



CENSUS
IT Security Works

INTRODUCING WIFIPHISHER

A TOOL FOR AUTOMATED WIFI PHISHING ATTACKS



wifiphisher

B-SIDES LONDON 2015

GEORGE CHATZISOFRONIOU (@_sophron) sophron@census-labs.com www.census-labs.com

> WHOAMI

- Security Engineer at CENSUS S.A.
 - Cryptography, WiFi hacking, web security and network security
- Academic research
 - Design of Privacy-enabling / Anonymity-providing protocols
- Lead author of wifiphisher



> AGENDA

- IEEE 802.11 ISSUES
- NETWORK MANAGER ISSUES
- EVIL TWIN & KARMA ATTACKS
- WIFIPHISHER
- COUNTERMEASURES
- Q&A



> WIRELESS COMMUNICATION

- Rapid growth in recent years
- People may access Internet anywhere and anytime
- “75% of Americans said that a week without WiFi would leave them grumpier than a week without coffee” –Iconic Displays



> IEEE 802.11

- Specification for WLAN communication
- Two basic entities
 - Station (STA)
 - Access Point (AP)
 - Identified by Service Set Identifier (ESSID)



> MANAGEMENT FRAMES

- Enable stations to establish and maintain communications
- Beacon frames
 - Transmitted by AP to announce its presence
- Probe request frames
 - Transmitted by the station asking information from an AP
 - A NIC would send a probe request to determine which APs are within range



> IEEE 802.11 ISSUES



> AP SELECTION

- No clarification on the case where multiple available APs are around with the same ESSID
 - Up to the software to decide
 - Most clients will choose the AP with the best signal



> UNPROTECTED FRAMES IN THE AIR

- Management frames are not cryptographically protected
 - WEP / WPA / WPA2 networks protect data only after the association has been established
 - Vulnerable against eavesdropping, modification or replay attacks



> WIFI JAMMING

- DEAUTH frame
 - A management frame (transmitted unencrypted)
 - Sent when all communication is terminated
- Kick out a client by forging DEAUTH frames
 - 1 from the AP to the client
 - 1 from the client to the AP
 - 1 from the AP to the broadcast address



> NETWORK MANAGER ISSUES



> ESSID PROBING

- Modern OS probe for every ESSID they have associated with in the past
 - Show me your ESSIDs, I'll tell you where you are (and maybe who you are!)



> WIFI AUTO-CONNECT

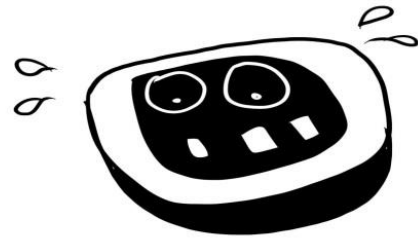
- Most of the time, devices will connect to an AP with a known ESSID without any warning
 - “Usability vs security” case
 - Flag auto-connect is enabled by default on Ubuntu, OSX and Windows 7



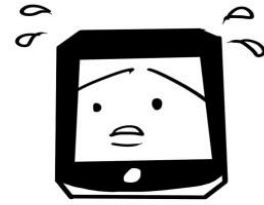
> EVIL TWIN ATTACK

1. Forge DEAUTH packets to disrupt existing connections
2. Create a phony AP modeled by the target AP





Target AP



Victim

DEATH
VICTIM!

I AM THE
AP!



Attacker

Evil Twin Attack

> OPEN NETWORKS

- Evil Twin attack against an open network
 - ALL clients will automatically connect to the rogue AP
 - This is a typical attack against captive portals



