A Novel approach for Evil Twin or Rogue AP mitigation in wireless environment

Ankit Panch
Department of Computer engineering,
Suresh Gyan Vihar University, Jaipur, India
ankitpanch@gmail.com

Santosh Kumar Singh
Department of Computer engineering,
Suresh Gyan Vihar University, Jaipur, India
sksmtech@yahoo.com

ABSTRACT

Evil Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers.[1] The phony Access point, with suspicious intentions broadcasts the Service Set IDentifier (SSID) the same as the legitimate network or Access Point, which diverts the network traffic indented for the real AP towards the phony AP, which in turn can steal sensitive information from the client side. Here in this paper, a simple approach is introduced which uses, Wireless Connection Session DataBase, where a system database file can be configured on the client and server side (gateway of real AP), to maintain a track record of successful sessions between trusted systems to identify the credentials of the AP and hence makes it possible to identify the fake Access point, with a very simple approach, without any modifications at the infrastructure or the hardware.

Keywords: *Rouge Access point, Evil Twin, Wireless Security*

1. Introduction

Evil Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers.[1] Evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. Wireless devices link to the Internet via "hotspots" - nearby connection points that they lock on to. But these hotspots can act like an open door to thieves. Anyone with suitable equipment can locate a hotspot and take its place, substituting their own "evil twin". This type of *Evil Twin Attack* may be used by a hacker to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent Web site and luring people there.[2]

2. Problem Background

The attacker uses a bogus base station that someone connects to using Wi-Fi wireless technology. By imitating the name of another, legitimate wireless provider, they can fool people into trusting the internet services that they are providing. When the users log into bank or e-mail accounts, the phishers have access to the entire transaction, since it is sent through

their equipment. Unwitting web users are invited to log into the attacker's server with bogus login prompts, tempting them to give away sensitive information such as usernames and passwords. Often users are unaware they have been duped until well after the incident has occurred. Users think they have logged on to a wireless hotspot connection when in fact they have been tricked into connecting to the attacker's base station. The hacker jams the connection to the legitimate base station by sending a stronger signal within proximity to the wireless client - thereby turning itself into an 'evil twin.' A rogue Wi-Fi connection can be set up on a laptop with a bit of simple programming and wireless card that acts as an access point. The access points are hard to trace, since they can suddenly be shut off, and are easy to build. A hacker can make their own wireless networks that appear to be legitimate by simply giving their access point a similar name to the Wi-Fi network on the premises. Since the hacker may be physically closer to the victim than the real access point, their signal will be stronger, potentially drawing more victims. The hacker's computer can be configured to pass the person through to the legitimate access point while monitoring the traffic of the victim, or it can simply say the system is temporarily unavailable after obtaining a user id and password.[3]

Several free programs available on the Internet can decode packets to reveal clear-text logins and passwords. Using an Evil Twin attack a hacker is able to harvest Web applications such as email that could send passwords in clear text.Hackers typically setup Evil twin attacks near free hotspots, such as airports, cafes, near student residences, hotels or libraries [4].

3. Assumptions

In multiple connection environments, considering a situation where a Legitimate AP connected to an enterprise gateway is providing access to a client A. The client A regularly gets connected to the AP, and utilizes its services. During a new session, a Fake AP, or evil twin, starts broadcasting the same SSID as of the real AP, and as the signal strength is high the Client AP gets connected to it due to the preferred network settings or a deliberate connection.

As, this authentication approach works mid way in the process of discovery and connection to a preferred AP which is fake in this case. Still the connection is established. Previously, we should not forget that there is a mutual key exchange between the server and the client, before the session is established. The approach elongates the authentication process with a very slight variation. The explanation is as under.

1. The server responds with the key exchange after mutual handshake, and the connection is established.
2. The client connecting to the server needs to verify the legitimacy of the server, through probing (*figure 1*).
3. If the server authenticates itself, then the connection can be maintained else it is dropped.

