Conference Paper Title*

*Note: Sub-titles are not captured in Xplore and should not be used

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert**

攻撃モデル先に言いたい感ある.

I. Introduction

IP 見ればすぐわかるから攻撃者は MITM パターンできますよっていう説明

II. Related Works

Rogue AP (rAP) detection methods are mainly classified into two categories: network administrator side detections and user side detections. Network administrator side detections focus on the physical device's features such as RSSI and clock skew which cannot be spoofed by an adversary unlike MAC address. RAP can be detected compared with the features in the whitelist predefined with equipment setup such as a traffic sensor in each Wi-Fi network.

Wu et al. [**?**] utilize the RSSI as the feature for whitelist which is a measurement hard to forge arbitrarily and highly correlated to the transmitter's location and power. An AP which has different RSSI but same MAC address from that in the whitelist shows it is a rAP with spoofed MAC address set by an adversary at different location. However, it is hard to detect rAP which has no big difference in location because RSSI is not as microscopic as it can tell a small difference of the nearby location. Although it is useful as a supplementary feature, using only RSSI is insufficient to detect a rAP with high accuracy.

In order to detect in more detail, Lanze et al. [**?**] focus on clock skew as a device fingerprinting based purely on physical properties. Clock skew is an unvoidable physical phenomenon that causes crystal oscillator based clocks to run with minuscule yet measurable deviations in speed. However, these network administrator side detections are inapplicable to Wi-Fi hotspots because they have little motivation to guarantee no attacks nor will setup additional sensors or install detection software in their infrastructure to collect each data or detect them besides free Internet service.

Meanwhile, user side detections do not need Wi-Fi hotspot to be setup costly devices. They focus on the transmission characteristics caused by the extra hop to a rAP on the path between a lAP and user's device. Such evil hop results in several measurable changes, compared with legitimate networks, in transmission characteristics such as Round Trip Time (RTT) and channel used between a user device and DNS server.

Mustafa et al. [10] differentiate rAPs and lAPs by measuring the RTT between the user device and the DNS server through different target APs (rAPs or lAPs). Because the evil hop, introduced by the rAP, is added on the path, this leads to a longer RTT than that of the victim directly connecting to the lAP. Although those schemes which utilize the packet delay are useful to the attack which the adversary set rAP up on the laptop for, Jang et al. [12] reveal the fact that the computational power of the software bridging mainly accounted for the packet delay. Thus, these schemes which utilize the packet delay cannot detect hardware-based rAPs having little bridging delay unlike software-based rAPs.

In order to detect both types of rAPs, namely, software-based and hardware-based, [12] focuses on two communication channels utilized by a rAP between a user's device and lAP, respectively. Although a rAP intervene between a user's device and lAP, two distinct channels are used to reduce communication delay caused by channel interference each other. For example, channel 1 and 6 are used as the channel for a user's device and that for a lAP, respectively. That scheme detect rAP by finding out these two channels with the throughput of the transmission from the user's device to the DNS server. Although the throughput used for finding these two channels out is largely dependent on the network environment, that scheme is the most robust user side detection independent of the performance of the rAP currently because it is reasonable attack model to be setup hardware-based rAP by adversary. Thus, in this paper, we select [12] as a previous scheme and aim at propose the user side detection which enable to detect rAP regardless on each network environment and performance of the rAP.

Identify applicable funding agency here. If none, delete this.

III. ATTACK MODEL AND PREVIOUS SCHEME

A. Attack Model

In an evil twin attack, the adversary sets up his AP using the SSID of the targeted Wi-Fi network and also MAC address cloned from one of the APs in the network. As a result, a user's device receives SSID broadcast from both the lAP and the rAP, but it cannot differentiate between these APs. The user's device simply assumes that both the APs are legitimate and associates with the one that has a higher RSSI value. We assume the model that a rAP relays WLAN traffic between a legitimate AP providing Internet connectivity and a user's device, and may act as a man-in-the-middle-attack. By avoiding to use mobile Internet access, e.g., 3G/4G, the adversary can evade detection with ISP names or Global IP addresses [10]. Also, we assume the adversary launched hardware-based APs which cannot be detected accurately by existing schemes. Thus, it cannot be detected because hardware-based APs do not cause a computational delay by the software bridging.

B. Previous Scheme

1) Overview of the Previous Scheme: The main idea of the previous scheme [12] is that the adversary needs to use two distinct communication channels on the path from user's device to the DNS server to avoid channel interference each other: one for the path between lAP and rAP and the other for that betweeen rAP and user's device. Thus, from the perspective of the user's device, there exists another channel on the route different from a channel the device uses with the connected AP. Since the throughput value is dependent on the traffic on the path, the channel which is used between a lAP and rAP and not able to be seen directly from the user's device can be detected as a decline in the throughput by saturating that path. For example, when a user's device is using channel 1 with the targeted AP which cannot be judged to be legitimacy, the user-side device introduced for intentional channel interference transmit several packets with all the channel except channel 1 to saturate the path. If there exists the other channel on the route, the decline in the throughput can be observed by the user's device.

2) Shortcoming of the Previous Scheme: Although the previous scheme is successful in the detection for hardware-based rAP in the experimental environment, it cannot detect accurately in the real world because of various reasons such as collisions, network topology changes, unintentional interference and so on. Although the previous scheme is able to detect a rAP with high accuracy in the environment whose traffic is stable, the real environment is unsteady and subject to changes which can lead to decline the accuracy. Thus, it is necessary to propose the scheme which is independent of the traffic environment.

REFERENCES

[1] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks, " n Proc. of ACM Annual International Conference on Mobile Computing and Networking, MOBICOM, 2004, pp. 30-44.

[2] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, " Enhancing the security of corporate Wi-Fi etworks using DAIR, " in Proc. of ACM International Conference on Mobile Systems, Applications, and Services, MobiSys, 2006, pp. 1–14.

[3] R. Chandra, J. Padhye, A. Wolman, and B. Zill, " A location-based management system for enterprise wireless LANs," in Proc. of USENIX Symposium on Networked Systems Design and Implementation NSDI, 2007.

[4] D. B. Faria and D. R. Cheriton, " Detecting identity-based attacks in wireless networks using signalprints, " in Proc. of ACM Workshop on Wireless Security, 2006, pp. 43–52.

[5] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, " Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. of the 27th Conference on Computer Communications, INFOCOM, 2008.

[6] F. Lanze, A. Panchenko, B. Braatz, and T. Engel, " Letting the puss in boots sweat: detecting fake access points using dependency of clock skews on temperature, " in Proc. of ACM Symposium on Information, Computer and Communications Security, ASIACCS, 2014, pp. 3–14.

[7] S. Jana and S. K. Kasera, " On fast and accurate detection of unauthorized wireless access points using clock skews, " IEEE Trans. Mob. Comput., vol. 9, no. 3, pp. 449–462, 2010.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures, " in Proc. ofACM Annual International Conference on Mobile Computing and Networking, MOBICOM, 2008.

[9] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, " A novel approach for rogue access point detection on the client-side, " 27th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[10] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection, " IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1912–1925, 2011

[11] C. Yang, Y. Song, and G. Gu, " Active user-side evil twin access point detection using statistical techniques, " IEEE Trans. Information Forensics and Security, vol. 7, no. 5, pp. 1638–1651, 2012.

[12] R. Jang, J. Kang, A. Mohaisen and D. Nyang, "Catch Me If You Can: Rogue Access Point Detection Using Intentional Channel Interference," in IEEE Transactions on Mobile Computing.