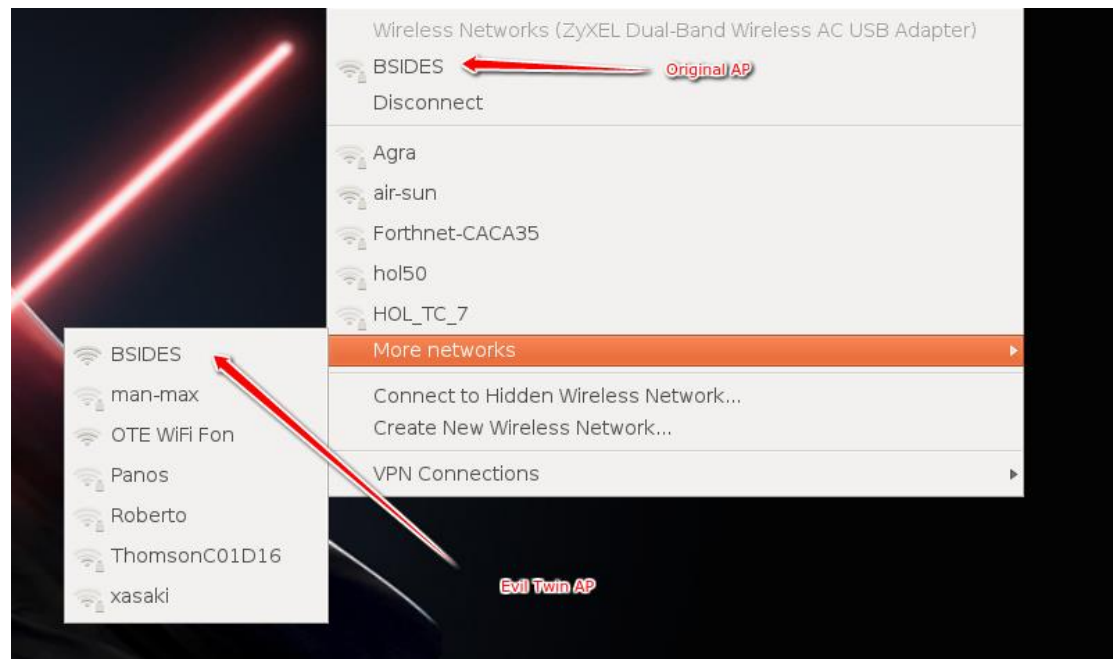
> ENCRYPTED NETWORKS

- Evil Twin attack against an encrypted network
 - Rogue AP can only be open
 - Attacker doesn't know the pre-shared key
 - Devices will note the difference in encryption and won't connect automatically to it



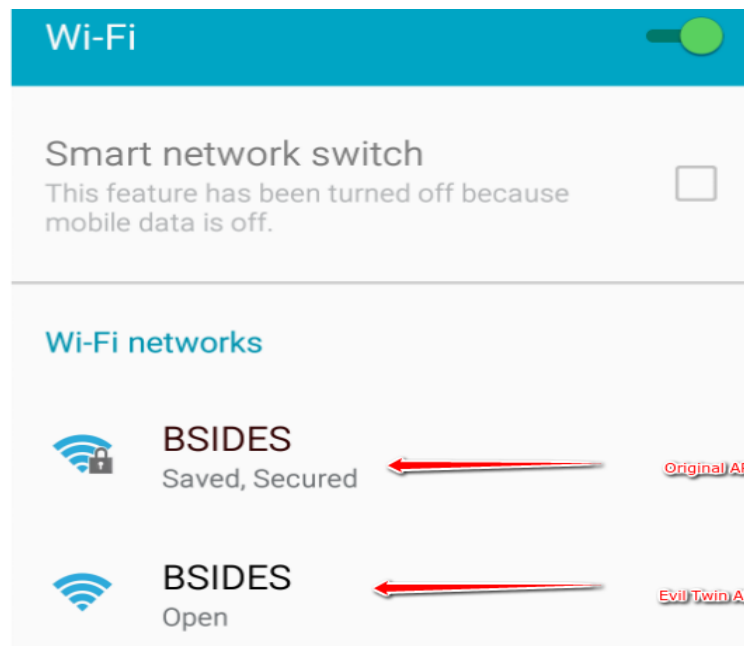
> UBUNTU BEHAVIOR

- Requires a manual connection to the unencrypted network



> ANDROID BEHAVIOR

- Requires a manual connection to the unencrypted network



> WINDOWS BEHAVIOR

- Connects after providing a warning that the network has changed



> KARMA ATTACK

1. Forge DEAUTH packets to disrupt existing connections
2. Create a phony AP based on probe request frames
 - The probe request frame must be intended for an open network
 - The attack is effective only if victim has already stored open networks
 - Most of the time, victim will auto-reconnect without warning



> KARMA OR EVIL TWIN?

