POSTER: WiFi AP Infection Spread

Amirali Sanatinia, Sashank Narain, and Guevara Noubir

Northeastern University
{*amirali, sashank, noubir*}*@ccs.neu.edu*

1. MOTIVATION

WiFi APs are ideal targets of attack. They are the main gateway to residential networks with direct access to home computers, as such they are highly prone to man-in-the-middle attacks. They are also wirelessly interconnected, independent of the wired Internet. WiFi APs can transmit at one Watt, they do not run anti-virus software, do not have an automatic updating mechanism, and are rarely patched by their users, thus enabling a wireless spreading of APs infections. This makes the detection and mitigation of their spreading very difficult. Furthermore, a compromise of WiFi APs can result in global scale denial-of-service attacks on both targeted remote Internet infrastructure and the RF spectrum. Due to the increasing trend of mobile operators offloading traffic from cellular networks to WiFi networks, the WiFi RF spectrum (2.4GHz and 5.2GHz) is now coupled with the cellular bands. Jamming the WiFi would cascade in a collapse of cellular networks.

Wi-Fi Protected Setup(WPS), Figure 1, was introduced in 2006 to facilitate establishment of secure connections, but in 2011 Stefan Viehbock found flaws in WPS [3]. APs from major vendors, such as Cisco, Belkin, D-Link, Linksys, and Netgear have been affected. APs' embedded operating systems, such as VxWork and dd-wrt, are also known to suffer from vulnerabilities. The preliminary results of this work have been presented [1]. In the light of some new vulnerabilities [2] we are working on more accurate propagation models and location estimation that also consider diurnal properties. We hope to be able to receive feedback from other members of the research community.

Question: can one wirelessly spread an infection of WPS/ WEP vulnerable APs by starting from one?

2. DATA COLLECTION AND ANALYSES

The data was collected by war-driving in four neighborhoods of Boston: Allston, Back Bay, Fenway and South Boston, shown in Figure 3. The hardware consisted of an ASUS Eee PC 1000HE, equipped with three TP-LINK TL-WN722N wireless N150 high gain USB Adapters and a GlobalSat BU-353 USB GPS navigation receiver.

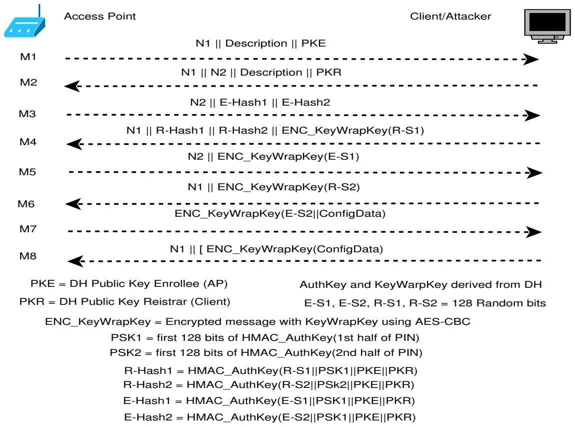

Access Point
Client/Attacker
M1
N1 || Description || PKE
M2
N1 || N2 || Description || PKR
M3
N2 || E-Hash1 || E-Hash2
M4
N1 || R-Hash1 || R-Hash2 || ENC_KeyWrapKey(R-S1)
M5
N2 || ENC_KeyWrapKey(E-S1)
M6
N1 || ENC_KeyWrapKey(R-S2)
M7
ENC_KeyWrapKey(E-S2||ConfigData)
M8
N1 || [ENC_KeyWrapKey(ConfigData)
PKE = DH Public Key Enrollee (AP)
PKR = DH Public Key Reistrar (Client)
AuthKey and KeyWarpKey derived from DH
E-S1, E-S2, R-S1, R-S2 = 128 Random bits
ENC_KeyWrapKey = Encrypted message with KeyWrapKey using AES-CBC
PSK1 = first 128 bits of HMAC_AuthKey(1st half of PIN)
PSK2 = first 128 bits of HMAC_AuthKey(2nd half of PIN)
R-Hash1 = HMAC_AuthKey(R-S1||PSK1||PKE||PKR)
R-Hash2 = HMAC_AuthKey(R-S2||PSk2||PKE||PKR)
E-Hash1 = HMAC_AuthKey(E-S1||PSK1||PKE||PKR)
E-Hash2 = HMAC_AuthKey(E-S2||PSK1||PKE||PKR)

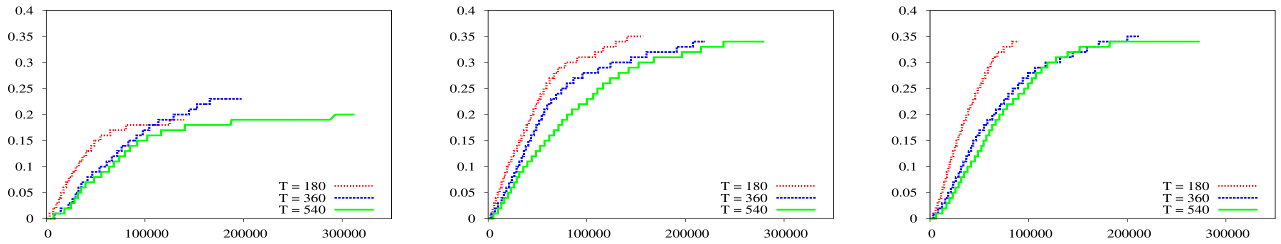
Figure 1: Simplified diagram of WPS protocol.

