ARC'18
مؤتمر مؤسسة قطر السنوي للبحوث
QATAR FOUNDATION ANNUAL RESEARCH CONFERENCE
البحث والتطوير: التركيز على الأولويات، وإحداث الأثر
R&D: FOCUSING ON PRIORITIES, DELIVERING IMPACT
19-20 مـــارس
19-20 MARCH

مـؤسـسـة قـطـر
Qatar Foundation
لإطـلاق قـدرات الإنـسـان.
Unlocking human potential.

Computing & Information Technology - Poster Display

http://doi.org/10.5339/qfarc.2018.ICTPD1124

SLiFi: Exploiting Visible Light Communication VLC to Authenticate WiFi Access Points

Hafsa Amin*, Faryal Asadulla, Aisha Jaffar, Gabriele Oligeri, Mashael Al-Sabah

Qatar University
* ha1306152@qu.edu.qa

This work presents an effective and efficient solution (SLiFi) to the evil twin attack in wireless networks. The evil twin is a rogue Wifi Access Point (AP) that pretends to be an authentic one by using the same network configuration, including the (i) Service Set Identifier (SSID), (ii) the communication channel, and finally (iii) the MAC address of the purported AP. The evil twin is a trap set-up by an adversary willing to eavesdrop on the user's Internet traffic. The attack is relatively easy to implement, hard to detect and it can have a severe impact on a user's privacy. Many researchers focused on this attack and provided defences from different perspectives: network, access point and client side. Unfortunately, all the solutions provided so far are still not ready for mass deployment since they involve significant modifications to the 802.11 WiFi protocol. In the following, we report some of the most important ones. Gonzales et al. [1] proposed to construct a context vector containing the order of all APs detected at a particular time, with their SSID and RSSI values. This enables the client to compare its future associations with the stored context vector. Bauer et al. [2] proposed SWAT which is a request-response protocol. This approach provides a one-way AP authentication and allows the client to establish a connection to the network through a shared secret key to create a secure session based on the principle of trust-on-first-use (TOFU). Lanze et al. [3] introduced a new technique using the aircrack-ng suite. The tool airbase-ng is set up on all the devices and the beacon frames are collected from various APs. The proposed approach compares the Timing Synchronization Function (TSF) timestamps and their corresponding receiving times in order to spot anomalies due to message proxying and therefore, the presence of a malicious AP. Finally, Gangasagare et al. [4] propose a

دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

Cite this article as: Amin H et al. (2018). SLiFi: Exploiting Visible Light Communication VLC to Authenticate WiFi Access Points. Qatar Foundation Annual Research Conference Proceedings 2018: ICTPD1124 http://doi.org/10.5339/qfarc.2018.ICTPD1124.

fingerprinting technique based on network traffic enabling to detect if the AP relays the traffic through another wireless connection. SLiFi does not require any changes to the already existing communication protocols and it enables the access point authentication (by the users) in a fast and reliable way. Indeed, SLiFi enables the user to authenticate the legitimate AP by exploiting a Visible Light Communication (VLC) channel. SLiFi involves two parties, i.e., the (honest) AP provided with a Wi-Fi interface and able to transmit data through a VLC channel, and an end-user, provided with a software that enables data to be read from a VLC channel, e.g., by using a webcam. SLiFi exploits four phases: AP's Public Key (PubKey) broadcast. The AP transmits its own PubKey to the end-user via an authenticated channel (VLC). The PubKey broadcast process is completely transparent to the user since each bit of the PubKey is delivered by quickly switching on and off the light of the room in which the user is. This is achieved by standard techniques of VLC: the human eye cannot perceive the fast blinking light but other devices, such as special webcams, can detect the brightness change. Subsequently, the brightness changes can be translated to a sequence of bit values. Seed generation. The end-user retrieves the public key from the VLC channel by using a webcam and transmits back to the AP a randomly generated seed encrypted with the AP's public key. The PubKey is securely delivered to the user since any other non-authorized light source can be easily spotted. Therefore, only one authorized VLC transmitter will be in place and it will deliver the PubKey of the AP. The client can now use the trusted PubKey to send back to the AP an encrypted seed to be used for the key generation. Secret key generation. The AP receives the user's encrypted seed via the Wi-Fi channel, decrypts the seed using its private key, and sends an acknowledgment message encrypted with the seed back to the end-user. This phase performs the key-agreement and both the AP and the user's device converge to a shared secret key. Encrypted communication. Any further communications between the end-user and the AP will be encrypted with the shared secret key, i.e., the seed generated by the client. SLiFi is compliant with multiple clients, indeed the AP can easily deal with concurrent communications. Moreover, from a practical perspective, SLiFi can be adopted to only generate the shared secret key and passing it to the already existing encryption algorithm, e.g., WPA2 or WPA2-Enterprise. To evaluate SliFi, we built a proof-of-concept using a (1) Raspberry Pi which emulates the AP, a (2) set of LEDs to transmit the PubKey, and (3) standard laptops to act as clients with webcams. All the software components have been implemented and tested. We performed several tests to evaluate the feasibility of our solution. To test reliability of VLC transmission, we ran various experiments to measure the Public key transmission errors as a function of the VLC bit-rate, and we observed that PubKey can reliability transmitted within a reasonable time frame. Finally, our results prove the feasibility of the solution in terms of time to establish the key and robustness to the evil-twin attack. References 1. H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker. Practical Defenses for Evil Twin Attacks in 802.11. In IEEE Globecom Communications and Information Security Symposium (Globecom 2010), Miami, FL, December 2010. 2. K. Bauer, H. Gonzales, and D. McCoy. Mitigating Evil Twin Attacks in 802.11. January 2009. 3. F. Lanze, A. Panchenko, T. Engel, and I. Alcaide. Undesired Relatives: Protection Mechanisms against the Evil Twin Attack in IEEE 802.11. 4. M. Gangasagare. Active User-Side Evil Twin Access Point Detection. International Journal of Scientific & Engineering Research, May 2014.