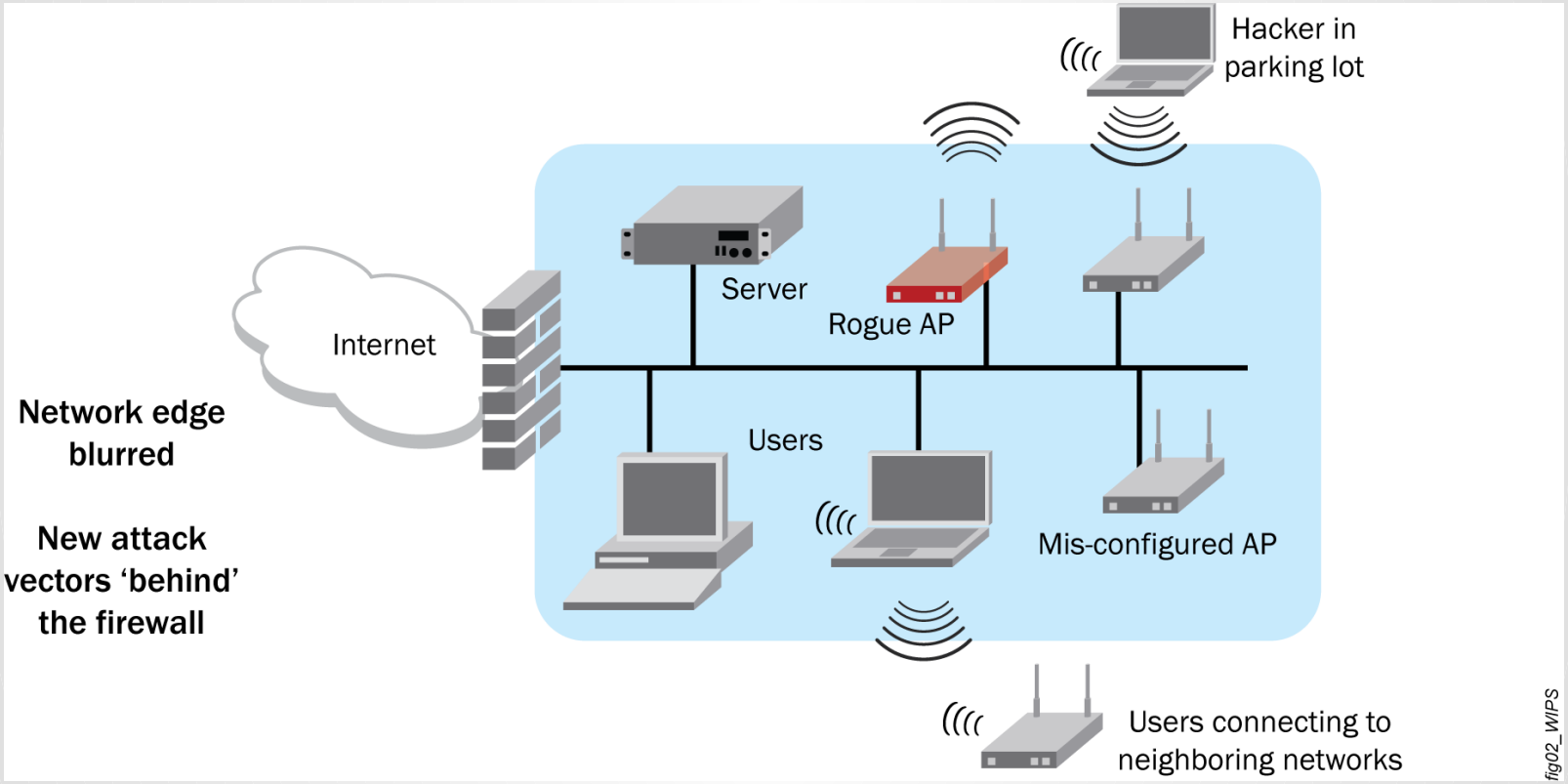
Wireless Intrusion Prevention

Traditional-Primary Purpose of WIPS

Prevent unauthorized network access to LAN’s and other information assets by wireless devices.


