E-Book

Wi-Fi Security with More Control & Less Complexity

Table of Contents

Mobility Meets Security

Are the consumer devices in your environment exploding? Are your employees bringing their own devices? And has mobility become mission-critical rather than just convenient to your business?

With the rapid expansion of employee owned (BYOD) and corporate-issued consumer devices in the enterprise, organizations have the potential to usher in new levels of user productivity and convenience.

However, whilst your organization demands mobility, it remains the responsibility of IT to maintain appropriate levels of security.

Organizations are hitting a crossroads when planning for both secure and flexible network access. With a variety of users and devices craving connectivity, it is a difficult balance, on the one hand IT wants to allow users the freedom to connect and roam, however this must not come at the expense of network security.

Staff
Organizations typically provide wireless access to their staff today, as it increases flexibility within the workplace. With corporate-issued devices typically centrally managed, it is an easier task for IT to manage the on-boarding of internal devices versus user-owned smartphones and tablets etc. That said, Although easier, it is still not '*easy*', given the increasing number of devices requiring wireless connectivity, with often limited resources to support mobility initiatives.

BYOD
Still a buzzword to some, BYOD provides organizations with the opportunity to improve worker flexibility while simultaneously reducing IT spend. The challenge with consumer devices is how to allow access to the corporate network without compromising security, or overburdening the IT department given an often lack of central management, making onboarding difficult.

Guest
No matter where we go, we expect wireless connectivity, and organizations recognize this for their visitors. The challenge of course is how much do we really trust outsiders connecting to the infrastructure? We need to be able to supply Internet connectivity or network access but in a secure manner. We also want our visitors to have a good experience, which is why we must make access straightforward.

How Do You Secure Your Network?

Some organizations opt for bare bones protection with open connections or PSK (pre-shared key). Others implement certificate-based access to ensure that every user and device is known to the network and restricted appropriately according to their role, but WLAN's provide much more than authentication these days.

As a result of the ever-changing landscape of mobility-focused networks, an increasing number of security measures are moving to the edge of the network. Today, the WLAN infrastructure is responsible for not only authenticating, but also policing; monitoring and reporting connected users, devices, and applications.

Wireless networking has gone through several evolutionary steps to equal – and in some cases, exceed – the security found in wired networks. The first step in this evolution was the development of pre-shared keys, or PSK. Each device in a network uses a pre-shared key to encrypt traffic, thus providing additional security. The disadvantages of classic PSK include the fact that it is impossible revoke the network-wide key should an individual leave the organization, as well as the fact that it is relatively easy to crack.

Today, the clear choice in authentication for enterprises that are deploying or upgrading wireless networks is 802.1X. However, moving from PSK to 802.1X can prove to be challenging, as some devices do not support 802.1X or are cumbersome to set up. This can lead to the choice between the purchase of new equipment or a compromise in security. 802.1X also faces challenges when used to secure devices not owned by the enterprise, such as those of guests, students, subcontractors etc. Because 802.1X requires the installation of a software client, it is difficult or impossible to use on such unmanaged devices.

In the near future, other challenges will arise from a sharp increase in wireless connected devices through IoT (Internet of Things) developments. Devices such as lighting and air-conditioning, building controls and surveillance sensors etc. will require Wi-Fi connectivity. Many of these additional endpoints will not support enterprise levels of authentication, and organizations may be faced with reverting to PSK based network, leaving the embarrassing prospect of having the network hacked through a light bulb a distinct possibility.

Quite the predicament, with organizations having two typical options:

- 802.1X – Secure but certainly not simple and may cause unnecessary overhead for IT
- PSK - Simple but by no means secure in most cases. Leave it for home networks.

Balancing Security With Simplicity

With a range of devices to support, IT departments are looking for a simple way to on-board and secure both corporate and personal devices, whether BYO or guest. However simple and secure are not two words that are typically associated with one another.

IT departments are also looking for context - understanding who is connected, what devices they can connect with, which apps they are permitted to use, and where they are able to roam. Why? Because mobility has changed the way we approach network security at the access layer, and context is key to a successful deployment.

