A Study of Secure Communications in WiFi Networks

Bumjo Park[1] and Namgi Kim[11]

[1]Dept. Of Computer Science, Kyonggi Univ.
San 94-1, Iui, Yeongtong, Suwon, Gyeonggi, 443-760, Korea
parkbumjo@gmail.com, ngkim@kgu.ac.kr

Abstract. WiFi networks, which have been widely used along with the explosive increases in the supply of smartphones, can provide high network speeds but cannot prevent user information spills though rogue Access Points (APs). Therefore, we need a method to exchange SSL session keys through more secure networks to be used in WiFi networks in order to prevent such spills.

Keywords: secure communication, rouge AP, WiFi, 3G

1. Introduction

Along with the explosive increase in smartphones, users have come to install Access Points (APs) that enable easy and fast wireless access to the Internet at home or a place of business without any restrictions. [1][2] However, rogue APs that are installed by attackers with a view to obtaining users' confidential information have become great threats to wireless Internet security.

A method that can be commonly used in web services to prevent hackers' attacks on WiFi networks with low security is encrypting the data exchanged in HTTP protocols using Secure Socket Layers (SSLs) to ensure data confidentiality in communication. However, even when SSLs are used, users' confidential information can be easily extracted using Man in the Middle (MITM) attacks. [3] Therefore, recently, studies to detect and block rogue APs have been actively conducted in order to prevent these security hazards. [4] However, this method has problems, because it involves additional overheads, since in order to detect rogue APs, wireless packets should be analyzed and AP lists should be managed, and even when these additional overheads have been added, rogue APs have not been pefectly detected.

2. Secure Communications in Rogue AP Environments

WiFi networks provide mobility and convenience to users by enabling wireless communication. However, they are vulnerable to hacking and information spills, because they provide open wireless communication. To make up for this weakness, web service data can be encrypted for confidentiality using SSLs in HTTPS protocols.

1 Corresponding author: Namgi Kim

SSLs are protocols that create security connections between clients and servers to encrypt the data being exchanged. In SSLs, clients and servers using exchange authentication keys and encrypt data with the keys before transferring the data. However, recently, attack methods have been found that enable malicious rogue APs to illegally decrypt encrypted user data by manipulating, in the middle between clients and servers, the process through which authentication keys are transferred.

Figure 2 shows a scenario that demonstrates this vulnerable point of SSLs. In the figure, a rogue AP serves the role of a proxy in the middle of a client and a server, requesting the server for authentication keys to be used by the rouge APs and sending counterfeit authentication keys created by the rogue AP to the client. Thereafter, the client encrypts data using the counterfeit authentication keys transferred by the rogue AP, and thus the rogue AP can decrypt the data in the middle. As such, if rogue APs are used, weak points in security can be used to hack important user data even when SSLs are used. To prevent this, many studies have been conducted to detect rogue APs. Representative studied methods include methods to detect rogue APs through an AP authentication server [5], methods to detect rogue APs through traffic analysis [6], and methods to detect rogue APs through comparisons of server authentication certificates [7].

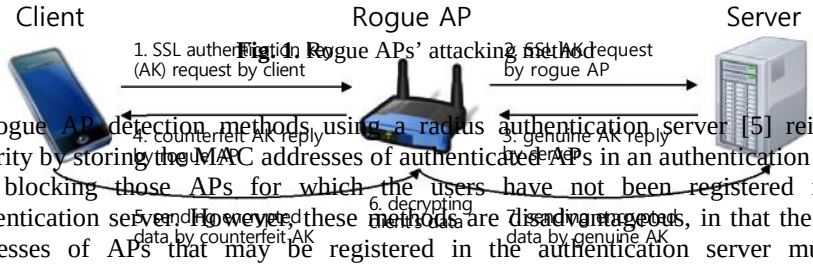

Fig. 1. Rogue APs' attacking method

Rogue AP detection methods using a radius authentication server [5] reinforce security by storing the MAC addresses of authenticated APs in an authentication server and blocking those APs for which the users have not been registered in the authentication server. However, these methods are disadvantageous, in that the MAC addresses of APs that may be registered in the authentication server must be periodically maintained and managed, and none of the public APs that have not been maintained and managed can be used. In addition, these methods cannot detect rogue APs that have reproduced even the MAC addresses. Second, some methods [6] detect rogue APs by analyzing the characteristics of the traffic in routers. These methods scan the source IP address and source port number of the transferred data and judge whether the source host is an authenticated host or a rogue AP by analyzing the characteristics of wireless and wired packets. However, these methods are disadvantageous too, in that to detect and block rogue APs, a traffic analysis module should be installed in each router device, and information should be collected and analyzed every time through the traffic analysis module. Finally, there is a method to detect rogue APs by receiving a server's authentication keys through more secure

networks such as 3G networks and comparing them with authentication keys received through WiFi networks [7]. This method is the most similar to the method proposed in the present paper. In this method, when the authentication keys of a server received through heterogeneous networks are different from each other, the AP used in the relevant WiFi network is judged to be a rogue AP and is not used. However, if an AP received through a WiFi network is judged to be a rogue AP, the WiFi network, which is fast, will not used anymore and thus network efficiency will be decreased. On the contrary, in the case of our method, since authentication keys securely received by 3G networks are immediately used again in WiFi networks, WiFi networks can be securely utilized without detecting rogue APs that may be inaccurate while requiring large overheads.

5. Conclusion

In this paper, we reviewed threats of rouge APs which can be installed by attackers for obtaining users' confidential information. Recently, in order to prevent attacks with rogue APs in WiFi networks, lots of researches have been conducted. However, the sequrity threats by rough APs have not been efficiently solved. This is because most previous researches require much additional overhead but not completely detect rouge APs. Therefore, we need a new method which communicates more securely while utilizing the efficiency of WiFi networks. The proposed method should utilize fast WiFi networks more securely even where rogue APs may exist.

Acknowledgment

This work was supported by the GRRC program of Gyonggi province.

References

1. IEEE: Information technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks-Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11 (1999)
2. Crow, B. P., Widjaja, I., Kim, J. G., Sakai, P. T.: IEEE 802.11 Wireless Local Area Networks. IEEE Communications Magazine, Vol. 35, No. 9 (1997) 116-126
3. Wikipedia: Rogue Access Point. http://en.wikipedia.org
4. Beyah, R.: Rogue Access Point Detection Challenges, Solutions, and Future Directions. IEEE Security and Privacy Article, Vol. 9(5), IEEE (2011) 56-61
5. Kim, D.-P., Jiang, Z., Kim, S.-W.: Rogue AP Protection System based on Radius Authentication Server. in Proc. of KISS Spring Conferences (A) (2004) 316-318
6. Shetty, S., Song, M., Ma, L.: Rogue Access Point Detection by Analyzing Network Traffic Characteristics. Proc. of Milcom (2007)
7. Lee, J., Tu, C., Jung, S.: Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G Network. in in Proc. of IARIA (2012)