UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

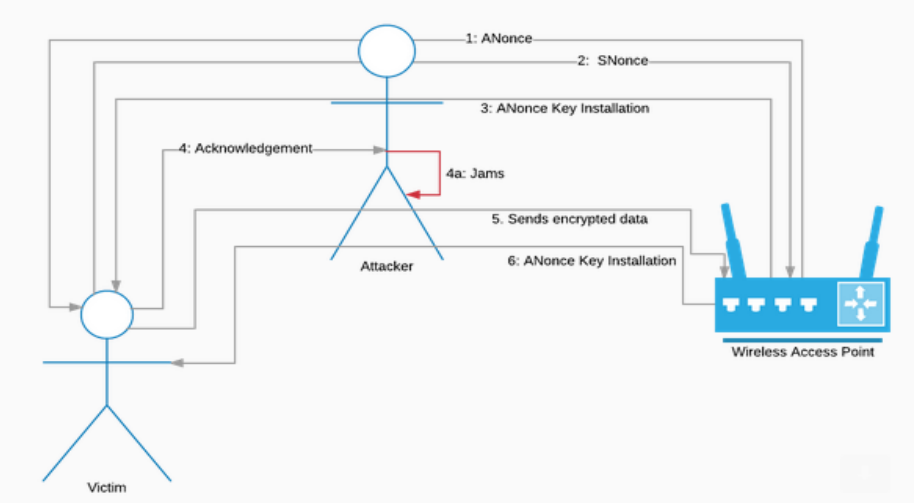
16/10/17

KEY REINSTALLATION ATTACK (KRACK) EXPLOIT ATTACK

Scope: KRACK exploit targeting WPA2 as publicly disclosed in a research paper by Mathy Vanhoef and Frank Piessens [https://papers.mathyvanhoef.com/ccs2017.pdf]

Severity: CERT.UG rates the severity of this vulnerability as **MEDIUM** due to the fact that an attacker has to physically be close to the target Wireless Access Point to potentially attempt this attack. The main affected vendors are Aruba, Cisco, Espressif Systems, Fortinet, the FreeBSD Project, HostAP, Intel, Juniper Networks, Microchip Technology, Red Hat, Samsung, Toshiba and Ubiquiti Networks.

Exploit Note: From the Research, Wireless access points use the 4-way handshake within the WPA2 encryption protocol to ensure data being sent to the client is encrypted. The handshake contains the sending of a nonce token from the access point to the client, which then replies with a signed nonce. Then a signed key is installed within the client and the client acknowledges the installation and transaction. KRACK uses a flaw within the 802.11 standard, which states that until acknowledgement is received, the message that triggers the key to be installed will be retransmitted. A visual representation of the attack workflow discussed can be seen in the image below



Using this knowledge an attacker can jam the acknowledgement of the installation in order to assist with decrypting all encrypted content sent from that client to the WAP. This can further continue with the retransmission of the signed keys. Attackers can leverage the vulnerability to decrypt traffic, hijack connections, perform man-in-the-middle attacks, and eavesdrop on communication sent from a WPA2-enabled device.

Risk Assessment: Provided the attacker is within appropriate physical range of the client and the access point, the attacker could decrypt the communications between the client and the WAP. This potentially means traffic being sent over the network to the client can be read by the attacker.

All versions of WPA are vulnerable.

Risk Mitigation: **1.** Consider using a VPN and/or properly implemented secure protocols such as SSH or TLS to secure any sensitive content being transmitted over wi-fi networks.

2. Update the Firmware of your Wireless Access Point. Many vendors have started patching (both client updates and WAP updates) – check the website of the vendor for the Wireless Access Point you are using on your network.

For information, here is the list of affected vendors:- http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

Uganda National Computer Emergency Response Team
NITA-U
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug
www.cert.ug