- Depends on the target
 - Organizations that make use of captive portals are more exposed to Evil Twin
 - KARMA works better against individuals
 - If they have any stored open networks in their devices
- Both can be used at the same time
 - May raise suspicion



> GOT MITM, NOW WHAT?

- KARMA and Evil Twin aid the attacker to achieve MITM position
- Plenty of attacks to mount from there
 - Data sniffing
 - Data modification
 - Malware infection
 - Phishing



> WIFIPHISHER

- Automates the process of Evil Twin + phishing attacks
- Recently caught the attention of WiFi hackers
 - ~3300 stars and ~550 forks on Github :-)
- Requires no Internet connection
- Yes, it works on Kali Linux
- Requires two wireless network adapters
 - One capable of injection




```
Jamming devices:
```

```
[*] 2c:26:c5:74:40:1c - 1c:65:9d:91:b8:68 - 9 - air-sun  
[*] 2c:26:c5:74:40:1c - 1c:99:4c:d3:6e:30 - 9 - air-sun  
[*] 2c:26:c5:74:40:1c - 9 - air-sun
```

```
DHCP Leases:
```

```
1432462884 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42
```

```
HTTP requests:
```

```
[*] GET 10.0.0.62  
[*] POST 10.0.0.62 wfphshr-wpa-password=crippledblackphoenix
```

```
[!] Closing
```

Wifiphisher

> PHISHING PAGES

- Comes with a set of community-built templates for various scenarios
 - Router configuration pages
 - Fake a firmware upgrade and obtain WPA / WPA2 passwords
 - 3rd party login pages
 - E.g., those of social networking sites
 - Captive portals
 - Like the ones that are being used by hotels and airports





Web Administration

FIRMWARE UPGRADE:

A new firmware is available to improve functionality and performance.

DOWNLOAD AND UPGRADE:

Current Firmware Version: 1.04

WPA Password:

Submit

Router phishing page

> IDENTIFYING THE MANUFACTURER

- Beacon frames include the MAC address of the AP
- It is possible to determine the router manufacturer by the MAC address
- We can later customize the fake pages accordingly and make the phishing part more effective



> SUCCESS FACTORS

- Victim's network manager
 - Will it reconnect automatically or prompt a warning?
- Effectiveness of jamming
 - Depends on the power of the wireless card & the distance to the victim
- Awareness of the victim
 - For the social engineering part



> TECHNICAL DETAILS

- Requires Python 2.7
- Leverages:
 - Hostapd
 - Dnsmasq
 - And some others
- Custom web server using SimpleHTTPServer
- Custom jamming method using Scapy
 - Written by Dan McInerney



> FUTURE WORK

- Add KARMA attack
- Check if captured credentials are valid
 - Stop the attack only if the received credentials are correct
- Provide more phishing pages for different scenarios



> COME ABOARD

- Wifiphisher is open-source (under the MIT license)
- Join us!
 - Design phishing pages
 - Implement features
 - Fix bugs



> SIMILAR S/W TOOL :: LINSET

- Mounts Evil Twin attack to obtain WPA/WPA2 passphrase
- Written in BASH
- Supported by Seguridad Wireless



> SIMILAR H/W TOOL :: PINEAPPLE

- KARMA tool
- Comes with its own hardware
- Supported by HAK5
- Plenty of plugins (infusions) to customize your attack



> COUNTERMEASURES



> WIDPS

- Wireless Intrusion Detection and Prevention Systems
- Sensors scan the wireless spectrum and send the data to the WIPS server for analysis
- Server compares the MAC addresses and if needed provides immediate and specific information on the root causes



> 802.1X PORT ACCESS CONTROL

- Provides an authentication mechanism to devices wishing to attach to a WLAN
 - Robust mutual authentication
- The client provides credentials (username and password or a certificate)
- EAP-TLS or PEAP validate server's signature
 - Client authenticates the server. The server authenticates the AP.



> SECURITY AWARENESS

- Employees need to have a solid understanding of phishing attacks



> CONCLUSIONS

- 802.11 spec leaves room for different stack behavior
- Network managers favor usability over security
- KARMA and Evil Twin will be with us for some time



Q & A



Thank you!



CENSUS

IT Security Works