WLAN (WPA2) Attacke **KRACK**

CGI
Experience the commitment®

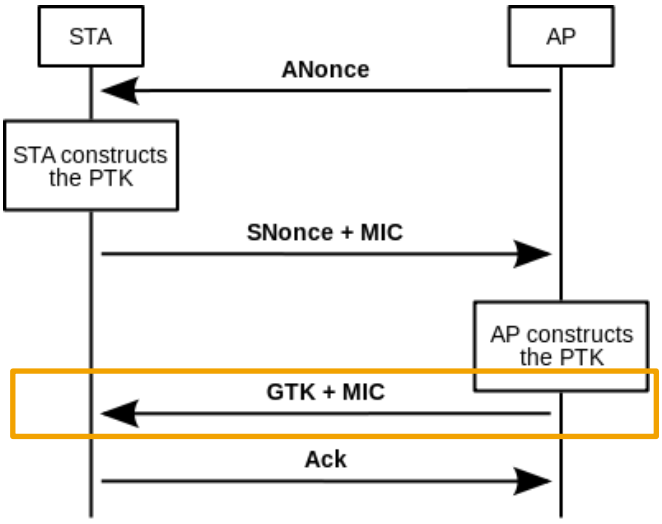
Aktuelle Sicherheitsinformation

Als **K**ey **R**einstallation **A**tta**ck** bezeichnet man das Ausnutzen einer Design-Schwachstelle im WPA2-Protokoll zum Mitlesen des Datenverkehrs einer geschützten Verbindung. Der Angriff kompromittiert dazu das Aushandeln des Session Keys beim Verbindungsaufbau.

Die erste Bekanntgabe der Attacke geschah über Twitter am 15.10.2017 mit einem Teaser bei einer Präsentation zur *Conference on Computer and Communications Security (CCS)*. Der Sicherheitsforscher Mathy Vanhoef veröffentlichte die vollständigen Details unter https://www.krackattacks.com.

HINTERGRUND

Der WLAN-Standard 802.11i nutzt Kryptographie, um die Kommunikation zwischen den Teilnehmern – in diesem Fall Access Point (AP) und Client Station (STA) abzusichern. Hierfür wird bei Verbindungsaufbau mittels eines Vier-Wege-Handshakes über Pairwise Transient Keys (PTK) schließlich der gemeinsame Schlüssel (Group Temporal Key (GTK) mit Message Integrity Code (MIC)) ausgetauscht und wechselseitig überprüft:



(Abbildung: Schritte im Session Handshake, Quelle: Wikipedia)

Der Client und der Access Point können mittels dieses Protokolls eine sichere Kommunikation aufbauen. Um die beiden Kommunikationspartner von der Broadcast-Kommunikation des AP abzukoppeln, wird versucht, den GTK von Zeit zu Zeit zu erneuern.

FACT SHEET WLAN-KRACK

Übersicht der Cybersecurity Lösungen:

Strategy, Compliance & Transformation

- Informationssicherheits- und Notfallmanagement
- Best Practices nach ISO 27001, ISO 25999, IT-Grundschutz und A-960/1
- Vulnerability Assessments und Penetration Testing
- Risikomanagementstrategien
- Aufbau von Sicherheitsprozessen
- Datenschutz und Datensicherheit
- EU-Datenschutzgrundverordnung
- Awareness Training

Secure Systems Engineering

- Sichere Netzarchitekturen
- Identity & Accessmanagement
- Sichere Softwareentwicklung
- Security Testing

Managed Security Services

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

de.cgi.com/cybersecurity

DER ANGRIFF

Genau hier setzt der Angriff ein. Durch Blockade des dritten Schritts im Handshake (gelb) mittels eines Störsignals verhindert der Angreifer die Bestätigung (Ack) in Schritt 4. Der Client führt somit den vorherigen Schritt erneut durch und der Angreifer kann einen zuvor bereits ausgehandelten Schlüssel erneut einspielen. Dazu sendet der Angreifer ein entsprechendes Signal an den Client. Dieses Signal muss eine höhere Sendeleistung aufweisen, als das Signal des Access Points an den Client.

Bei einigen Linux-Versionen und Geräten mit Android 6.0 und höher ist der Angriff umso kritischer, da es möglich ist, den Handshake-Algorithmus zu zwingen, einen Default-Key (Dummy-Key) mit dem Wert „0“ zu nutzen.

Der Angriff muss für jeden Client separat durchgeführt werden.

Auswirkungen des Angriffs

Betroffen davon sind quasi alle Geräte mit WLAN-Standard 802.11i und r:

- WPA1 und WPA2,
- Personal und Enterprise Networks und
- Krypto-Verfahren WPA-TKIP, AES-CCMP und GCMP

Analog gilt der Angriff für 802.11r im Roaming von AP zu AP.

Wenn der Angreifer nah genug ist, um den Client durch die stärkere Sendeleistung zu stören, kann er folgende Angriffe durchführen:

- Abhören der Kommunikation zwischen Client und Access Point
- Einspielen von Paketen in die Kommunikation (Fälschung der Informationen), falls nicht AES-CCMP verwendet wird
- gewisse Linux-Distributionen: de facto Ausschalten der Verschlüsselung

Abgrenzung

Ein Angreifer kann hierbei nicht den im Client und AP konfigurierten Netzwerkschlüssel für das entsprechende Netz auslesen.

AD HOC GEGENMASSNAHMEN

Sollte ein Patchen von Systemen nicht zeitnah möglich sein, gibt es folgende Möglichkeiten um das Risiko zu reduzieren:

1. Verzicht auf WLAN-Nutzung bei unternehmenskritischen Daten
2. Verschlüsselung des gesamten, über das Netz übertragenen Traffics mittels VPN oder HTTPS
3. Einschalten von AES-CCMP bei allen Access Points
4. Erhöhung der AP-Sendeleistung (zwingt Angreifer näher an den AP)

PRÄVENTIVER SCHUTZ

Neben den beschriebenen Gegenmaßnahmen, die auch präventiv wirken, kann eine Überwachung des Netzes auf nichtgenehmigte AP erfolgen.

CGI bietet einen solchen Dienst im Rahmen ihres komplett deutschsprachigen SOC as a Service-Angebotes an, denn

“Cybersecurity is part of everything we do”.

ÜBER CGI

Mit 70.000 Mitarbeitern an 400 Standorten in 40 Ländern übernimmt CGI vor Ort Verantwortung für den Erfolg seiner Kunden und bietet ihnen gleichzeitig globale Lieferfähigkeit. Seit unserer Gründung im Jahr 1976 pflegen wir eine strikte Lieferdisziplin, dank der unsere Projekte in Bezug auf Zeit- und Budgettreue in der Branche führend sind. Mit Business und IT Consulting, Systemintegration sowie Outsourcing Services auf höchstem Niveau unterstützt CGI seine Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue Technologie- und Business-Strategien einzusetzen, mit denen sich optimale Lösungen für die gesamte Wertschöpfungskette erreichen lassen.

Das Resultat unseres Commitments zeigt sich im gemessenen Kundenzufriedenheitswert, der in den vergangenen zehn Jahren durchgängig mehr als 9 von 10 möglichen Punkten betrug.

IHR ANSPRECHPARTNER

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

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

Für weitere Informationen kontaktieren Sie uns unter csi@cgi.com oder besuchen Sie uns auf de.cgi.com/cybersecurity.