Here if the key or certificate exchange is compromised, or the AP provided another certificate to trust by the client which gets accepted. Then the chances of the Fake AP to establish a true look alike connection with the client are increased to many folds.

4. Mitigation Approach

The approach here begins from the first connection established by the requesting client, here a mechanism to provide the authenticity of the AP by probing about previous connections that were successfully established and managed, can lead to a decision making alternative for the client to either trust and connect or not to trust and drop the connection. This approach do not need any hardware modification or up gradation but requires for the generation of a system file and an inclusion of a *wireless connection session database (wC_SessionDB)*, which can provide the historical evidences of the authenticity of the AP.

Considering, the AP and the Client were already connected 1 time and a *wCSession_DB* field entry was created by the backend gateway of the AP to the client to relish the connection services, can contain the following field types.

1. Session Number -- *sessionNum*
2. MAC Id of client -- *clientMacId*
3. Session Key -- *sessionKey*
4. Session Date -- *sessionDate*
5. Establishment Time -- *sessionTime*
6. Others (if Any)

So,

wC_SessionDB_field				
sessionNum	*clientMacId*	*sessionKey*	*sessionDate*	*sessionStartTime*

This wireless session database can be configured and stored in the configured system database file on both client and server sides. Along with these fields, an inclusion of Hash can bring up the desirable results, and will ease in propagation of parameters.

4.1 Working

Such a system database file is maintained and updated as required on the server and client side; the requesting client can probe the server about connection history, through hash value transmission. As it is only the genuine AP/ server, which has the same updated Wireless Session Identifier table, as the same whose carbon copy lies on the client side, can easily make the client distinguish between the Real and the Fake AP. The fake AP gateway can not answer the probing questions by the client so the client do not trusts the AP and drops the connection, with a warning message to the end user.

Client ID/MAC					
	Session Number	Session Date	Session Key	Session Establish Global Time	HASH DIGEST
	1	120310	FWE23432DSXCV	1900	HASH1

	2	130310	WER26753DFERC	1343	HASH2
	3	160310	SWE34523FDFGFK	2332	HASH3
Resultant Hash					*rHASH*

TABLE 1.1 Server Side Database

Server ID/MAC					
	Session Number	Session Date	Session Key	Session Establish Global Time	HASH DIGEST
	1	120310	FWE23432DSXCV	1900	HASH1
	2	130310	WER26753DFERC	1343	HASH2
	3	160310	SWE34523FDFGFK	2332	HASH3
Resultant Hash					*rHASH*

TABLE 1.2 Client Side Database Table

(The values in the table fields are arbitrary.)

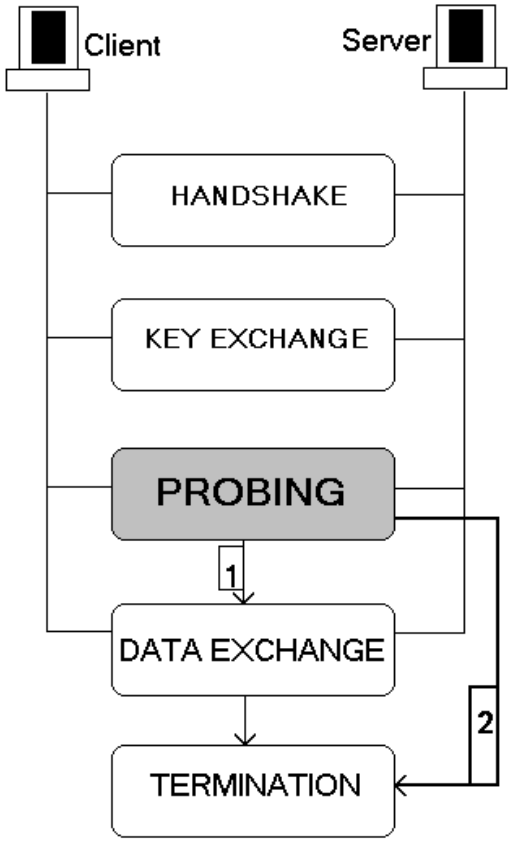

FIGURE 1: Probing through the use of Wireless Connection Database.

