Stop WiFi Pineapple and Other Attacks Cold with Intelligent WIPS

WLPC Phoenix 2019

Robert Ferruolo
Technical Solutions Engineer
@raferruolo
RF@arista.com

Survey

- WIPS auto **detection** enabled on customer networks or networks you managed?

- WIPS auto **prevention/mitigation** enabled on customer networks or networks you managed?

Threat Categories

Rogue AP: May allow attackers to bypass perimeter security and gain access to data, systems, etc.

Evil-Twin / Honeypot AP: Users may unwittingly fall prey to a Man-in-the-Middle (MITM) attacks enabling hackers to spy on traffic, steal data / login credentials and infect systems.

Misconfigured AP: Opens networks to attack as a result of configuration errors, such an authorized / encrypted SSID accidentally deployed with encryption disabled.

Rogue Client: Clients that have connected to rogue APs may have become compromised (e.g. infected with malware).

Misassociated Client: Allows client to circumvent security perimeter and content filters. Client may become compromised.

Ad-Hoc AP: Uses peer-to-peer connections that enables users to circumvent security controls and risk exposure to malware.

Recent Attack Using WiFi Pineapple

US Justice Department’s Indictment

Related to:

- Olympic doping scandal
- Nuclear power operations
- Novichok gas attack

"Serebriakov's **backpack**, in particular, included "additional technical equipment that the team could also use to surreptitiously intercept Wi-Fi signals and traffic," the indictment reads. Though it doesn't spell out how that equipment could penetrate password-protected WiFi networks, it does mention that Serebriakov carried a **Wi-Fi Pineapple.** Those book-sized devices are designed to spoof Wi-Fi networks so that victims connect to them rather than the intended, legitimate one, acting as a **"man-in-the-middle"** capable of spying on or altering their subsequent internet traffic.”

Source: wired.com
https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/

Detecting Threats

What Works

- Wire-side packet injection / Marker Packets
- Wireless-side packet injection / Marker Packets

What Works Sometimes…

- Wireless-side tracing
- CAM table lookups
- Passive MAC address correlation
- Signatures

