SafeWLAN: A WLAN-based SDN Approach for Securing WLAN Traffic

Mostafa Uddin,Ashish Kshirsagar, Tamer Nadeem
Old Dominion University

1. INTRODUCTION

Given the large number of mobile devices with numerous apps, wireless LANs (WLANs) (i.e., WiFi networks) is typically the most prominent wireless communication that we use in our daily life. For example, a recent research found that 64% of the smartphone users hit WiFi hot spots at least once a day outside their home or office (e.g., at cafe, hotel, school campus, train/bus stations, etc.) [2] and that 74% of smartphones data goes through WiFi [3]. However, due to the broadcast nature of WiFi links, wireless traffic are exposed to any eavesdropping adversary within the WLAN.

Despite the user authentication, data confidentiality, and data integrity schemes of 802.11i standards that is utilized in most WLANs, there are several user-related information that could be inferred from the encrypted wireless traffic. For example, network SSID, and the MAC address of both the user device and the WiFi access point (AP) from probe request and probe response frames. Such, seemingly innocuous and small amount of information can be used to uniquely identify the user, track user's location history, and infer many other user behavior. Several previous works have shown that, even with encrypting the WiFi data and control frames, by extracting specific features of WLANs traffic such as frame size, data rate, ratio of incoming to outgoing frames, inter-arrival time of the frame, etc., several user-related information still could be inferred such as user identity [4] and user's online activities [6] such as browsing, chatting, gaming, downloading/uploading, video streaming and P2P file sharing.

In this paper, we aim to highlight one additional significant vulnerability of the current WLANs by demonstrating potential privacy threats resulting from analyzing passively captured encrypted wireless traffic from different smart device applications. More specifically, we show how an eavesdropping adversary could identify what smart device applications the user is using and when exactly these applications have started. In consequence, these leaked information would lead to inferring many other information about the user identity. For example, consider a scenario of a house occupied by a family consists of husband, wife, and two kids. An adversary with a cheap hardware and free software tools such as WireShark could capture passively the WiFi traffic of the house members over long period such as a week. By analyzing the traffic and the corresponding application usage activities such as what application start when (as we will discuss later), and giving that different individuals have different application interests [5], the adversary will be able to correlate the detected application activities to different members of the house. Thus, the adversary could infer the occupancy periods of each member over the week. Even simpler, the adversary will be able to identify which time periods no one is in the house. This example shows how knowing online activities and application usages of individual is not just only a privacy issue, but also could be a serious threat to the individual safety.

2. *SAFEWLAN* SYSTEM

In addressing such vulnerabilities of WLANs, we propose in this paper SafeWLAN. The basic idea of SafeWLAN is applying flexible and transparent traffic shaping techniques on the wireless traffic between the user device and the AP of the WLAN. In designing SafeWLAN, we extends many of the "data plane" components of the Software Defined Network (SDN); OVS, OpenFlow, Traffic Scheduler, to make it adaptable for our solution [1]. Moreover, SafeWLAN allows us to utilize a software define approach in applying optimal traffic shaping technique per flow-type per app. Note that, this system is compatible with both legacy smart devices and legacy APs. If both a smart device and a AP support SafeWLAN, they will be able to apply traffic shaping techniques to hide the app's traffic from the adversary.

The SafeWLAN system can apply different traffic shaping techniques such as padding bytes, aggregating, splitting, and delaying packets based on apps or app's flow-type to "pollute" the data packets generated from the app. Note that, SafeWLAN don't pollute all data packets or frames. Based on certain predefined settings or scheme some of the app's data packet get polluted and some remains original. Moreover, in order to reduce the overhead of traffic shaping techniques, SafeWLAN system addresses several design related questions. Such as, in padding, *How many bytes to pad?* In aggregating, *What is the maximum byte limit of aggregating consecutive packets?*In splitting *How many packets to split into?* Defining these parameters and how they should be set, are some of the key questions we like to address in our on going work. Furthermore, we like to evaluate the QoE of the mobile apps for the implications of our traffic shaping techniques.

3. REFERENCES

[1] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. Ethane: Taking Control of the Enterprise. SIGCOMM '07. ACM.

[2] Devicescape. Facing data caps, consumers keep turning to wi-fi., June, 2011. `http://tinyurl.com/qx3mo6l`.

[3] FierceWireless. Android smartphone users download just 870 mb over cellular per month., September, 2012. `http://tinyurl.com/p7doszj`.

[4] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. 802.11 User Fingerprinting. MobiCom '07. ACM.

[5] B. Yan and G. Chen. Appjoy: Personalized mobile application discovery. MobiSys '11. ACM.

[6] F. Zhang, W. He, X. Liu, and P. G. Bridges. Inferring Users' Online Activities Through Traffic Analysis. WiSec '11. ACM.