Though using IEEE 802.1X is the most secure approach to Wi-Fi authentication, this method is typically only implemented for devices managed by IT staffs, where they have control over the domain infrastructure, user accounts, and wireless clients being used. For BYOD, contractors, or guests, the IT staff may not have the access rights required, the knowledge to configure 802.1X clients for all the different wireless devices involved, or even the time to perform such tasks. Future devices used within IoT scenarios will most likely not even support 802.1X. The next best option has traditionally been to use a pre-shared key for these devices. As already discussed, however, classic PSK trades off many of the advantages of 802.1X such as the ability to revoke keys for wireless devices if they are lost, stolen or compromised, and the extra security of having unique keys per user or client device.

To draw on the strengths of both pre-shared key and IEEE 802.1X mechanisms without incurring the significant shortcomings of either, Aerohive has introduced a new approach to WLAN authentication:

'Private' PSK
Private PSKs (PPSK) are unique pre-shared keys created for individual users on the same SSID. They offer the key uniqueness and policy flexibility that 802.1X provides with the simplicity of pre-shared keys, without any of the inherent drawbacks. As the keys are still industry standard WPA2-PSK's, they are compatible with any device that supports PSK today, requiring no additional software to be installed on the client device. For the user, PPSK's are a simple method of accessing the network, and for the administrators who now know exactly who is connecting to the network, there are powerful possibilities available with context-based controls and reporting.

Enabling Mobility for Guests, BYOD, and IoT

The complexity of WLAN design will continue to increase over the coming years as more devices go mobile, Aerohive's PPSK reduces the burden placed on IT teams to on-board, secure, and monitor the wireless network. Aerohive's Private PSK addresses the security and management challenges of legacy clients, mobile devices, and guests that cannot be moved to 802.1X, allowing enterprises to use 802.1X where they can and Private PSK everywhere else. This dramatically improves Wi-Fi security and manageability while it reduces wireless LAN deployment and operating costs.

- Private PSKs are unique pre-shared keys created for individuals or groups of users on the same SSID.

- They allows users to be uniquely identified and authenticated similar to RADIUS, with tight policy enforcement including what apps the user has access to, time of day connectivity, location availability, bandwidth restrictions or priorities, and layer 7 firewall policing.
- No complex configuration required for clients. The same simplicity of PSK, making it ideal for BYOD and guest deployments.
- Easily revoke access, for a single device or individual, without affecting everyone else.
- Thousands of keys can easily be managed and distributed via the cloud or mobile application, or you simply allow users to self-register.

Who, When, What, Where, Wi

Authentication is only part of the security challenge. Once devices are connected, that's when the real work should begin. As previously mentioned, it's all about knowing who is on your network, and that's where PPSK comes in, with the ability to unlock contextualized information.

Aerohive's security suite consists of a powerful application firewall, user profiling, quality of service, location based restrictions, VPN and GRE tunneling, RADIUS server, all built-in to every single access point, so now organizations can ensure a secure mobility platform that starts with a single AP.

Unbeknown to the user who simply clicks and connects seamlessly to the network, there are powerful security services running in the background of the wireless infrastructure that determine who the user is. Once a user has entered their PPSK (or AD credentials), requesting access onto an Aerohive wireless LAN, the infrastructure will quickly analyze every detail of this user, and assign a user profile based on their role within the organization. This could simply be staff or guest for example, however organizations can be as granular as required, say by year groups within a school.

This user profile stays with the user as they roam the wireless infrastructure, with active security mechanisms that permit/deny the use of certain applications (AVC), throttle or enhance the users performance (QoS), restrict usage in certain locations, tunnel their traffic to a DMZ (GRE), and limit how long they are allowed to spend on the network. Once assigned a user profile, the infrastructure will next determine what device the user is accessing the network with, be it personal or corporate-issued, and depending on the type, will potentially assign an entirely new set of attributes to limit BYOD capabilities, or simply to enhance or restrict the performance and capabilities of certain devices (smartphones or tablets) on the network to ensure network efficiency and a productive working environment.

With an arsenal equipped of strong authentication, simplified onboarding, application visibility and control and strategic alliances, organizations can rest assured that their network is ready for the next evolution of the mobility driven world with Aerohive's PPSK and security suite.

About Aerohive

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our tens of thousands of customers worldwide, every access point is a starting point. Aerohive was founded in 2006 and is headquartered in Sunnyvale, CA.

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA

phone: 408.510.6100
toll-free: 866.918.9918
fax: 408.510.6199

www.aerohive.com
info@aerohive.com