Professional Skills Assignment 1

Daniel Hannon (19484286)

Part A - Journal

Journal Name: Computers & Operations Research

Journal Scope: General Application of computers in a variety of fields Including but not limited to Ecology, Transport, and Cybersecurity.

Impact Factor: 3.002 (2018)

Publisher: Elsevier

Source:
https://www.journals.elsevier.com/computers-and-operations-research/

Part A (2) – Researcher

Name: Vanhoef, Mathy

Institute: New York University

Field of focus: Cyber security, Wireless Networks.

Citations: 563 overall

i10 Index: 10
H index: 10

Source:
https://scholar.google.com/citations?user=02_-sZ0AAAAJ&hl=en&oi=sra

Part B – Research Paper of Interest

The Paper I have chosen to summarize is called “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”. It was published in the CCS Journal in late 2017 and it was authored by Mathy Vanhoef and Frank Piessens. What this paper set out to do was bypass all security measures of the WPA2 Wi-Fi encryption system which was defined in 2004 and has since been the main form of wireless network encryption (IEEE Std 802.11i. 2004.). Compared to other attacks which focused on things like flaws in WPS (Wireless Protected System)[1] or Flawed RNGs[2] , This attack targets the four way Authentication handshake itself by taking data from attempting to connect and sending false information back in order to make the WAP (Wireless Access Point) think your device has the Key to allow you to access the network. The novel approach about this is that your device does not have the password, nor does it get the password but at the same time it allows you to reuse session keys and potentially set your own session key and grants you full access to any WPA2 network of choice, not only this, it allows people to commit man in the middle attacks and potentially steal peoples Data.

This paper has a very large impact within the field of cybersecurity as WPA2 has been the standard for many years so many of the current networks are very much vunerable to this attack. Although Wi-Fi Alliance has since defined the WPA3 Standard[3], The effects of this attack will last until all WPA2 Routers get phased out.

[1] (Viehback. Brute forcing Wi-Fi protected setup. USENIX Security (2011))
[2] (Vanhoef, Piessens. Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. USENIX Security. 2016)
[3] (Wi-Fi Alliance. WPA3$^{\text{tm}}$ Specification Version 1.0, wifi.org, 2018)

Source:
http://scholar.google.com/scholar_url?url=https://lirias.kuleuven.be/retrieve/504264&hl=en&sa=X&scisig=AAGBfm0PvNU0oVHIM9RLQ-1NKNfNExv98Q&nossl=1&oi=scholarr