Two APs are considered to be connected if they are in R-proximity of each other. To analyze the connectivity graph, we investigated radii of 15, 30, 50, 75 and 90 meters. To estimate a lower bound for the range of APs, we computed the diameter of the convex hull of all the points where each AP was heard. Using our radius computation approach, we estimated 41 meters as the radius of an AP coverage. This radius would significantly increase at off-peak times when there is less interference. For example, based on our experiments at 4 am, a radius of 90 meters becomes much more plausible. At normal transmission power, WiFi signals can easily be heard from a distance of 25 to 50 meters, however most APs are configured to transmit at a lower power than they are capable of. If the transmission power is increased through the administrative interface of the devices and at off-peak times, WiFi signals can travel much farther and can be heard from a distance of 100 to 150 meters.

We collected a total of 32787 unique BSSIDs from Back-Bay; 15422 from Allston; 14756 from South Boston and 26306 from Fenway. Table 1 shows the basic statistics of WiFi AP encryption. As we can see surprisingly in all neighborhoods more than 11% of APs still use WEP, although is known to be flawed. Due to size limit we did not include all areas in the table.

Table 2 depicts connectivity statistics of APs using various radii. From the table, we can infer that generally a WEP connectivity graph has more components than a WPS connectivity graph, indicating that the spread of malware

WiSec'14, July 23–25, 2014, Oxford, United Kingdom
Copyright is held by the owner/author(s).
ACM 978-1-4503-2972-9/14/07. .



(a) R = 50m

(b) R = 75m

(c) R = 90m

Figure 2: Graph of spread, considering three different radii (50, 75, and 90) m, with 3 different duration of time to recover WPS PIN. X-axis is time (T) in minutes.

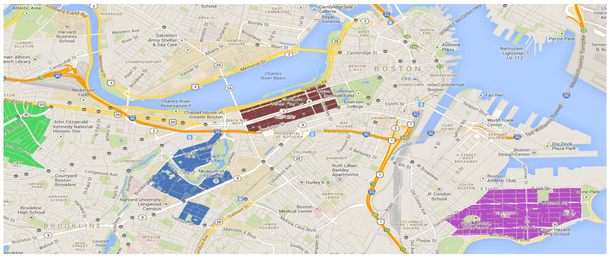


Figure 3: Coverage map in four neighborhoods of Boston

Encryption	Number of APs	Percentage
WEP	5369	16.38%
Open	5051	15.41%
WPA/WPA2	22367	68.22%
WPS	7809	34.91%

Table 1: Surprisingly in all neighborhoods more than 11% of APs still use WEP.

with small radii is less practical in WEP networks. However, when we combine WEP and WPS networks, the number of components is reduced to more than half which shows a significant improvement in terms of feasibility of attacks.

Based on the parameters we used for infection spread, the theoretical average upper bound in a single connected component is 32%. As seen in figure 2 with R = 50m, on average we can infect 19% to 23% in 97 to 137 days, with R = 75m, 33% to 35% in 109 to 194 days and for R = 90m, we reach 34% to 35% in 62 to 189 day.

3. CONCLUSION AND FUTURE WORK

In this work, we looked at the design flaws in WPS and how it can give an adversary leverage to compromise a connected network of APs. We passively collected beacon frames from APs in four neighborhoods of Boston, and we developed a SIR model to study the spread of an infection that exploits WPS and WEP vulnerabilities. Our experimental study showed the feasibility of such attacks, especially when WPS flaws are supplemented with WEP vulnerabilities. Interestingly, all the neighborhoods explored exhibit very similar infection and spreading characteristics even when they have distinct population demographics.

For a long time, APs have been considered as a self contained box, but current advancements in the field of networking advocates separation of control plane and data plane.

Radius	No. of Edges	Avg. Deg.	Conn. Comp.
WEP			
15	111739	42.62	216
50	306303	115.10	1
90	698785	261.30	1
WPS			
15	152744	40.02	124
50	614203	157.90	3
90	1497259	383.49	1
WEP + WPS			
15	425520	65.48	57
50	1535754	233.73	1
90	3726970	565.78	1

Table 2: Connectivity statistics of APs in Back Bay and South Boston, using different radii.

Many new wireless enabled systems are leaving the traditional designs. For example, Meraki produces many network appliances, including wireless APs, that have central cloud based control, which provides flexible administration. Roku produces digital media receivers that are updated regularly from the cloud by the producer. Although these approaches provide more flexibility and better opportunity, they are still mostly closed to third-parties and do not provide interoperability; Yet, incorporating a safe-update component to allow manufacturers and ISPs to patch security vulnerabilities in APs in a seamless manner, like Roku, could significantly help mitigate many such attacks that exploit misconfiguration and policies.

4. REFERENCES

[1] A. Sanatinia, S. Narain, and G. Noubir. Wireless spreading of WiFi APs infections using WPS flaws: an epidemiological and experimental study. In *IEEE Communications and Network Security (CNS) 2013*.

[2] Sophos. Gaping admin access holes found in SoHo routers from Linksys, Netgear and others. `http://nakedsecurity.sophos.com/2014/01/03/gaping-admin-access-holes-found-in-soho-routers\` `\-from-linksys-netgear-and-others/`, 2014.

[3] S. Viehbock. Wi-Fi Protected Setup PIN brute force vulnerability. `http://www.kb.cert.org/vuls/id/723755`, 2011.