A. Einleitung

A.00 WPA2 Krack?

KRACK ist die Abkürzung für Key Reinstallation Attack. Es handelt sich um einen Angreifer, der einen einmaligen Schlüssel wiederverwendet, der zur Verfügung gestellt wird, wenn ein Client-Gerät versucht, einem Wi-Fi-Netzwerk beizutreten. Auf diese Weise könnte der Hacker in die Lage versetzt werden, Informationen zu entschlüsseln, die zwischen dem Access Point und dem Client-Gerät ausgetauscht werden, was dazu führen könnte, dass persönliche Daten wie Kreditkartennummern, Nachrichten und Passwörter bei weiteren unverschlüsselten Sitzungen (ohne Verwendung von https, VPN usw.) offengelegt werden.

A.01 Ursachen

Schwachstelle im Protokoll 802.11r (Fast BSS Transition) selbst, wo das Protokoll nicht ausreichend vor böswilligen Angriffen schützt.

A.02 Betroffene Geräte

Clients und AP
Lieferantenunabhängig

A.03 Voraussetzungen

Nicht aktualisierte Geräte
Angreifer muss sich in der Nähe der Zielgeräte befinden.

A.04 Risikobewertung

Mittleres Risiko (relativ hohe Anforderungen an Technik und Wissen, nur Lesezugriff)
Nachdem eine gehackte Sitzung geschlossen wurde, muss der Angreifer den Prozess erneut starten.

A.05 Detaillierte Beschreibung

Der Angriff bezieht sich auf verschiedene Schlüsselhandshakes, die zwischen dem Wi Fi Client und dem AP (Authenticator) verwendet werden, um Verschlüsselungsschlüssel abzuleiten und zu installieren. Verschiedene Implementierungen reagieren auf unterschiedliche Art und Weise, wenn „Handshake“ Nachrichten erneut übertragen werden - einige dieser Antworten berücksichtigen nicht, dass die erneute Übertragung auf die Aktion eines Angreifers (Mann in der Mitte) und nicht auf einen einfachen Paketverlust zurückzuführen ist, da diese Schwachstellen mit Implementierungsfehlern zusammenhängen. Eine Schwachstelle bezieht sich auf 802.11r (auch bekannt als Fast BSS Transition). Dieser Angriff liegt im Protokoll selbst, wo das Protokoll nicht ausreichend vor böswilligen Angriffen schützen.
Eine ausführliche Beschreibung des WPA KRACK finden Sie hier:
https://papers.mathyvanhoef.com/ccs2017.pdf

B. Wie löst man das Problem?

B.01 Allgemeines Vorgehen

WPA2 Krack ist nur ein Beispiel dafür, wie Angreifer versuchen, Zugang zu sensiblen und geheimen Informationen von Unternehmen zu erhalten. Dieses kann einen großen Einfluss auf das Geschäft und die Finanzen des Unternehmens haben.
Daher sollte die Unternehmens-IT in zwei Richtungen handeln:
B.1 Erkennung von Schwachstellen, die Abwehr von Angriffen und die Durchsetzung von IT-Richtlinien, verbunden mit einem entsprechenden Compliance-Reporting
B.2 Sobald ein Angriff erkannt worden ist, sind entsprechende technische Maßnahmen zum Upgrade ALLER betroffenen Geräte (HW und / oder SW) zu ergreifen oder die entsprechenden Geräte sind vom Netzwerkzugang auszuschließen.
Für den WPA2 Krack müssen entsprechende SW-Patches auf ALLEN Clients und APs installiert werden, unabhängig vom Anbieter.

B.10 Erkennen, Verhindern, Richtlinieneinhaltung und Berichtswesen: Installieren Sie HPE-Aruba RFprotect™ und HPE-Aruba ClearPass™.

