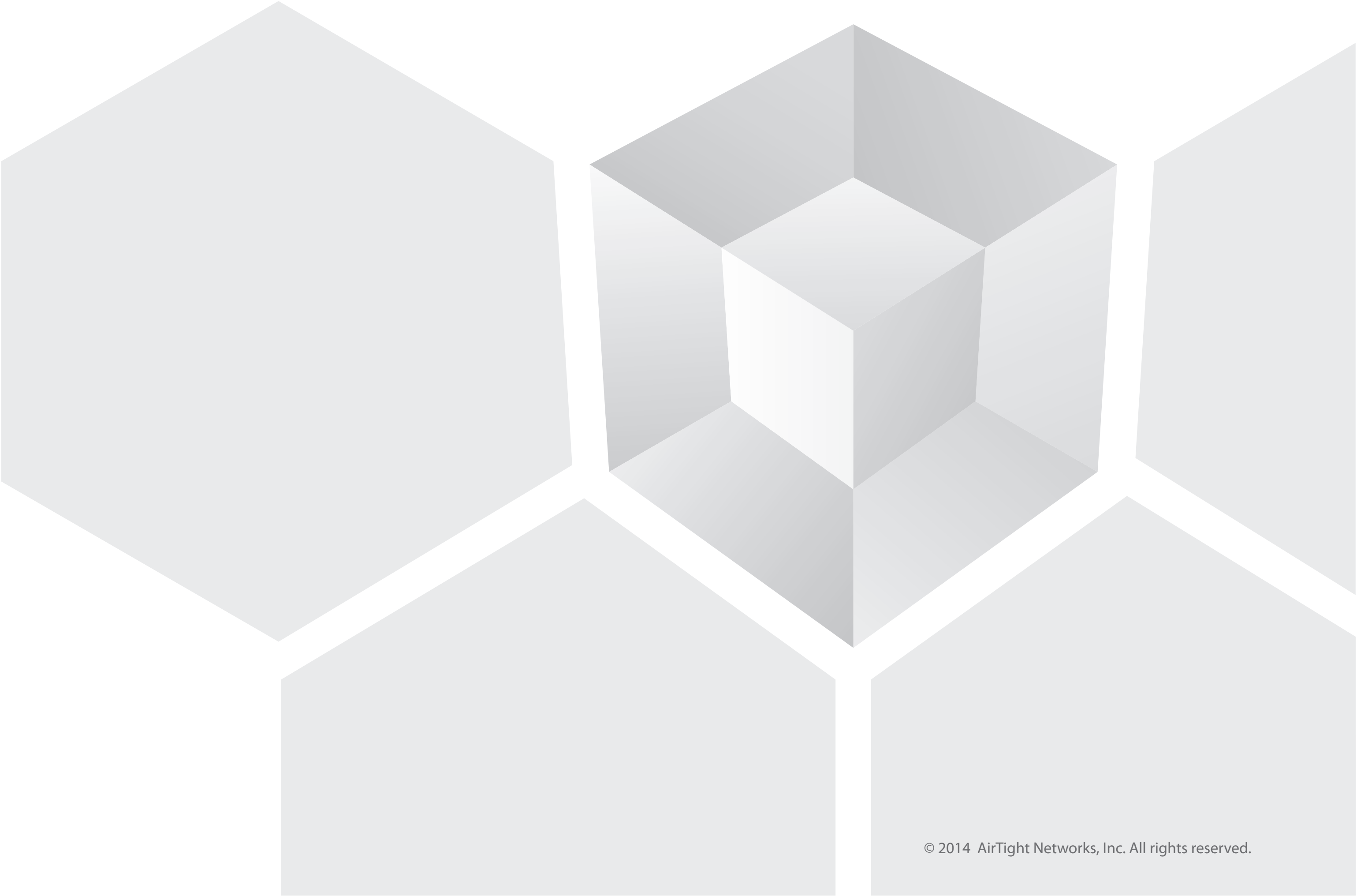
AIRTIGHT NETWORKS WHITEPAPER

Wireless Security Strategies for 802.11ac and the Internet of Things

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com

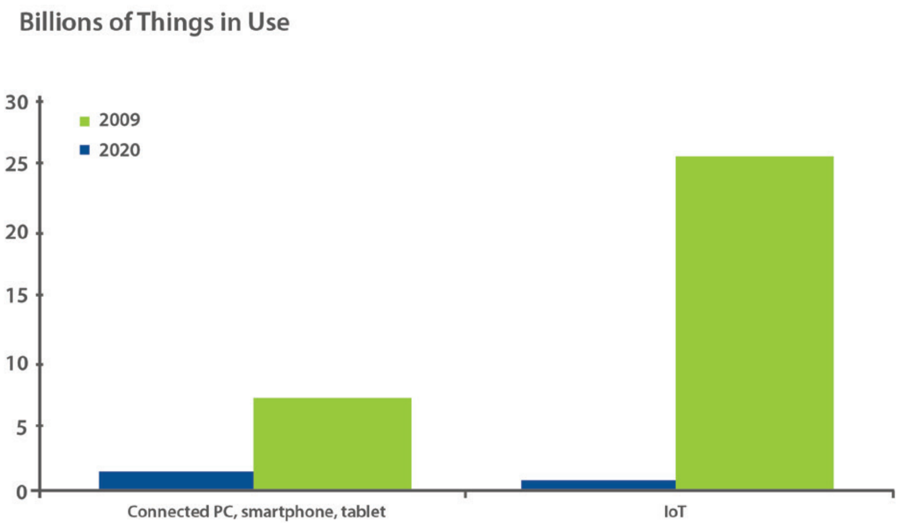


The "Internet of Things" is a double-edged sword. While it confers many benefits ranging from intelligent medical equipment and smart home appliances to wearable technology, it also opens networks up to an exponential risk of security vulnerabilities, cyber-attacks, and compliance issues. This paper discusses the magnitude of the IoT security challenge, identifies common client threat scenarios facing IT security professionals, and highlights AirTight's unique differentiators for effective wireless threat protection.

Wi-Fi Security Implications in an IoT world

According to Gartner, the ever increasing number of connected devices that make up the "Internet of Things" (IoT), which excludes PCs, tablets and smartphones will grow to 26 billion units installed in 2020 representing an almost 30-fold increase from 0.9 billion in 2009.

This technology is fast moving, with new devices introduced frequently, so forward thinking enterprises are already taking steps to address these concerns. Gartner analysts estimate that by the end of 2017, over 20 percent of enterprises will recognize the need to protect business units which use Internet of Things (IoT) devices, and as a result, will be required to invest more heavily in security.



Source:
Gartner Forecast: The Internet of Things, Worldwide, 2013

