| Version | Content | Datum | Autor |
|---|---|---|---|
| 0.1 RKU | Creator for the document | 21.11.2017 | rku/ybe |


| A. | Introduction | Version |
|---|---|---|
| A.00 | WPA2 Krack? | 0.1 |
| A.01 | Reason | 0.1 |
| A.02 | Effected Devices | 0.1 |
| A.03 | Prerequisites | 0.1 |
| A.04 | Risk assessment | 0.1 |
| A.05 | Detailed description | 0.2 |
| B. | How to solve the Issue | 0.1 |
| B.01 | General approach | 0.1 |
| B.10 | Detecting, Prevention, Policy enforcing and Reporting: Install HPE-Aruba RFprotect™ and HPE- Aruba ClearPass | 0.1 |
| B.11 | What is the HPE- Aruba RFprotect™ product? | 0.1 |
| B.12 | What is the HPE- Aruba ClearPass? | 0.1 |
| B.20 | Upgrade the Aruba Controller with the Aruba Fix | 0.1 |
| B.21 | Upgrade your Aruba IAP | 0.1 |
| B.30 | Upgrade your Clients | 0.1 |

# A. Introduction

## A.00 WPA2 Krack?

KRACK is an acronym for Key Reinstallation Attack. It involves an attacker reusing a one-time key that's provided when a client device attempts to join a Wi-Fi network. Doing so, the hacker could be enabled to decrypt information being exchanged between the access point and the client device, which could leave personal details like credit card numbers, messages and passwords exposed on further un-crypted sessions (not using https, VPN etc.).

## A.01 Reason

Vulnerability in the protocol 802.11r (Fast BSS Transition) itself, where the protocol does not adequately protect against malicious attack

## A.02 Effected Devices

Clients and AP
Supplier independent

## A.03 Prerequisites

Not updated devices
Attacker is located close to the attacked devices

## A.04 Risk assessment

Medium risk (relatively high technical and knowledge requirements, Read-Access only)
After a hacked session is closed, the attacker has to start the process again

## A.05 Detailed description

The vulnerabilities are related to different key handshakes, used between the Wi Fi supplicant (client) and the AP (authenticator) to derive and install encryption keys.
Different implementations respond in different ways when keying handshake messages are retransmitted – some of these responses did not anticipate that the retransmission may be due to an attacker's action (Man in the middle) rather than simple packet loss, because these vulnerabilities are related to implementation flaws.
One vulnerability is related to 802.11r (also known as Fast BSS Transition).
This vulnerability is in the protocol itself, where the protocol does not adequately protect against malicious attack.
A complete description for the WPA KRACK you can find here:
https://papers.mathyvanhoef.com/ccs2017.pdf

# B. How to solve the Issue

## B.01 General approach

WPA2 Krack is only one example, how attackers are trying to get access to companies sensible and secret information. It may have huge influence on company's business and finance.
Therefore, company's IT should act one two points:
B.1 take care for detecting vulnerabilities, preventing attacks, enforcing policy accomplished by an according compliance reporting
B.2 Once an attack is detected, take according technical measures in upgrading ALL effected devices (HW and / or SW) or exclude the device from network access

For WPA2 Krack according SW patches have to be installed on ALL clients and AP, independently of the supplier

## B.10 Detecting, Prevention, Policy enforcing and Reporting: Install HPE-Aruba RFprotect™ and HPE-Aruba ClearPass

RFprotect™ and ClearPass detects vulnerabilities, prevents attacks, enforces policy, and ensures compliance reporting. It secures your wireless network against intrusions that are perpetrated intentionally and from vulnerabilities caused accidentally through misconfigured network equipment. It prevents denial-of-service and man-in-the-middle attacks like WPA security vulnerabilities and mitigates over-the-air security threats.
Both solutions are working independently from each other but could also deployed together.

