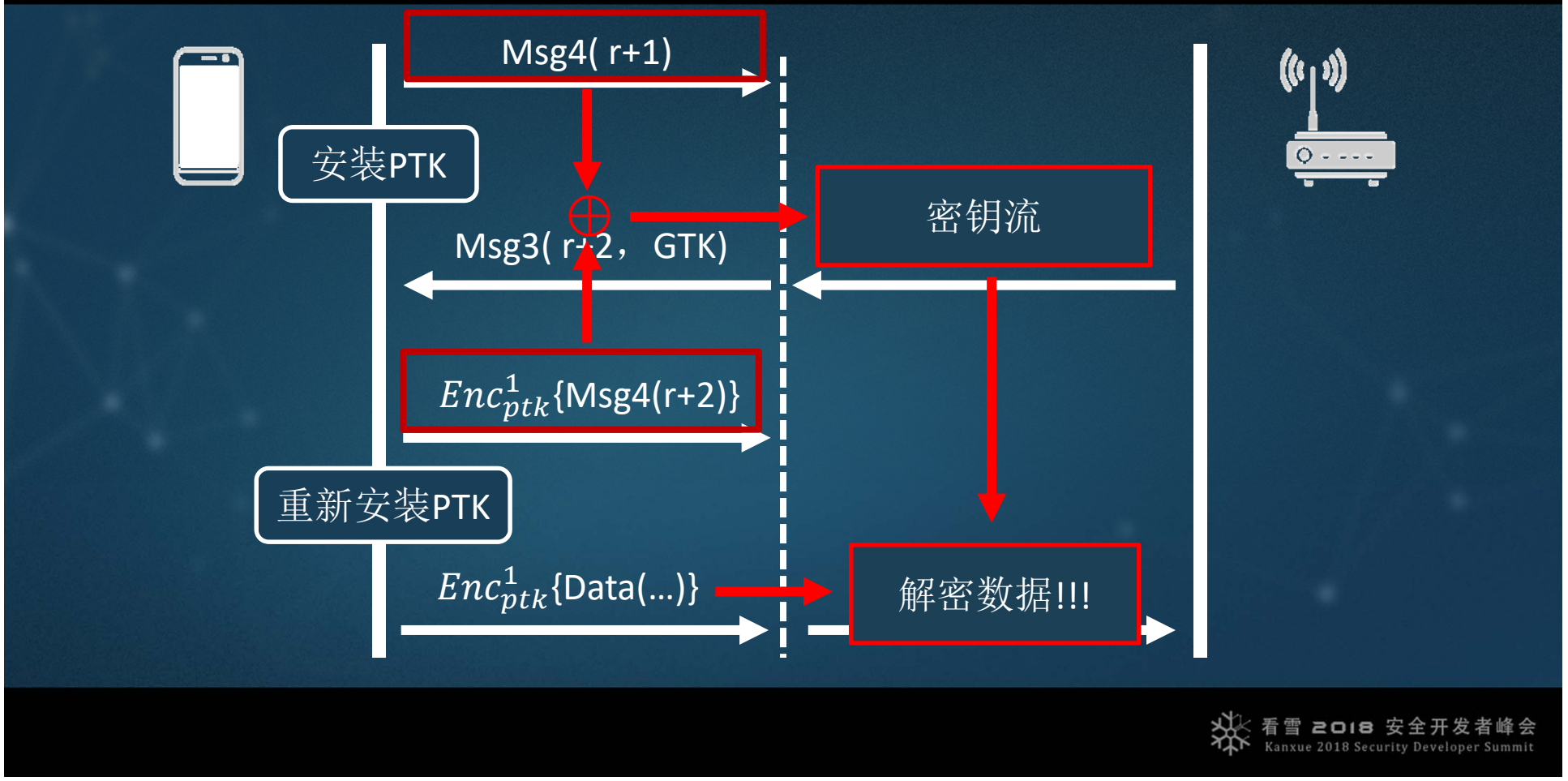
如何攻击Msg3传输


Msg4(r+1)
安装PTK
Msg3(r+2， GTK)
Msg3(r+2， GTK)
密钥重装
Nonce被重置
Enc^1_{ptk}{Msg4(r+2)}
重新安装PTK

如何攻击Msg3传输


Msg4(r+1)
安装PTK
Msg3(r+2， GTK)
Msg3(r+2， GTK)
使用了相同
的Nonce!!!
Enc^1_{ptk}{Msg4(r+2)}
重新安装PTK
Enc^1_{ptk}{Data(...)}
Enc^1_{ptk}{Data(...)}

如何攻击Msg3传输


Msg4(r+1)
安装PTK
密钥流
Msg3(r+2， GTK)
Enc^1_{ptk}{Msg4(r+2)}
重新安装PTK
Enc^1_{ptk}{Data(...)}
解密数据!!!

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：

重放

解密

(AES-)CCMP

伪造

(WPA-)TKIP
GCMP

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

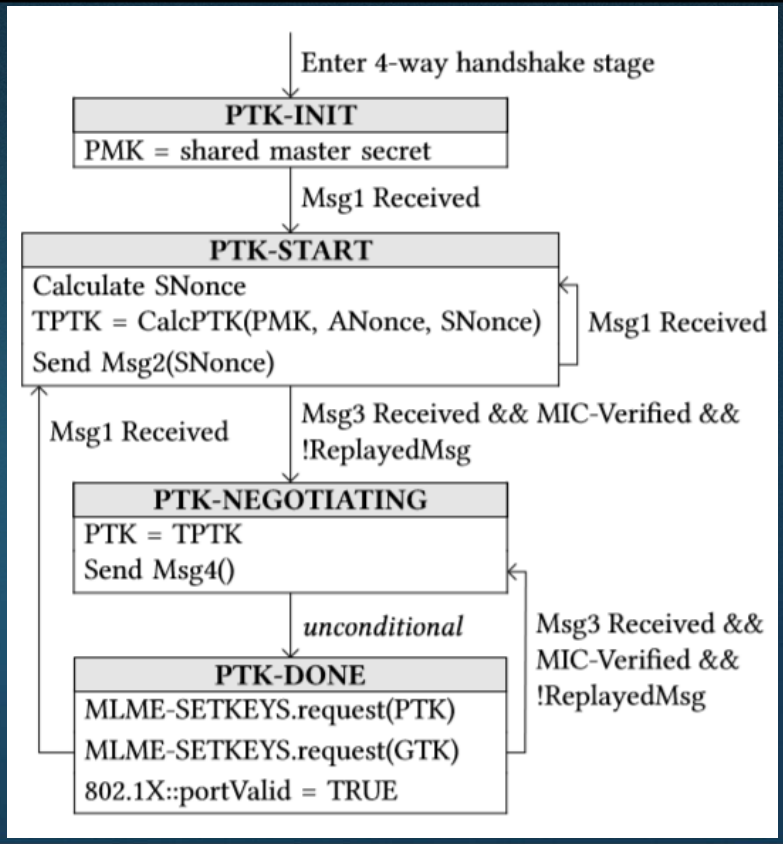
问题的核心：nonce重用

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