Hacker in
parking lot
Server
Rogue AP
Internet
Network edge
blurred
New attack
vectors 'behind'
the firewall
Users
Mis-configured AP
Users connecting to
neighboring networks
fig02_WIPS

In July 2009, the PCI Security Standards Council published wireless guidelines for recommending the use of WIPS to automate wireless scanning for large organizations.

Wireless scans alone cannot defend organizations against all threats from rogue access points.

The combination of integrated wired and wireless scans is the most effective approach to detection and containment of rogue devices.

To be successful at both goals, solutions must be able to:

- accurately assess the threat levels of devices
- provide a framework for prioritizing risk mitigation tasks
- alert staff of threats based on the enterprise’s specific security policies and requirements.

Effectively managing wireless security presents many challenges.

Because wireless networks are based on RF spectrum, they are inherently hard to control and allow malicious attacks much more easily than with wired networks.

Attackers can execute wireless attacks, such as denial-of-service and man-in-the-middle, using simple, off-the-shelf hardware and free software.

Another security issue involves well-meaning users who set up rogue (or unauthorized) consumer-grade access points (APs) in the workplace.

These users, unaware of the security implications of their actions, can easily compromise the corporate network’s security.

Related problems occur when laptops in dense urban settings or open, public Wi-Fi networks connect to the organization’s wired network.

Regulatory compliance is a key motivator that drives many organizations to implement stringent security processes for their enterprise wireless networks. The most common regulations are:

- Payment Card Industry (PCI) Data Security Standard
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX).

Despite setting strict policies that ban the installation of unauthorized APs, few enterprises have the tools or resources to adequately enforce these guidelines and to follow up and resolve threats consistently. Some organizations try to get by with periodic manual scans by security or network engineering teams using handheld scanners. This method is time-consuming and random, and thus provides little return on a significant investment.

Threat Identification

- Rogue AP– WIPS should understand the difference between Rogue AP and External (neighbor’s) AP
- Misconfigured AP
- Client Mis-association
- Unauthorized association
- Man in the Middle Attack
- Ad-hoc Networks
- Mac-Spoofing
- Honeypot / Evil Twin Attack
- Denial of Service (DoS) Attack

Traditional Prevention

WIPS solutions use one of three fundamentally different architectures, each offering distinct tradeoffs that should be part of any security assessment. Which one is right for you will depend on the individual emphasis put on cost, security and vendor lock-in.

PCI auditing features should allow organizations to monitor, audit and demonstrate real-time PCI compliance on the network.

- The system can alert network staff whenever a configuration error is detected, providing complete information as to how the configuration violates defined policy.
- Look for systems that seamlessly integrate so you can have a complete view into a wide range of requirements, including default password enablement and wireless association information.
- You will want detailed user tracking and session history, showing who is connected to your network, when they connected and where they’ve roamed.

Time Slicing

The first and most rudimentary WIPS architecture leverages an access point's (AP) existing radio for WIPS scanning. In other words, the AP momentarily slips from serving connectivity to Wi-Fi clients, to scanning for intrusion, and back to serving clients. In this approach, Wi-Fi APs are doing double duty: as APs forwarding traffic and as security sensors scanning the air for anomalies.

“Time” is Money

This approach is a cost-effective way to detect the presence of possible rogues, but without proper management tools to classify the devices found, using authorized APs to find rogues can potentially identify thousands of potential threats with no follow-up mechanism.

In addition, this approach is only effective in detecting rogues within RF range of the authorized APs.

In organizations without comprehensive wireless coverage, this approach potentially leaves a great deal of space exposed. It is precisely these uncovered areas where employees and hackers are most likely to install their own access points. Further, wireless networks may have inadvertent coverage holes that create blind spots.

“Collocation”

The second WIPS architecture is an integrated solution where a dedicated WIPS scanning radio is collocated in the client serving AP. The dedicated radio means the WIPS solution is always scanning the air, addressing the limitation of time slicing.

One Master

WIPS functionality can be supported with the deployed APs, holding costs down.

This consolidated functionality means a single AP is simultaneously servicing clients and policing itself. Configuring it with dual personalities can result in either lower WLAN performance, less effective security monitoring or perhaps both.