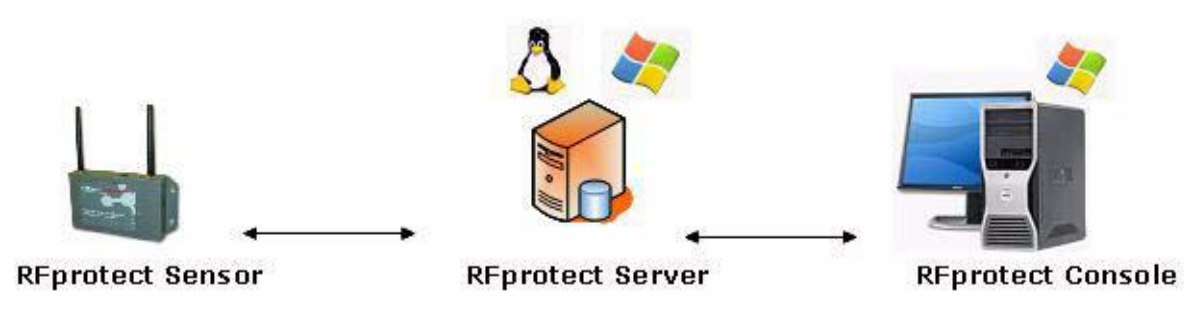
RFprotect™ und ClearPass™ erkennen Schwachstellen, verhindern Angriffe, setzen Richtlinien durch und erstellt Compliance-Berichte. Es schützt Ihr drahtloses Netzwerk gegen vorsätzliches Eindringen und gegen Schwachstellen, die versehentlich durch falsch konfigurierte Netzwerkgeräte verursacht wurden. Es verhindert Denial-of-Service-Angriffe und Man-in-the-Middle-Angriffe wie WPA und WPA2 -Sicherheitslücken und mildert Over-the-Air-Sicherheitsbedrohungen.
Beide Lösungen arbeiten unabhängig voneinander, können aber auch gemeinsam eingesetzt werden.

B.11 Was ist HPE- Aruba RFprotect™?

RFprotect™ schützt Ihr gesamtes Netzwerk vor unautorisierten Wi-Fi-Clients und Ad-hoc-Netzwerken, indem kontinuierlich die RF-Umgebung gescannt wird, forensische Daten zentral ausgewertet werden, Hackergeräte aktiv vom Netzzugriff ausschließt und Gerätekonfigurationen sperrt.
Das RFprotect™ Distributed System besteht aus den folgenden Komponenten:

- Sensor - Ein spezielles Gerät, das eine kontinuierliche RF-Überwachung und Datenaggregation ermöglicht, um die Sicherheit Ihres Netzwerks zu gewährleisten. Sensoren empfangen und analysieren 802.11-Pakete, analysieren Daten und senden verarbeitete Daten an den Server.
- Server – Verwaltungssoftware unter Windows oder Linux, die Daten von Sensoren analysiert, speichert und integriert, Warnungen generiert und eine Datenbank für Konsolenbenutzer verwaltet.
- Konsole (Client) - Win32-Software-Anwendung, beinhaltet alle Tools zum Anzeigen und Verwalten der vom Server und den Sensoren von RFprotect™ bereitgestellten Informationen, bietet verschiedene Ansichten der drahtlosen Aktivitäten, Sicherheitswarnungen und RF-Umgebungsanalysen.

- AutoReports - Windows-Softwareanwendung, die es Ihnen ermöglicht, automatisch generierte RF-Sicherheits-, Leistungs- und Statusberichte zu planen, um sicherzustellen, dass Ihr drahtloses Netzwerk sicher funktioniert und den gesetzlichen Vorschriften entspricht.