Moreover, organizations are burdened with universal security challenges:

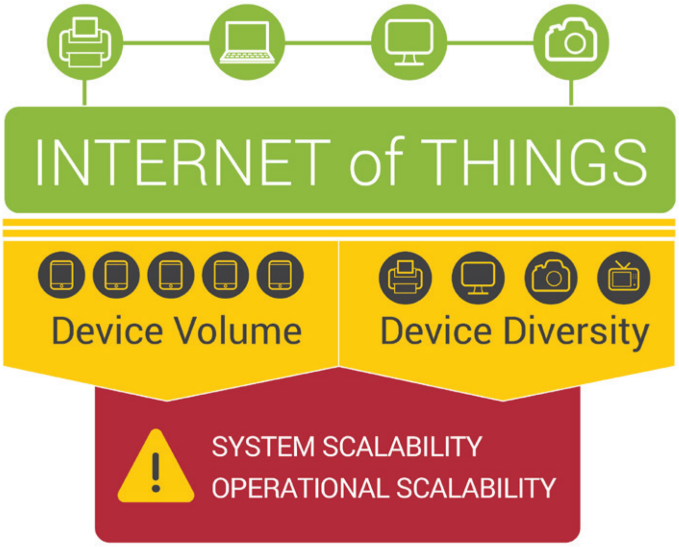
- Thin IT & security staffing
- Knowledge gap with respect to wireless vulnerabilities
- Increasing pace of breaches – the most recent being Home Depot and Target
- Compliance requirements – such as PCI and HIPPA
- Distributed networks

Earl Perkins, research vice president at Gartner underscores that security in the era of IoT is something of a "Wild West": "The IoT is a conspicuous inflection point for IT security -- and the CISO will be on the front lines of its emerging and complex governance and management." Perkins noted: "At this time, there is no "guide to securing IoT" available that provides CISOs with a framework for incorporating IoT principles across all industries and use cases. What constitutes an IoT device is still up for interpretation, so securing the IoT is a 'moving target.' However, it is possible for CISOs to establish an interim planning strategy, one that takes advantage of the 'bottom up' approach available today for securing the IoT." (Reference: http://www.zdnet.com/future-of-the-enterprise-heavy-investment-in-internet-of-things-security-7000033610/)

While the benefits of these market trends are fueling new applications, operational efficiencies and business value, the security challenges presented by these trends make it impossible for legacy 802.11n WLAN security systems to protect sensitive data, meet compliance requirements, and secure the enterprise.