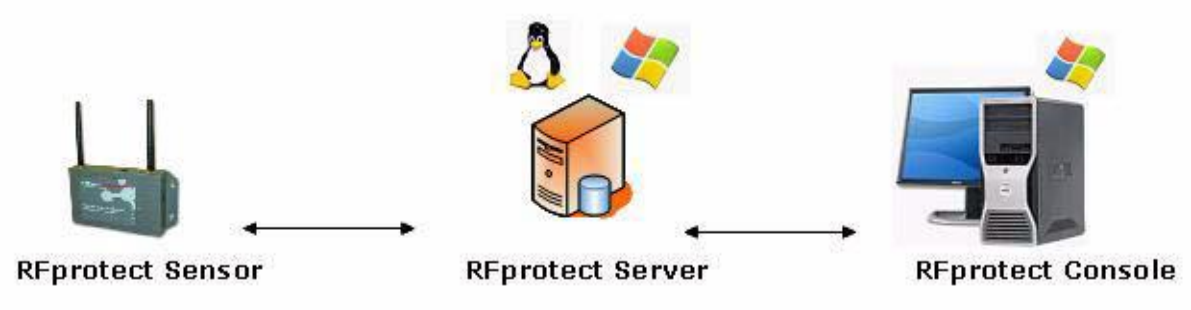
## B.11What is the HPE- Aruba RFprotect™ product?

The RFprotect™ protect your entire network against unauthorized Wi-Fi clients and ad hoc networks by continuously scanning the RF environment, centrally evaluating forensic data, actively containing rogue devices, and locking-down device configurations.

The RFprotect™ Distributed System is comprised of the following components:

- Sensor – purpose-built device that provides continuous RF surveillance and data aggregation to manage the security of your network. Sensors receive and analyze 802.11 packets, analyze data, and send processed data to the Server.
- Server – management software application running on Windows or Linux that analyzes, stores, and integrates data from Sensors, generates alerts and maintains a database for Console users.
- Console (Client) – Win32 software application that is the main suite of tools for viewing and managing the information provided by the RFprotect™ Server and Sensors, and provides views of wireless activity, security alerts, and RF environmental analysis.

- AutoReports – Windows software application that allows you to schedule automatically generated RF security, performance and status reports to ensure your wireless network is operating securely and complying with legal mandates.




**RFprotect™ can be deployed for supplier independent Wi-Fi network infrastructure!**

***In order to mitigate the risks your network may suffer of, we offer you our HPE- Aruba RFprotect™ product-License with 30 days free-trail version. After the 30 days free-trial period has finished, we would be happy to provide you a commercial offer. Please contact our Sales Team via***
sales@aeroaccess.de

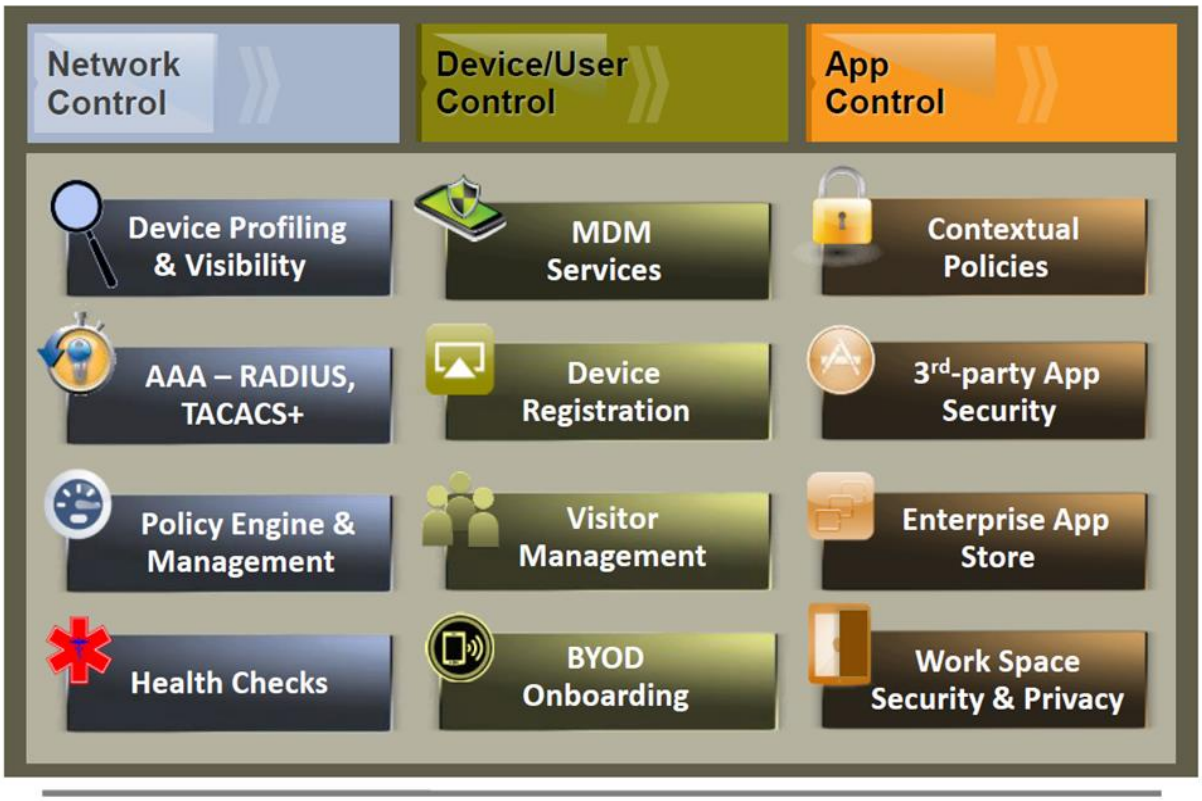
**Please note:** Dependent on your installed infrastructure base two different trial scenarios are possible.