Preventing/Mitigating Threats

What Works

- Wire-side ARP poisoning
- Over-the-air ARP poisoning
- Cell splitting

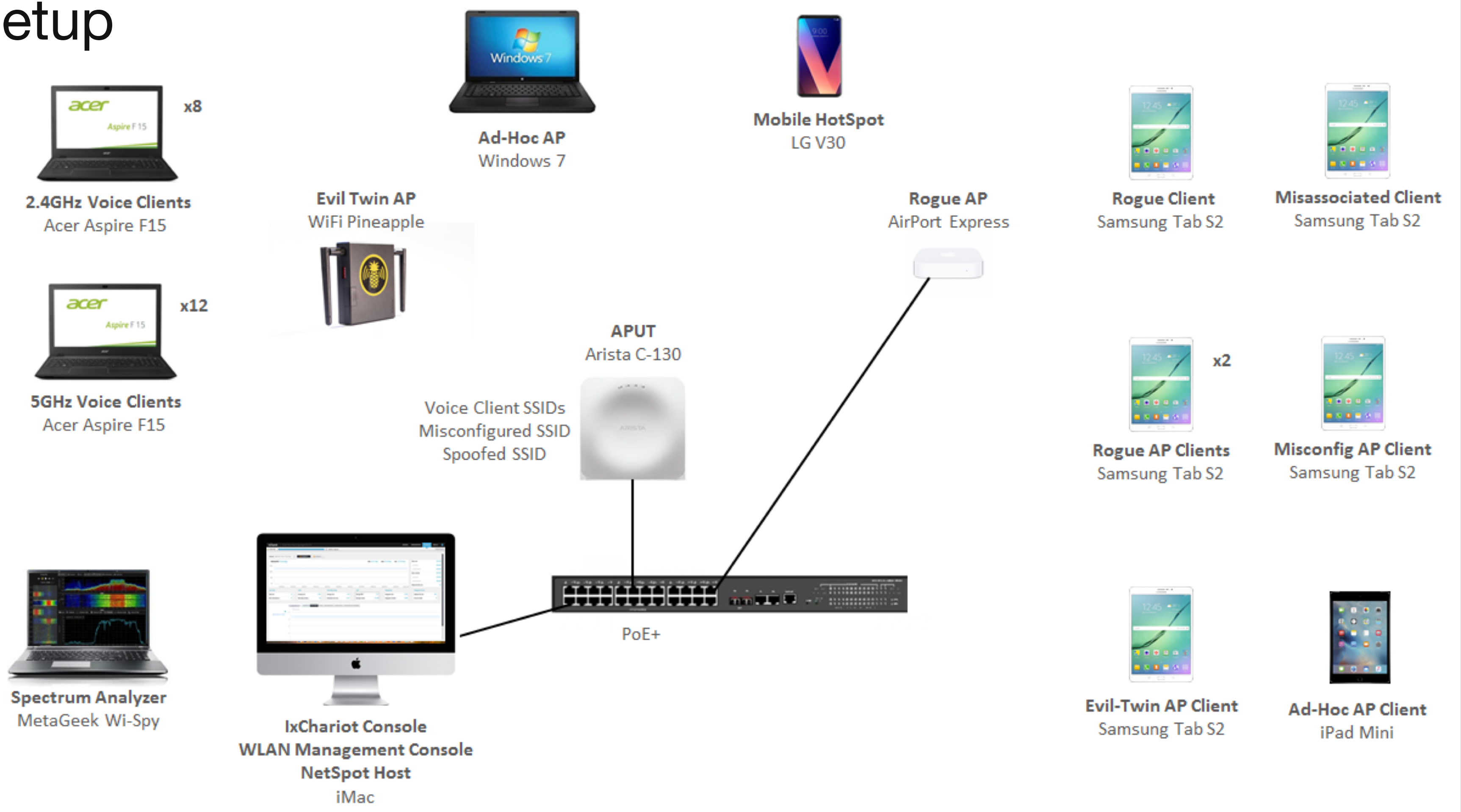
What Works Sometimes…

- Switch port blocking
- Tarpitting
- Over-the-air prevention (e.g. deauthentication if PMF is not used)

Tests

Test	Detection	Prevention
Rogue AP + Voice	Marker Packet	Wire-side ARP poisoning
Evil-Twin AP + Voice	Marker Packet + Authorized SSID Match	Over-the-air prevention
Misconfigured AP + Voice	Configuration compliance	All associations disallowed
Rogue Client + Voice	Marker Packet (to classify rogue AP) + Auto client classification	Rogue client associations disallowed
Misassociated Client + Voice	Auto client classification	Over-the-air prevention
Ad-Hoc AP + Voice	Marker Packet + To DS: 0 From DS: 0	ARP poisoning / cell splitting
All Threats Simultaneously + Voice	All of the above	All of the above