Device Density, Device Diversity

System Scalability: One of the first and most obvious wireless security challenges prevented by IoT is system scalability. The significant number of new of Wi-Fi enabled devices that need to be monitored will stress the scalability of most Wireless IPS monitor systems. WIPS sensors will need to sort through more devices than ever before to determine which devices pose an actual threat. This applies to both Wi-Fi enabled clients as well as WLAN network devices. Any true "IoT-ready" security solution must be able to quickly auto-classify discovered devices as either approve or unapproved without the delay and inaccuracies associated with signature matching, threshold anomaly detection and CAM table look-ups.



The diversity of devices will present a second challenge to signature based WIPS systems. These signature based WIPS systems will be plagued by "signature gridlock" as vendors attempt to keep pace with influx of new wireless enabled client devices and their respective characteristics. The limitations of signature based WIPS systems combined with complex user-defined rules for threat detection can create a storm of alerts where security personnel are consistently chasing false alerts while at the same missing potentially catastrophic threats.

Operational Scalability: The last challenge is operational scalability. The volume of data being processed and stored for threat detection, forensics, and diagnostic analysis will become overwhelming to most systems, and even more so for administrators tasked with keeping the network secure and performing at peak performance. The fear of disrupting neighboring networks due to false alarms while safely enforcing wireless security policy on one's own network often prevents the network administrator from enabling automatic threat prevention. As such, IT personnel will need to painstakingly investigate every event raised by the monitoring system in order to determine what devices and connection behavior pose a genuine threat. This problem becomes compounded for organizations with a large number of distributed locations such as branch offices, retail locations, quick serve restaurants, and regional medical clinics where local IT staff is limited or non-existent.

Complete Visibility into 11ac Threats

In addition to the challenges presented by IoT, the adoption of the 802.11ac standard presents yet a different challenge to enterprise security. With 802.11ac comes a new format for wireless frame transmission that is unknown to the 802.11n systems. So, if both endpoints of a wireless connection are 802.11ac devices, their communication is invisible to the 802.11n monitoring radio. This inability of the 802.11n WIPS security sensors to monitor "pure" 11ac connections can leave an enterprise vulnerable. For example, critical systems in enterprise 802.11ac WLAN can be tricked into connecting to 802.11ac honeypot and the 802.11n WIPS system will be a sitting duck against it.

While it is true that the vast majority of Wi-Fi enabled clients in use today are not 11ac, new 11ac client devices are beginning to show up in force. And the numbers of these new devices continue to grow at an unprecedented pace. So it's imperative for enterprises to fully test their 11ac security solutions to ensure that they can in fact detect and block 11ac threats as advertised.

AirTight Networks 802.11ac WIPS and IoT

As the number of Wi-Fi enabled devices continues to explodes, so will the frequency of client based exploits. The frequency of client mis-associations will increase as Wi-Fi enabled clients continue to probe and automatically try to connect to an SSID that it has successfully connected to before. Malicious hackers are known to set up "Honey pot" APs with default SSIDs (e.g. Linksys, Netgear, default, etc.), hotspot SSIDs, and even corporate SSIDs outside of buildings and watch a large number of clients automatically connect to the AP. These APs can then inflict a variety of attacks on the client or attempt password stealing by presenting a login page to the client over the mis-associated wireless connection.

This scenario is very common for two reasons. If the device has connected to a Linksys, Netgear or other home or hot spot access point using the default SSID, it will automatically connect to another AP with the same SSID without the user being aware of the connection. Secondly, neighboring Wi-Fi networks can spill into the enterprise. Users may continue to connect to these networks to bypass network policy controls or they do not want their outbound traffic monitored.

Wireless clients can also create peer-to-peer connections. A peer-to-peer connection can be exploited by a malicious hacker who may try to then inflict a variety of attacks on the client such as port scanning to explore and exploit client vulnerabilities.

