Multipot: A More Potent Variant of Evil Twin

K. N. Gopinath
Senior Wireless Security Researcher and Senior Engineering Manager
AirTight Networks

This presentation pertains to a discovery of a more potent variant of Evil Twin. We call it 'Multipot'. What is unique about Multipot is that the prevalent defenses against Evil Twin, in particular deauth based session containment, are totally ineffective against the Multipot. Multipot threat can occur naturally in enterprise and campus network environments or it can be presented by attacker with deliberate malicious intent. A demonstration of Multipot threat will be provided at the end of the presentation. Multipot provides a glimpse into complexities of evolving wireless vulnerabilities and their countermeasures [1,2].

Multipot: What It Is and How It Works

Multipot is a newly discovered threat scenario consisting of multiple APs which are configured with the same SSID and lure WiFi clients into connecting to them. The term Multipot is derived from "multiple" and "honeypot".

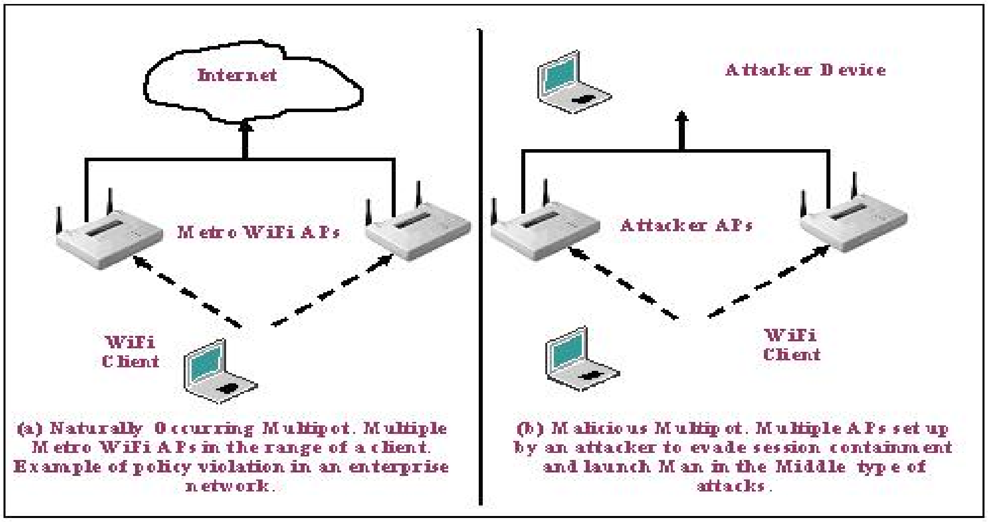
Multipot can occur naturally in the form of multiple Municipal APs or Metro APs around the victim client, all of which are naturally configured for the same SSID (e.g., GoogleWiFi). A client which has such an SSID in its WiFi profile can connect to such a Multipot. Another example of naturally occurring Multipot is multiple APs in the neighbor's corporate network around the victim client, which again are naturally configured with the same SSID. Neighboring networks which are open (i.e., do not use cryptographic security) and/or use manufacturer default SSIDs are good candidates for this type of Multipot. Wireless connections of corporate or campus clients to such naturally occurring Multipots can lead to non-policy compliant communication.

There can also be a handcrafted or malicious version of Multipot where an attacker can combine it with known Evil Twin attack tools (see references 3 to 8). Each of these APs in a handcrafted Multipot feeds data into a common end point (e.g., an attacker's computer). The attacker can then launch a man-in-the-middle attack using Evil Twin attack tools.

Prevalent Evil Twin Countermeasures do NOT Work Against Multipot

The prevalent Evil Twin defenses are ineffective against Multipot. In particular, the prevalent defenses include: i) Taking precaution so that clients are not lured to Evil Twins (e.g., specialized client side software), and ii) since these precautions are not always foolproof or practical, using a Wireless Intrusion Prevention System (WIPS) to block clients' connections to Evil Twins. Most of the current WIPS use deauthentication (deauth) based session containment to defend against this threat. In this presentation, we demonstrate that Multipot renders the deauth based session containment completely ineffective.

In more detail, when a WIPS attempts to block client’s connection to one of the APs in the Multipot, the client (including the prevalent Centrino client) automatically and swiftly “hops” to another AP in the Multipot and continues its communication. WIPS sensor detects and deauths client’s connection to the AP after a finite delay (e.g., typically around a second, even up to 10 seconds in some systems). Such a channel scanning and processing delay in the WIPS is unavoidable, as the WIPS sensor needs to continually circle through many channels for detecting unauthorized activity. Fast clients such as Centrino swiftly connect to other APs with the same SSID upon receiving sensor’s deauth. A WIPS sensor can be trapped into cat and mouse game by exploiting the inherent time disparities involved in detecting the new association and subsequently, starting session containment. We demonstrate that an application does not face any major disruption while this cat and mouse game continues.



(a) Naturally Occurring Multipot. Multiple Metro WiFi APs in the range of a client. Example of policy violation in an enterprise network.

(b) Malicious Multipot. Multiple APs set up by an attacker to evade session containment and launch Man in the Middle type of attacks.

Figure 1: Naturally occurring Multipot (a) and malicious Multipot (b)

Live Multipot Demonstration

We will demonstrate Multipot threat with two APs constituting the Multipot and a WIPS sensor that can deauth on one channel at a time. It will be shown that sustained ping and TCP connections are maintained by the victim client through the Multipot even in the presence of deauth based session containment from the WIPS. Though we will not demonstrate Multipot with more than two APs, following observations can be made. Even if the WIPS sensor can deauth on N channels simultaneously, a Multipot can contain/may be set up with N+1 constituent APs to make the session containment ineffective. Practically however, for a single WIPS sensor, N cannot be greater than 2 as otherwise containment does not work anyway as sufficient deauths cannot be continuously transmitted on any of the channels. Further, if Multipot can be implemented using soft APs, it can contain virtually unlimited number of APs.

Multipot Countermeasures

To defend against Multipot, it is required that WIPS perform session containment in a manner to keep the client from hopping to APs with similar SSIDs. One direction to pursue is to perform wireless session containment at layer 3 and above, so as not to disturb layer 2 connection and thus not prompt the client to hop the APs.

References

1. Joshua Wright, Weaknesses in Wireless LAN Session Containment, 5/19/2005, http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf
2. Jon Cox, Researchers crafting intelligent scaleable WLAN defense, Networkworld, Dec 2006, http://www.networkworld.com/news/2006/120706-intelligent-scaleable-wlan-defense-darpa.html
3. Christopher Null, Beware the “Evil Twin” Wi-Fi Hotspot, http://tech.yahoo.com/blogs/null/23163/beware-the-evil-twin-wi-fi-hotspot
4. CNN, 'Evil twin' threat to Wi-Fi users, http://www.cnn.com/2005/TECH/internet/01/20/evil.twins/index.html
5.. KARMA, http://www.theta44.org/karma/
6. Delegated, http://www.delegate.org/delegate/mitm/
7. Airsnarf, http://airsnarf.shmoo.com/
8. Hotspotter, http://www.remote-exploit.org/codes_hotspotter.html
9. Monkey jack, http://sourceforge.net/projects/airjack/