RFprotect™ kann für eine herstellerunabhängige Wi-Fi-Netzwerkinfrastruktur eingesetzt werden

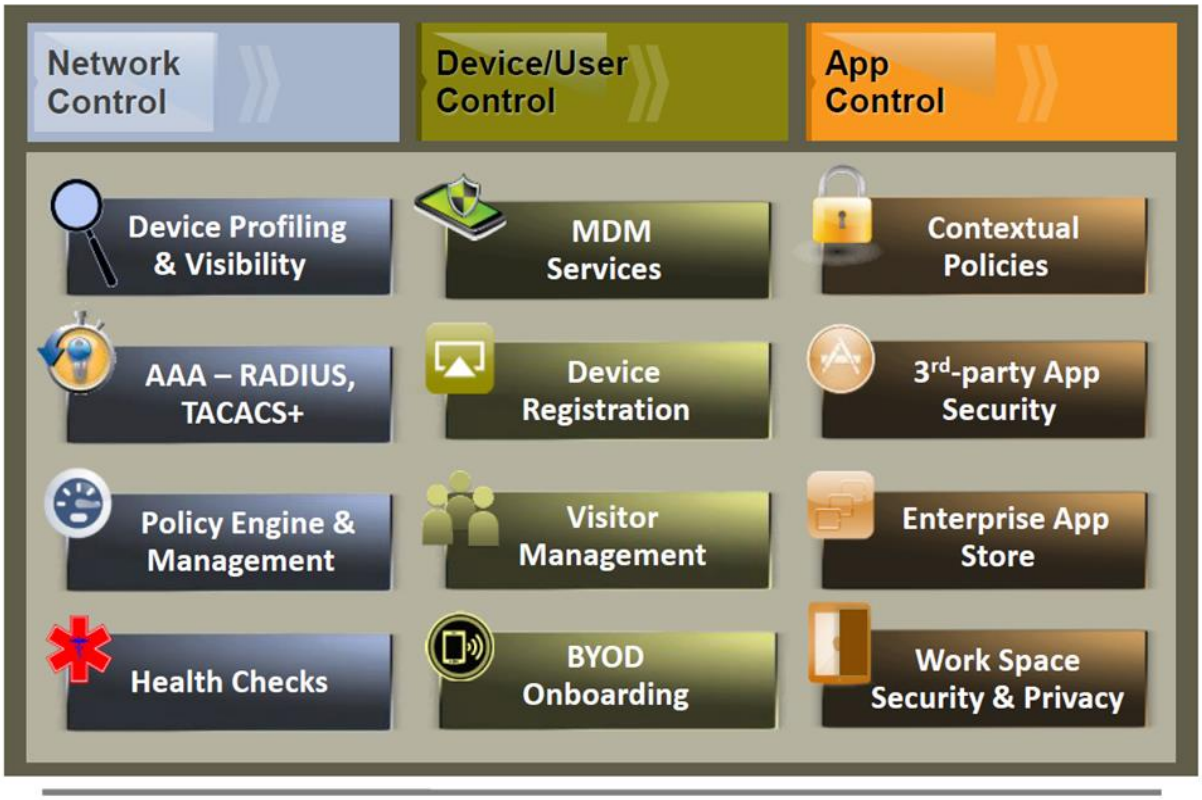
Um die Risiken für Ihr Netzwerk zu minimieren, bieten wir Ihnen unsere HPE- Aruba RFprotect™ Produkt-Lizenz als 30 Tage Free-Trail-Version an. Nach Ablauf der 30-tägigen Testzeit unterbreiten wir Ihnen gerne ein kommerzielles Angebot. Bitte kontaktieren Sie unser Sales Team
sales@aeroaccess.de

Hinweis: Abhängig von der installierten Infrastruktur sind zwei verschiedene Testszenarien möglich.

Szenario 1: Ihr Netzwerk besteht bereits aus HPE- Aruba HW AP's. Es wird lediglich eine RFprotect™ Software-Testversion benötigt. RFprotect™ Sensoren sind in den HPE- Aruba AP's verfügbar.
Szenario 2: Ihr Netzwerk besteht nicht aus HPE- Aruba HW AP's. Als Ergänzung zu einer RFprotect™ Software-Testversion müssen einige RFprotect™ Sensoren eingesetzt werden. Die Aeroaccess GmbH wird Ihnen bis zu 15 HPE- Aruba HW AP's kostenfrei für die Zeit des Tests zur Verfügung stellen, die als Sensoren fungieren würden.

B.12 Was ist der HPE- Aruba ClearPass?