4.2 Probing Method

1. During the procedure of handshake, the client asks the server just before the connection can be established successfully. To send it, the overall hash of all the connection parameters till now. And checks it with it own entry.
2. Along with this, the client can randomly ask for any hash digest of any random entry.
3. Trying this procedure for say, 3 times, if the server is not able to provide the satisfying probing answers, the connection is terminated, with a warning message to the end user (route 2 on Figure 1).
4. If in case the server is able to identify by answering the probing questions rightly, the connection can be established, and a newly generated session id is transmitted to the client, where then both of the sides update their tables. On mutually acceptable grounds, (route 1 on Figure 1).

4.3 Additional Details

1. The session ID field may or may not be available, in advance version of this approach, session ID can be used in creation of Hash, and later the hash can only be used, while the session ID may or may not be used again.
2. The inclusion of other fields is necessary to identify a specific connection with a unique hash to be able to establish authentication while probing.
3. Entries can be replaced depending on the time window or number of connection parameters, e.g., any entry which is over one month old can be removed, and the space can be allocated to another, or entry over 30 times of connections can be removed but should be done on a mutual understanding between the client and the gateway.
4. This approach is ready to be implemented in places like universities, libraries, where selected users are accessing services on regular basis, this approach can help them to detect fake Wireless Networks.

5. Future Work

1. Further Research can make this applicable for single session, like newly available hotspots that offer free services.
2. This approach can be used in interacting with enterprise portals, where the client machine can ask the server portal to prove its authenticity, because of the high frequency of connections.
3. This approach can be implemented in OS, or network connection management (application layer) and can aid in selectively discarding unwanted fake networks which pose as one trusted network.
4. With radio signal monitoring and crowd sourcing this approach, can be triggered when there is a possible detection of Rouge AP.

References:

[1] "Strange Wi-Fi spots may harbor hackers: ID thieves may lurk behind a hot spot with a friendly name." Andrew D. Smith. The Dallas Morning News. Knight Ridder Tribune Business News. Washington: May 9, 2007. pg. 1 Source type: Wire Feed ProQuest document ID: 1267536891

[2] "Security Watch. Daniel Wolfe. American Banker. New York, N.Y.: Feb 14, 2007. Vol.172, Iss. 31; pg. 7. (A security firm used an Evil Twin as a test to obtain passwords from attendees at RSA security conference). Source type: Newspaper ISSN: 00027561 ProQuest document ID: 1219496681

[3] "Computer Column." Craig Crossman. Knight Ridder Tribune Business News. Washington: Aug 24, 2005. pg. 1. Source type: Wire Feed ProQuest document ID: 886418531

[4] Access Without Authentification: how and why we let anyone surf our wireless."Donna Watkins. Computers in Libraries. Westport: Mar 2006. Vol.26, Iss. 3; pg. 10, 5 pgs. Source type: Periodical ISSN: 10417915 ProQuest document ID: 1000365471

Authors

Ankit Panch received his B.E. degree in Computer Engineering from Birla Vishwakarma Mahavidyalaya, under Sardar Patel University, Gujarat, India, year 2007 and is presently pursuing his M.Tech in Software Engineering at the School of Engineering, Suresh Gyan Vihar University, Jaipur, India. His current research interests include information security, intrusion detection & mitigation and wireless networks. He is being guided by Mr. Santosh Kumar Singh, towards the completion of his thesis.

Santosh Kumar Singh received his B.E. degree in Electronics and Communication Engineering from S. J. College of Engineering, under Mysore University, Karnataka, India, year 1995 and M.Tech in Information Technology in 2004. He having 13 year teaching experience and pursuing his Ph.D. degree in Engg. at the School of Engineering, Suresh Gyan Vihar University, Jaipur, India. He published one book and research papers in well-reputed publication. He has also presented several papers in International and National conferences. His current research interests include next generation wireless networks, wireless sensor networks and industrial embedded system.