WLAN (WPA2) Attack

KRACK

Experience the commitment®

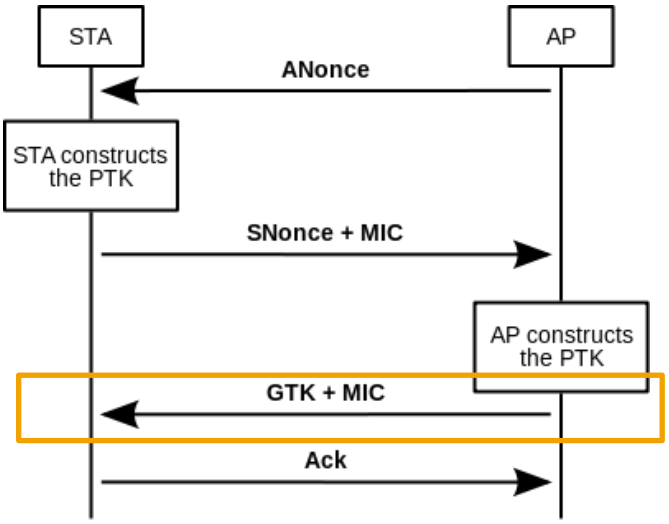
Current
Security Information

The phrase **K**ey **R**einstallation **A**tta**ck** refers to the exploitation of a design vulnerability within the WPA2 protocol that enables interception of a data exchange on a secured connection. The attack compromises the negotiation of a session key when the connection is established.

The first announcement of the attack was via Twitter on 15.10.2017 as a teaser for a presentation at the Conference on Computer and Communications Security (CCS). The security researcher Mathy Vanhoef has published complete details at https://www.krackattacks.com.

BACKGROUND

To secure communications between two participants, in this case the Access Point (AP) and Client Station (STA), the 802.11i standard uses encryption. Whilst negotiating the connection a four-way handshake uses a Pairwise Transient Key (PTK) to exchange and authenticate a shared Group Temporal Key (GTK) with Message Integrity Code (MIC):



(Figure: Steps in session handshake, Source: Wikipedia)

Using this protocol the STA and AP establish a secure connection. To disconnect both participants from the AP's broadcast communication an attempt is made to renew the GTK.

FACT SHEET WIFI-KRACK

Overview of Cybersecurity Solutions:

Strategy, Compliance & Transformation

- Information Security and Emergency Management
- Best Practices according to ISO 27001, ISO 25999, IT-Grundschutz and A-960/1
- Vulnerability Assessments and Penetration Testing
- Risk Management Strategies
- Implementing Security Processes
- Data Privacy and Data Protection
- EU Data Privacy (GDPR)
- Awareness Training

Secure Systems Engineering

- Secure Network Architectures
- Identity & Access Management
- Secure Software Development
- Security Testing

Managed Security Services

- Managed Services
- Monitoring & Alerting
- SIEM as a Service
- Forensics & Malware Analysis
- Advanced Threat Intelligence

de.cgi.com/cybersecurity

THE ATTACK

This is where the attack takes place. By blocking the third step in the handshake (yellow), the attacker prevents the acknowledgement (ACK) in step 4. The client then repeats the step and the attacker can inject a previously negotiated key. To do this the attacker sends the appropriate signal to the client but with greater transmission power than the signal sent from the AP to the client.

The attack is even more critical on several versions of Linux and devices running Android 6.0 and higher as it is possible to force the handshake algorithm to use a default key (Dummy-Key) with a value of “0”.

The attack has to be conducted separately for each client.

Effects of the attack

All devices implementing WLAN Standard 802.11i and 802.11r are affected:

- WPA1 and WPA 2
- Personal and Enterprise Networks, and
- Crypto-Processes WPA-TKIP, AES-CCMP and GCMP

The attack also applies to 802.11r when roaming from AP to AP.

If the attacker is close enough to disrupt the client through greater transmission power then it is possible to:

- Eavesdrop communications between Client and AP
- Inject packets (fake information), if AES-CCMP is not used
- Deactivate encryption for certain Linux distributions

Important

Of note, this attack does not allow the attacker to recover the network password.

AD HOC COUNTERMEASURES

In the event that patching isn’t possible, the following actions can be taken to mitigate the risk:

1. Disable WLAN use for business critical data
2. Encrypt all data transmissions using a VPN or HTTPS
3. Enable AES-CCMP on all Access Points
4. Increase the transmission power required for AP transmissions (forces the attacker to come closer to the AP)

PREVENTATIVE PROTECTION

Other than the above countermeasures it is also possible to monitor the network for rogue APs.

CGI offers this among other services in our comprehensive SOC as a Service offering, because

“Cybersecurity is part of everything we do”.

ABOUT CGI

CGI is a global service provider for IT and business processes. We were founded in 1976 and have a total of 70,000 employees at 400 locations in 40 countries. We are on-site for our customers - with business and IT consulting, system integration and outsourcing services at a top level. We support them in making better use of ongoing investments, while at the same time leveraging new digital technologies and business strategies that enable clients to achieve the best solutions across the entire value chain. Regarding time and budget, we are regularly awarded due to our strict delivery discipline.

To this end, we have consistently achieved more than nine out of ten potential points in customer satisfaction.

YOUR CONTACT PERSON

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

Ettore-Bugatti-Straße 6-14
51149 Köln
T: +49 2203 6993 1050

For more information please contact us at csi@cgi.com
or visit us
de.cgi.com/cybersecurity.