HPE-Aruba ClearPass bietet Transparenz, Kontrolle und Sicherheitsmechanismen für Unternehmen, die „überall, zu jeder Zeit und mit jedem Gerät arbeiten“.
Mit ClearPass kann die IT-Abteilung den Netzwerkzugriff und die Richtlinien verwalten, Geräte einbinden und verwalten, Gastbenutzer zulassen, den Gerätezustand beurteilen und sogar mobile Arbeitsanwendungen sichern, verteilen und verwalten.
Eine Übersicht über die Möglichkeiten von HPE-Aruba ClearPass finden Sie auf der untenstehenden Folie:



Aruba ClearPass™ kann für eine herstellerunabhängige Wi-Fi-Netzwerkinfrastruktur eingesetzt werden

Um die Risiken für Ihr Netzwerk zu minimieren, bieten wir Ihnen unsere HPE- Aruba ClearPass™ Produkt als 30 Tage Free-Trail-Version an. Nach Ablauf der 30-tägigen Testzeit unterbreiten wir Ihnen gerne ein kommerzielles Angebot. Bitte kontaktieren Sie unser Sales Team

sales@aeroaccess.de

B.20 Rüsten Sie den Aruba Controller mit dem Aruba Fix auf.

Die Sicherheitslücken wurden in den folgenden ArubaOS-Patch-Releases behoben, die alle sofort zum Download zur Verfügung stehen:

- 6.3.1.25
- 6.4.4.16
- 6.5.1.9
- 6.5.3.3
- 6.5.4.2
- 8.1.0.4

Für detaillierte Beschreibungen und Anweisungen zu den verschiedenen verfügbaren Upgrade-Verfahren wenden Sie sich bitte an unser Support-Team support@aeroaccess.de.

Hier erhalten Sie sofortige und hochqualifizierte professionelle Unterstützung. Der Support kann als On-Call-Support mit einfachen Anweisungen für das Upgrade oder als Full-Service angeboten werden.

B.21 Aktualisieren Sie Ihre Aruba AP

Die Schwachstellen wurden in den folgenden InstantOS-Patch-Releases behoben, die alle sofort zum Download zur Verfügung stehen:

- 4.2.4.9
- 4.3.1.6
- 6.5.3.3
- 6.5.4.3

Für detaillierte Beschreibungen und Anweisungen zu den verschiedenen verfügbaren Upgrade-Verfahren wenden Sie sich bitte an unser Support-Team
support@aeroaccess.de

Hier erhalten Sie sofortige und hochqualifizierte professionelle Unterstützung. Der Support kann als On-Call-Support mit einfachen Anweisungen für das Upgrade oder als Full-Service angeboten werden.

B.30 Aktualisieren Sie Ihre Clientgeräte

Es ist wichtig, dass das gesamte Netzwerk einschließlich ALLER Clients sicher ist. Daher müssen auf allen Clients Patches installiert werden, um WPA KRACK zu lösen.
Bitte besuchen Sie die Supportseiten der Lieferanten für die entsprechenden Informationen und Updates oder kontaktieren Sie sie mit einem Brief / E-Mail ähnlich dem unten eingefügten Vorschlag :

Sehr geehrte Damen und Herren,

Wie Sie wissen, gibt es ein Problem mit dem WPA-2 Schlüssel, der als WPA-2 KRACK bekannt ist. Da wir Ihr Produkt über WLAN nutzen, ist es uns wichtig, die Firmware entsprechend upzudaten. Können Sie uns ein Update oder eine andere Lösung zur Verfügung stellen?

Mit freundlichen Grüßen,

Eine Herausforderung für die Unternehmens-IT könnte die Frage sein, wie man alle Client-Typen und deren Typnummern ermitteln und erkennen kann, wie diese auf das Netzwerk zugreifen. Abhängig von den verfügbaren Netzwerkmanagementsystemen gibt es verschiedene Möglichkeiten.

Aeroaccess steht Ihnen gerne mit Rat und Tat zur Seite. Bitte kontaktieren Sie unser Support-Team über
support@aeroaccess.de