Over Lay

The third WIPS architecture is an overlay solution where dedicated WIPS sensors are deployed. These dedicated sensors provide the "always on" scanning necessary for tight security and are completely independent from serving wireless clients.

An overlay can locate rogue wireless devices, monitor for attacks and shield clients from attaching to rogue devices.

Overlay solutions bring the benefits of full-time scanning to bear, but add complexity.

- Network operations teams must manage yet another system.
- Systems must be updated constantly to keep them synchronized with the APs deployed on the network, which frequently change or are swapped out for maintenance.
- Too frequently, the overlay system does not recognize valid APs and contains them as rogues, which cuts off service to users.
- Overlay architectures are the most costly approach in terms of capital expenditure and operating costs.

Look for solutions that provide you with the ability to generate alerts and reports according to user-defined triggers, including a design that triggers action. Look for scans that can correlate and aggregate the data into a single device record that:

- Provides comprehensive information to assess and locate a potential rogue.
- Shows wireless scan result details, which includes SSID, number of discovering radios, encryption information, vendor, RF channel, radio MAC address or BSSID, and network type.
- Displays wireline scan data, including LAN MAC address, IP address, vendor and operating system.
- Uses wireless discovery information to link BSSIDs together, allowing and accurate identity to a single rogue that is broadcasting multiple BSSIDs.
- Compares the wired and wireless information to detect devices on the physical LAN, which avoids duplicate reports on a single rogue.

To find rogue APs that cannot be discovered via RF scans a successful strategy should be one that:

- polls the routers and switches on the network to obtain a full list of devices physically connected to the wired infrastructure,
- compares the MAC address of each device to a database of MAC address ranges enabling you to identify devices that fall within the ranges used by manufacturers of consumer-grade wireless access points.

Since these devices are rarely used by enterprise IT departments, they are the most common devices to be identified as rogues.

As an additional procedure for rogue detection, use SNMP and HTTP fingerprint scans, which allows the system to scan every IP address in a specified range. Since false-positive identifications are costly and time-consuming for IT to investigate, having the ability to interrogate a suspected rogue device to determine its operating system will help you weed out devices that are less likely to be rogues.

- It’s not all about configuring the AP’s. The Network needs to config the Laptop and devices too.

Cyber Crime

- In 2012 the FBI had over 1,000 agents in 56 Field offices – Intelligence Analysts and Forensic Specialists.
- Foreign Intelligence
- Terrorist
- Organized Crime
- Supply chain
- Trusted Insiders
- Proximity

2013 and the "Mobility" Factor

- Mobile malware increased more than 1,000% in 2012.
- Security researcher Andres Blanco from CoreSecurity discovered a serious vulnerability in two Wireless Broadcom chipsets used in Smartphones. 10/25/12 – The Hacker News.
- USB smartphone exploit turns Android into an invader – 01/20/2011 – Slash Gear
- 100,000+ Apps in Google Play considered "Suspicious" – 05/12/2012 – InAuth Mobile Security
- Cybercriminals can steal information about you from your social networking profile and posts and then tailor their attacks
- Negligent insiders are the leading cause of data breaches at U.S. companies and public sector agencies, according to a new study by the Ponemon Institute.

A global trend toward hactivism against domestic organizations and the U.S. Government.

- 46% of those surveyed in 2012 for enterprise level organizations indicated the belief that Hactivists posed the greatest threat.

WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox

File Edit View History Bookmarks Tools Help

wigle.net

My Web Search

Most Visited Getting Started Latest Headlines Famous High School ...

Home | Download | Forums | Post File | Query | Screenshots | Stats | Uploads | Web Maps | MapPacks/Trees | Wiki | Login

WIGLE.NET

Wireless Geographic Logging Engine: Making maps of wireless networks since 2001

83,407,830 wifi 2,015,557 cellular 1,743,793,877 unique observations

login user: password: login Don't expire auth cookie reset password or make a new account

news:

2,000,000 Cellular Networks
Thu Jan 10 11:20:22 2013

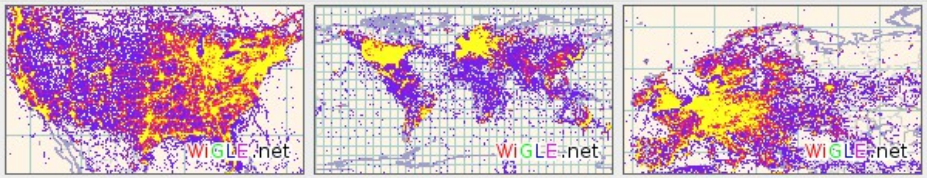
Congrats to user 'tehrhart' who found the two-millionth unique gps-located cellular network! We're a bit surprised by how fast that number has grown, and how many blue-squares that puts on the web maps. Keep on stumblin'.
-bobzilla

Updated Manufacturer Stats
Sun Dec 16 22:18:00 2012

We've updated the lookup tables for **Manufacturer Stats**, so they should be more useful. We have also updated the set of **Channel Stats**. Enjoy!
-bobzilla

80,000,000 nets ahoy
Tue Dec 4 22:35:07 2012

Yesterday, stalwart stumbler 's.mcduggal' notched the eighty millionth observed network in the WiGLE.net belt of oh-my-that's-alot-of-nets using the finest android nethugging package on github: WiGLE wifi! the counter keeps on ticking because of all of you madcap folks out there, and our purring pile of datakittens in here; safe



The wireless world this morning (GMT-6:00).

Find a wireless network by [**searching**] (must be registered) or [**browsing the interactive map**]

Add a wireless network to WiGLE [**from a stumble file**] or [**by hand**]

Add [**remarks**] to an existing network(must be registered)

See statistics: [**general**], [**personal**] (must be registered), or [**group**] (must be registered)

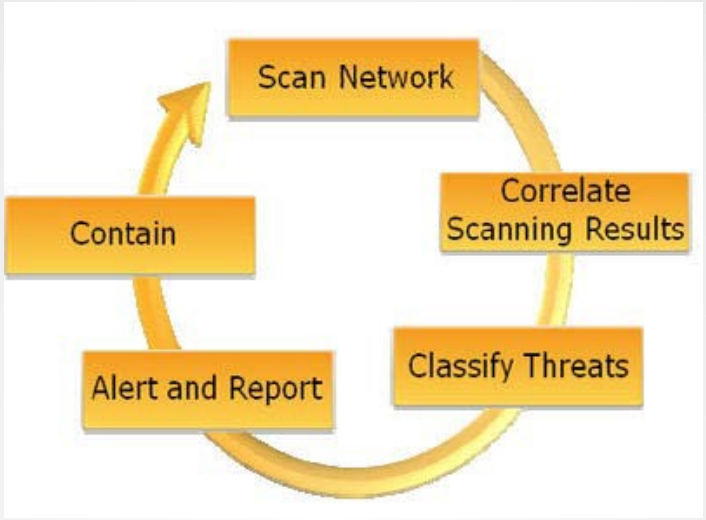
Download [**interactive clients**], [**location data for clients**],(must be registered) [**screenshots**], or [**random pictures**]

Engineering an Intrusion

- Most Smart Phones – Especially I-phones – Will automatically probe for Networks. Reading the SSID’s.
- Target the Individuals smart phone.
- Look up their address and find their home wireless through wigle.net.
- Honeypot or “Evil Twin” them at home when they look to connect to work.

How to Choose A Good WIPS Vendor

Today's Wi-Fi threats revolve more around client devices and rogue APs with custom embedded attack systems and are usually detectable only in the air. Everyone needs a way to uncover and thwart unwanted attempts to inject denial of service attacks, lure Wi-Fi client devices to malicious APs, piggyback onto a user's already established wireless connection, and more.



- Use of Third Party applications that are vendor neutral and can overlay the AP’s and Controllers.
- Have the ability to poll routers/switches for bridge forwarding data and ARP data allowing you to find out more information about rogue devices.
- Flexible rules for device classification. Look for additional triggers and reports to keep your network secure.
- The ability to monitor wired and wireless.
- Additional software client that allows Wi-Fi enabled devices to act as auxiliary RF sensors.
- The ability to correlate all the data to reduce false-positives.
- PCI compliance – must be real time.
- IDS Event Management – An ability to aggregate data for pattern detection.
- Manual and automated containment – an ability for immediate action even if staff is not present.

Alan Smith

Alan.smith@cox.net

402.212.5883