Setup



x8

2.4GHz Voice Clients
Acer Aspire F15

x12

5GHz Voice Clients
Acer Aspire F15

Ad-Hoc AP
Windows 7

Evil Twin AP
WiFi Pineapple

Mobile HotSpot
LG V30

Rogue AP
AirPort Express

APUT
Arista C-130

Voice Client SSIDs
Misconfigured SSID
Spoofed SSID

PoE+

Rogue Client
Samsung Tab S2

Misassociated Client
Samsung Tab S2

x2

Rogue AP Clients
Samsung Tab S2

Misconfig AP Client
Samsung Tab S2

Spectrum Analyzer
MetaGeek Wi-Spy

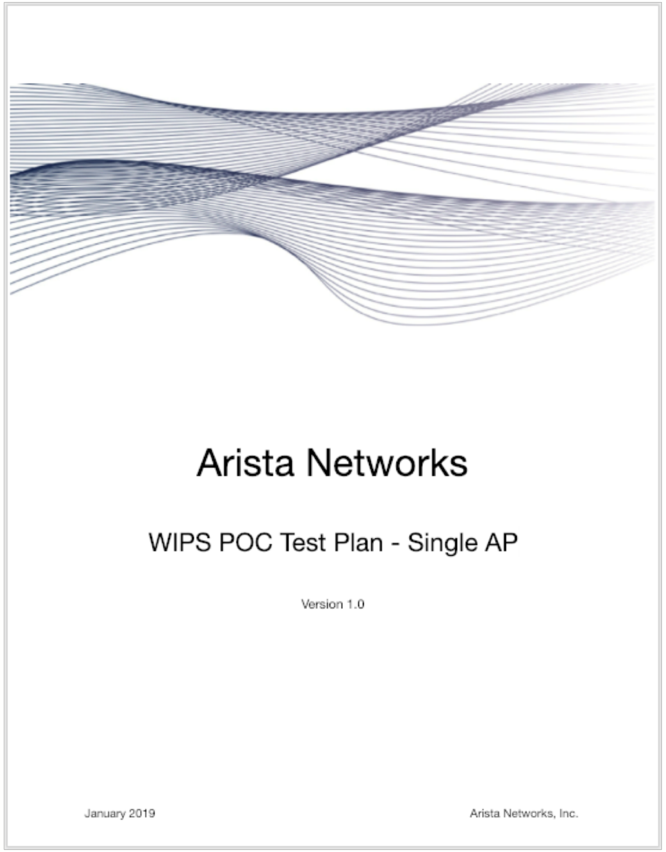
IxChariot Console
WLAN Management Console
NetSpot Host
iMac

Evil-Twin AP Client
Samsung Tab S2

Ad-Hoc AP Client
iPad Mini

Lab Mates

Resources



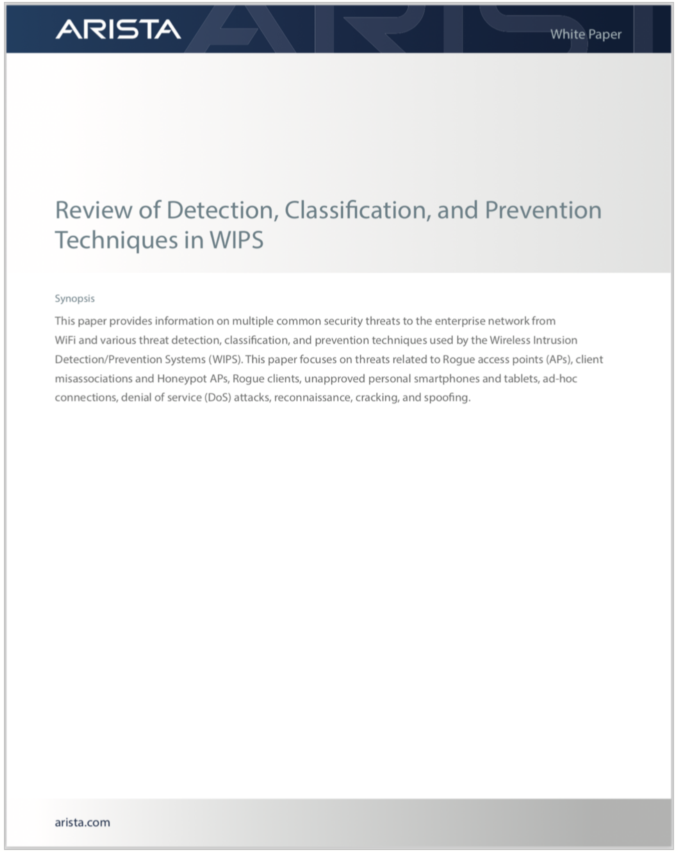
Arista Networks

WIPS POC Test Plan - Single AP

Version 1.0

January 2019

Arista Networks, Inc.



ARISTA

White Paper

Review of Detection, Classification, and Prevention Techniques in WIPS

Synopsis

This paper provides information on multiple common security threats to the enterprise network from WiFi and various threat detection, classification, and prevention techniques used by the Wireless Intrusion Detection/Prevention Systems (WIPS). This paper focuses on threats related to Rogue access points (APs), client misassociations and Honeypot APs, Rogue clients, unapproved personal smartphones and tablets, ad-hoc connections, denial of service (DoS) attacks, reconnaissance, cracking, and spoofing.

arista.com

Demo Video

Thank You!