Scenario 1: Your network already consists of HPE- Aruba HW AP's. Than only a RFprotect™ software trial version is required. RFprotect™ sensors are available in the HPE- Aruba AP's.

Scenario 2: Your network doesn't consist of HPE- Aruba HW AP's. Than in addition to the a RFprotect™ software trial version some RFprotect™ sensors have to be deployed. Aeroaccess GmbH will provide up to 15 HPE- Aruba HW AP's which would act as sensors FREE OF CHARGE for the trial period.

## B.12 What is the HPE- Aruba ClearPass?

HPE-Aruba ClearPass brings visibility, control and security response to the anywhere, anytime, any-device enterprise.
From one integrated platform, ClearPass lets IT manage network access and policies, onboard and manage devices, admit guest users, assess device health – even secure, distribute and manage mobile work apps.
An overview of HPE-Aruba ClearPass possibilities are shown on the slide below:




**ClearPass can be deployed for supplier independent Wi-Fi network infrastructure!**

***In order to mitigate the risks your network may suffer of, we offer you our HPE- Aruba RFprotect™ product-License with 30 days free-trail version. After the 30 days free-trial period has finished, we would be happy to provide you a commercial offer. Please contact our Sales Team via***
sales@aeroaccess.de

## B.20 Upgrade the Aruba Controller with the Aruba Fix

The vulnerabilities have been fixed in the following ArubaOS patch releases, which are all available for download immediately:

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

***For detailed descriptions and instructions of the different available upgrade procedures please contact our Support Team via***
support@aeroaccess.de
***Here you will get immediate and high qualified professional support. The support could be provided as on call support with easy instructions for the upgrade or could consist of full service.***

## B.21 Upgrade your Aruba IAP

The vulnerabilities have been fixed in the following InstantOS patch releases, which are all available for download immediately:

- 4.2.4.9
- 4.3.1.6
- 6.5.3.3
- 6.5.4.3

***For detailed descriptions and instructions of the different available upgrade procedures please contact our Support Team via***
support@aeroaccess.de

***Here you will get immediate and high qualified professional support. The support could be provided as on call support with easy instructions for the upgrade or could consist of full service.***

## B.30 Upgrade your Clients

It is essential that the complete network is save including ALL clients. Therefore, on all clients have to be installed patches, solving WPA KRACK.
Please visit suppliers support pages for the according information and updates or contact them with a letter / e-mail for e.g. below:

*Dear …,*

*As you know there is an issue with the WPA 2 key known as WPA 2 KRACK. Because we use your product via WLAN it is important to fix the firmware. Can you provide us an update or another solution?*

*Best regards,*

A challenge for company's IT could be the question, how to determine and detect all different types of clients and their numbers, accessing the network. Depending on the available network management systems exists different possibilities.

***Aeroaccess would be happy to provide support and give according guidance. Please contact our Support Team via***
support@aeroaccess.de