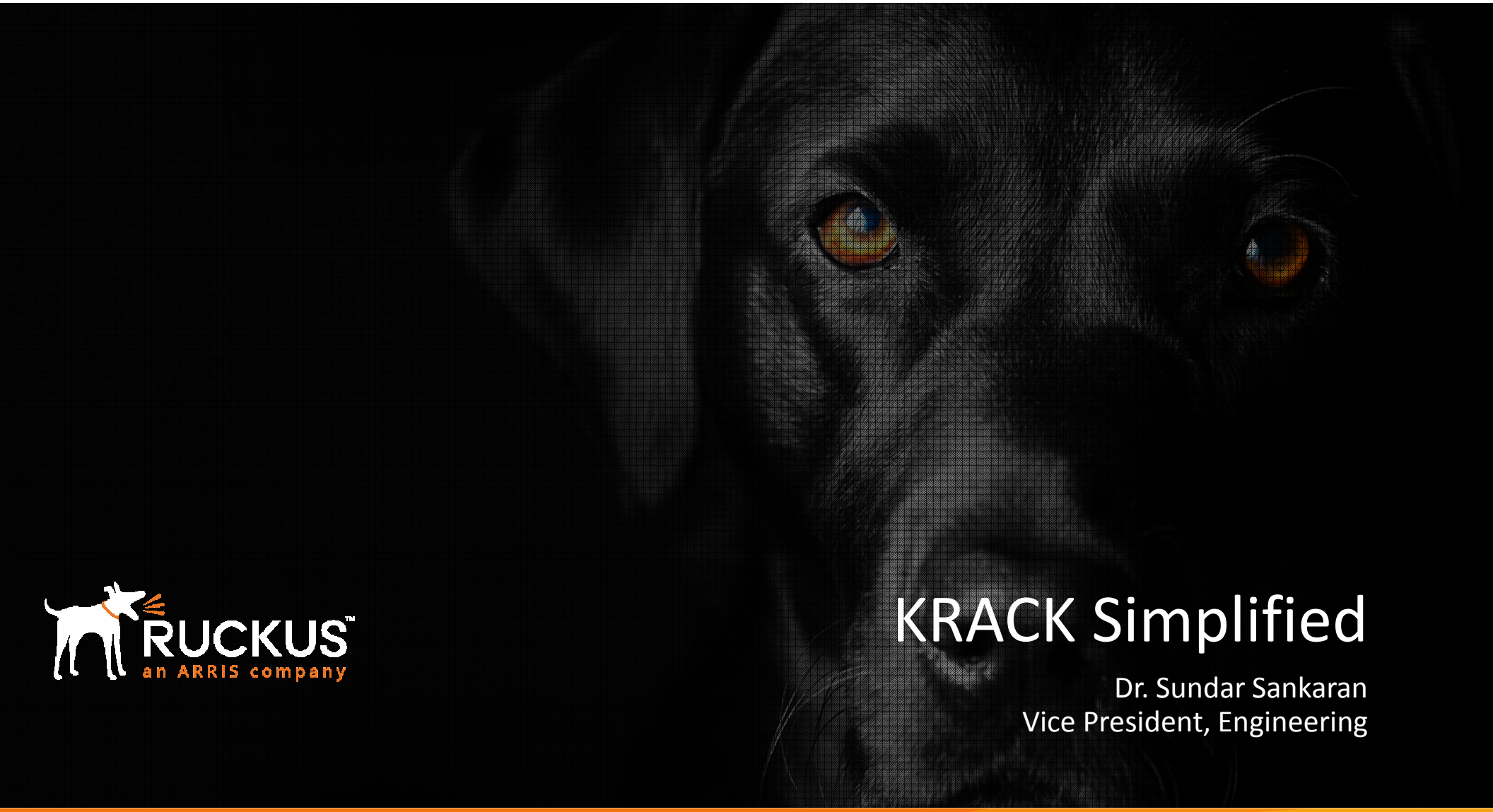


RUCKUS™
an ARRIS company

KRACK Simplified

Dr. Sundar Sankaran
Vice President, Engineering

Outline

- Cardinal Rules of Encryption
- What is the loop-hole exploited by KRACK?
- How to close this loop hole?
- What is the exposure?

Cardinal Rules of Encryption – Rule #1

Never accept an “old” packet again

- Imagine a sensor sending an encrypted packet to the AP that the temperature is too low
  - Heater gets turned up in response
- Imagine a malicious device “replaying” that same packet, as is, again (Replay Attack)
  - Heater gets turned up even more…. Consequences could be adverse!
- Receiver decides whether a packet is “old” or “new” by checking the Packet Number
  - AP keeps track of last received packet’s number
  - New packet is expected to have higher packet number than the last received packet.
    - Blindly-replayed earlier packet won’t have higher packet number and hence will be dropped
  - If a malicious device can trick AP into resetting last received packet number
    - And then replay an earlier packet
    - Packet number check will pass and AP will accept the “old” packet again