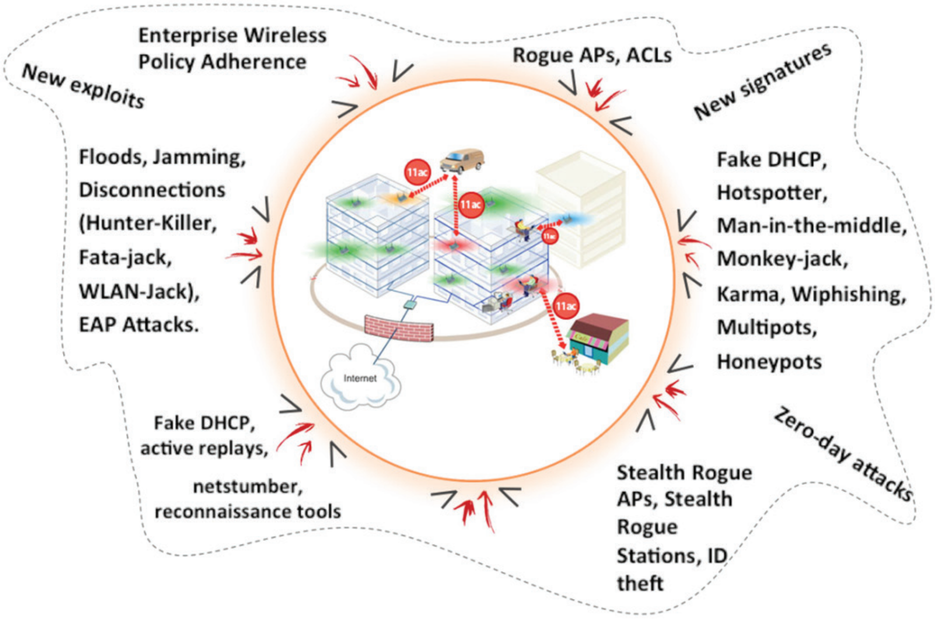
Rogue clients are those that are unauthorized to attach to an authorized corporate wireless network. This may occur through an authorized access point that has been mis-configured with encryption turned off, or through an access point that has had its encryption/authentication compromised and uses the key to connect to a properly configured authorized access point. Clients connecting to rogue access points also fall into this category.

Denial of service attacks are a threat that can wreak havoc on a large number of devices simultaneously. There are various forms of wireless denial of service attacks, but they typically involve flooding a channel or channels with de-authentication or similar packets that terminate all current and attempted client associations to access points. In the context of IoT, a denial of service attack could have a devastating impact on any enterprise reliant on interconnected wireless devices, such as hospitals and industrial applications.

To defend against these client based threats, an IoT-ready WIPS will need to determine which client connections pose a genuine threat or violate the network security policy. While new attack vectors will need to be addressed on a case by case basis, an advanced WIPS system using a protection oriented security paradigm will provide huge dividends in an 802.11ac-enabled IoT world.

AirTight WIPS is the only true 802.11ac wireless intrusion prevention system designed to protect the enterprise from current and future wireless threats without signature updates and heavy operational overhead. AirTight's patented wireless intrusion prevention (WIPS) technology allows for fully-automated 24X7 protection, with zero false positive / false negative operation, requiring minimal IT involvement for mitigation of wireless threats or compliance reporting.   It now has the ability to monitor 2000 active wireless devices per AP/sensor, which is critical as industries of all kinds move into realms of wider connectivity and prepare for an IoT-ready security strategy.

- Equally effective on all types of wireless threats
- Eliminates the time and effort of manually inspecting newly discovered Wi-Fi devices
- Protects both the network and the Wi-Fi clients
- Eliminates false positives and false negatives
- Patented Multi-channel, multi-threat and multi-level prevention
- Goes beyond simple de-authentication and uses several advanced prevention techniques depending on the type of wireless threat



Customers can confidently turn on prevention to let AirTight 802.11ac WIPS precisely block only those Wi-Fi connections that violate their corporate policies or pose a threat to their network security, without affecting legitimate Wi-Fi communication on own or neighbor's networks. Ironically, all competing (so-called WIPS) vendors recommend their customers NOT to turn on intrusion prevention with the fear that it may interfere or take down own or neighbor's Wi-Fi network.

Equally important is the capacity of AirTight's cloud management system to scale to hundreds of thousands of devices being monitored across multiple geographies and customers. This scalability is coupled with AirTight's patented 802.11ac wireless intrusion prevention (WIPS) technology, which allows for fully-automated 24X7 protection, with zero false positive / false negative operation, requiring no IT involvement for mitigation of wireless threats or compliance reporting.

Conclusion

With the increasing number of Wi-Fi enabled devices, the Internet of Things poses a serious threat to IT security. Client based vulnerabilities and malicious attacks will continue to compromise sensitive data and disrupt business operations. AirTight is helping network professionals prepare for the onslaught of the IoT by scaling up network monitoring and threat prevention capabilities on its 802.11ac platforms and providing the necessary safeguards to protect your business. AirTight 802.11ac access points with embedded WIPS are uniquely ready for the Internet of Things (IoT), so enterprises can confidently deploy Wi-Fi while minimizing security risks.

Comprehensive Cloud - Managed Wi-Fi