Cardinal Rules of Encryption – Rule #2

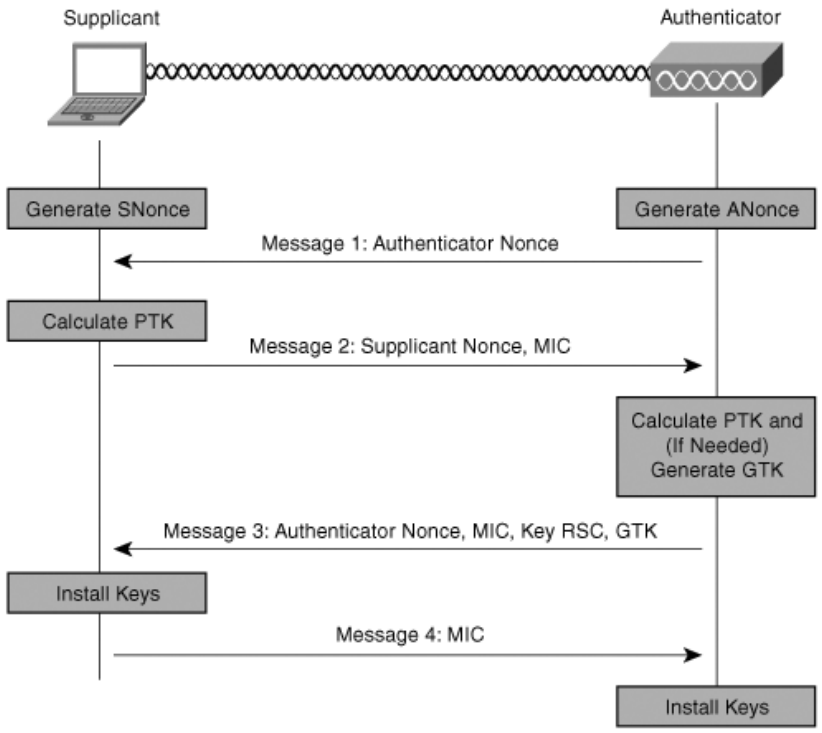
Never transmit 2 different packets with same encryption key

- Packets encrypted with same key can be decrypted in certain scenarios
  - Imagine someone tells you x + z; Difficult to determine 'x' without knowing z (Think of z as the encryption key)
  - Imagine someone tells you x + z and y + z
    - If I subtract the two, I get x – y, which doesn't depend on z => Effect of encryption disappeared
    - Now if I knew either x or y, I can determine the other
  - If one is a "known" packet, the second packet can be "decrypted"
- WiFi devices use a number called scrambler key (z) to encrypt each packet
  - Scrambler key generated by manipulating a fixed key and packet number
    - Scrambler key is a function of the Fixed key and Packet Number
  - If a malicious device can trick client into resetting its packet number
    - Two packets – one prior to packet number reset and another after – will be transmitted with same scrambler key

KRACK is all about tricking AP/Client into Resetting Packet #

Tricking Client Into Resetting Its Packet Number – Background

- Clients go through key “installation”
  - AKA EAPOL or 4-way Handshake
    - Client resets packet number at the end of this
      - Typically done after “M3” is received



Tricking Client Into Resetting Its Packet Number – Exploit

- AP transmits “M3” and client receives it
- Client transmits “M4” and resets the packet number
- Trick AP into thinking client did not receive “M3” by suppressing “M4”
- Client sends data packets, say P1 and P2, after this
  - These packets use keys assuming packet # is 1, 2
- AP retransmits “M3” and client receives it
- Client retransmits “M4” and resets the packet number again
- Client sends data packets, say P3 and P4, after this
  - These packets use keys assuming packet # is 1, 2
  - (P1 and P3), (P2 and P4) use the same scrambler key

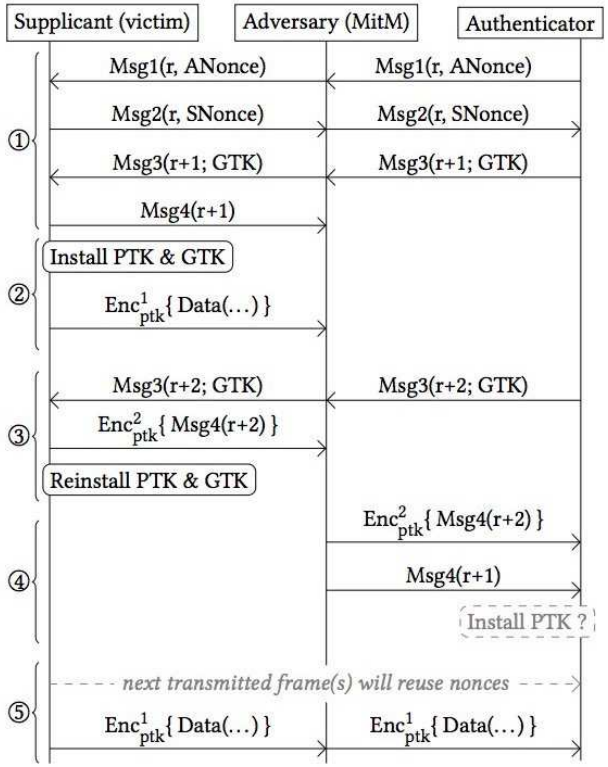


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

Figure taken from “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” M. Vanhoef and F. Piessens

Countermeasure Against Client Getting Tricked

- Client Side Patch (including Mesh and Point-to-Point)
  - Don’t reset the packet number if “M3” is received again (and again and again….)

- AP Side Patch
  - Don’t retransmit “M3,” if “M4” is not received
    - Restart the handshake, right from “M1,” if “M4” is not received
      - Additional overhead if “M3” is genuinely lost due to OTA collision or other reason
    - AP side fix mitigates client side exposure, but best to have clients patched as well

Tricking AP Into Resetting Its Packet Number – Background

- When clients roam, connection moves from one AP to another
- Every time client connects to new AP, authentication needs to be repeated
  - Go through 4-way EAPOL handshake again – takes time
- Some smart mechanisms exist to reduce this re-authentication time
  - Goes by the moniker “Fast Transition (FT)” or 802.11r, which is the standard used for FT
- APs reset packet number at the end of fast transition handshake
  - To be precise, when it receives the Re-association Request Frame from client

Tricking AP Into Resetting Its Packet Number – Exploit

- Record Re-Assoc Request
- Record subsequent data packets from client
- Replay recorded Re-Assoc Request
- AP resets its Packet Number – vulnerable to replay
- Replay recorded data packets
- AP accepts “old” packets
- Replay recorded Re-Assoc Request
- AP resets its Packet Number – vulnerable to replay
- Replay recorded data packets
- AP accepts “old” packets
- ….

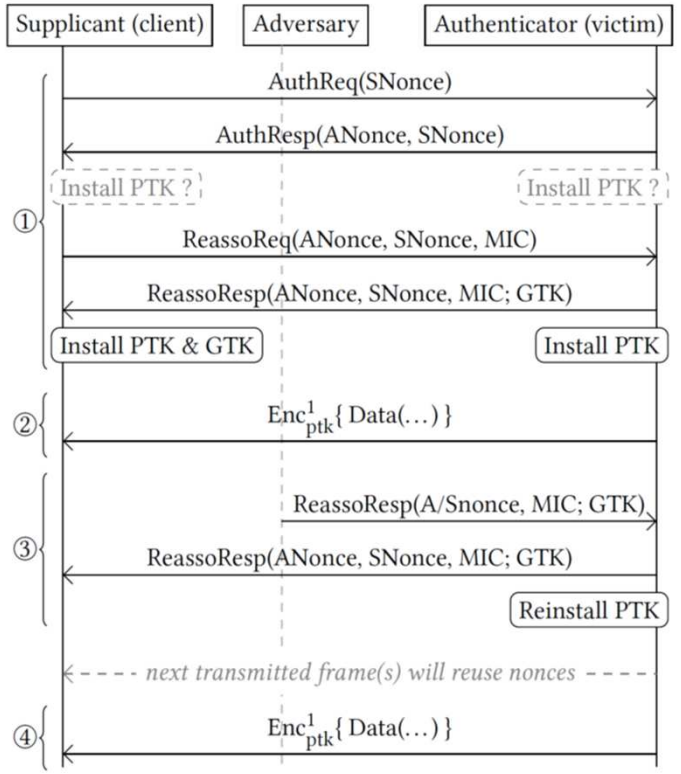


Figure 9: Key reinstallation attack against the Fast BSS Transition (FT) handshake. Note that a MitM position is not required, only the ability to eavesdrop and replay frames.

Figure taken from “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” M. Vanhoef and F. Piessens

Countermeasure Against AP Getting Tricked

- Workaround
  - Disable 802.11r
    - Loophole to trick AP into resetting receive packet number goes away
      - Additional overhead every time client moves from one AP to another
- Fix
  - AP side patch
    - Don’t reset packet number if Re-Assoc Req is received again (and again and again….)

What is the exposure?

- Needs a fairly sophisticated system (hardware/software) to attack
- System used to attack needs to be within the “reach” of both AP and client
- No known existence of an automated solution to execute this attack
- Intrusion protection (WIPS) prevents clients from connecting to Man-in-the-Middle
- No known way for the attacker to inject or forge packets
  - Limited to decryption and replay
    - Complete “decryption” not possible in the presence of other layers of protection such as HTTPS
- No known way for attacker to recover WiFi password and/or encryption key
- Client vulnerability exposed only during EAPOL exchange
  - In theory, malicious device can transmit “Deauth” and force client to go through EAPOL again
    - But Protected Management Frame is there to prevent this
- AP vulnerability exposed only during 11r “FT” exchange

Concluding Remarks

- KRACK is all about tricking AP/clients into resetting packet number
  - Triggered by Key Reinstallation
- Most vendors have released patch to address KRACK vulnerability
- WFA plans to enhance WPA2 certification test suite to include KRACK vulnerability check
- New security certification program (WPA3) launched by WFA to make WiFi more secure

SIMPLY BETTER EXPERIENCES