NetSHIELD™

Use Network Access Control to Secure Your Wireless Networks

WHITEPAPER

Table of Contents

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

PREFACE

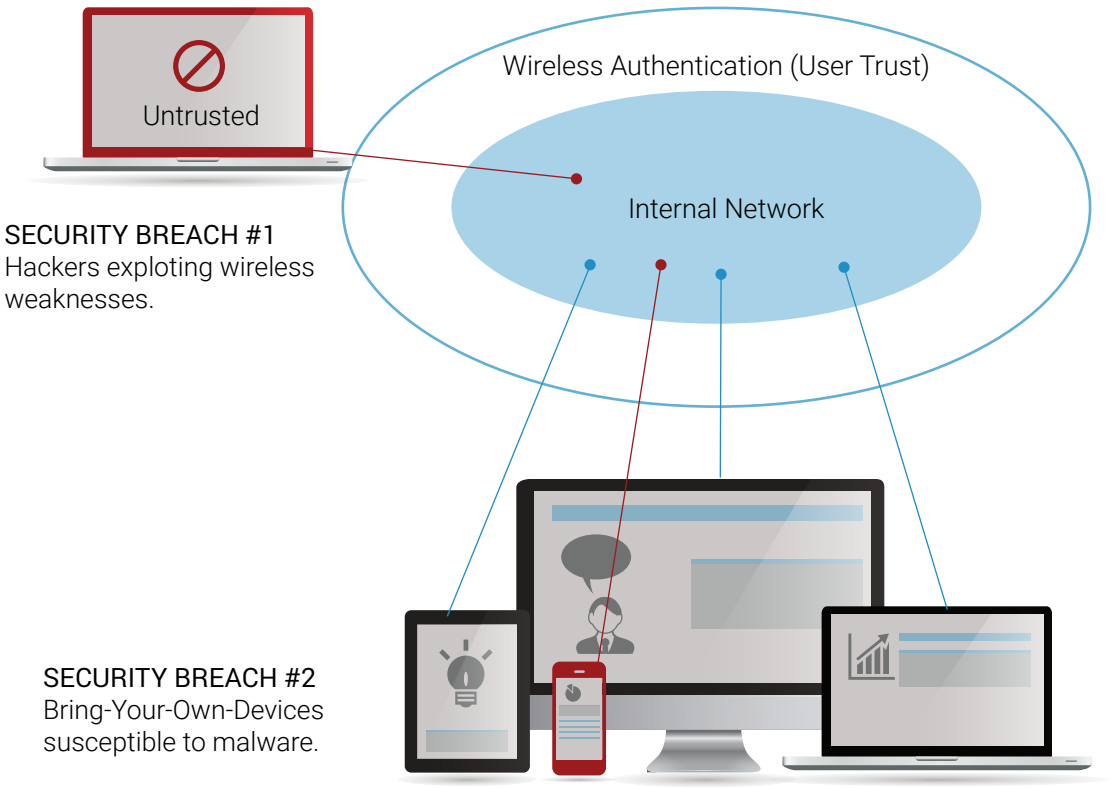
Two Immediate Threats to Your Network

At SnoopWall, we strive to keep our eyes and ears open not just to the industry "best practices," but the industry's "actual practices," when it comes to information security. We have found that in many cases, end users assume that the security features of their WLAN architecture – the entry point for many employee-owned mobile devices (BYOD) – is a sufficient level of security in a BYOD environment. This is a dangerous assumption in most cases, and most are unaware of the threats facing them this very moment: 1) Many wireless deployments have critical weaknesses that enable an untrusted user, or attacker to gain access to your network – even if the latest WPA2 encryption is used. 2) Trusted employees can utilize known WLAN credentials and apply them to their personal devices – devices which are unmanaged by the organization and pose a security risk as a result. Unmanaged devices are likely to be more susceptible to malware, which effectively tears down the walls of perimeter security devices like firewalls, since the attackers are effectively brought inside the organization. Untrusted devices pose such a serious risk today that 51% of business networks were breached due to employees using their personal devices.

Figure 1

Breach #1 can occur from a hacker near the premises, or in some cases far away, with a high-gain antenna.

Breach #2 refers to users that are trusted by the organization and therefore have wireless credentials that they can input into their personal devices, which either have malware already or are more susceptible to malware.



SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

NETWORK ACCESS CONTROL (NAC)

Protect Against Both Attack Vectors

NetSHIELD provides a powerful defense layer to the untrusted device problem – regardless of it being a hacker that has exploited wireless weaknesses to gain access to the network, or an employee who is trusted but connects an untrusted device. Mobile device management can be a helpful tool to convert an untrusted device to a state that you consider to be trustworthy, but before you can do that, you must have a way to enforce the following policy: untrusted devices should be denied access from trusted networks. As simple as this may sound, this has historically been a very expensive and time consuming proposition. We will discuss how NetSHIELD is designed to provide immediate visibility and control over untrusted devices, without the need for the complex and costly integrations that have plagued NAC deployments in the past.

THREAT #1

Wireless Weaknesses in Detail

In this section we will address the most common wireless configurations and deployment scenarios associated with them. Additionally, we will discuss current exploits that have been developed and what type of risk these exploits pose to your network. In many cases, one's ability to exploit these vulnerabilities is just a YouTube video demonstration away.

Figure 2

Common wireless configurations and deployment scenarios

	None (22%)	WEP (28%)	WPA/WP2 (50%)
None	Free Wi-Fi		
MAC	Guest Wi-Fi		
Pre-Shared Key (PSK)		Old barcode scanners	Some hand-held devices, smaller networks
LEAP			Old desktops, hand-held devices
EAP-FAST			Desktops, Laptops
PEAP (v0)			Desktops, Laptops, Mobile Phones, Tablets
EAP/TLS			Desktops, Laptops, Mobile Phones, Tablets
PEAP-EAP/TLS, PEAP v2, PEAP v1, EAP/GTC			

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Encryption: None
Authentication: None
Deployment scenarios: Free Wi-Fi

Open Wireless Networks

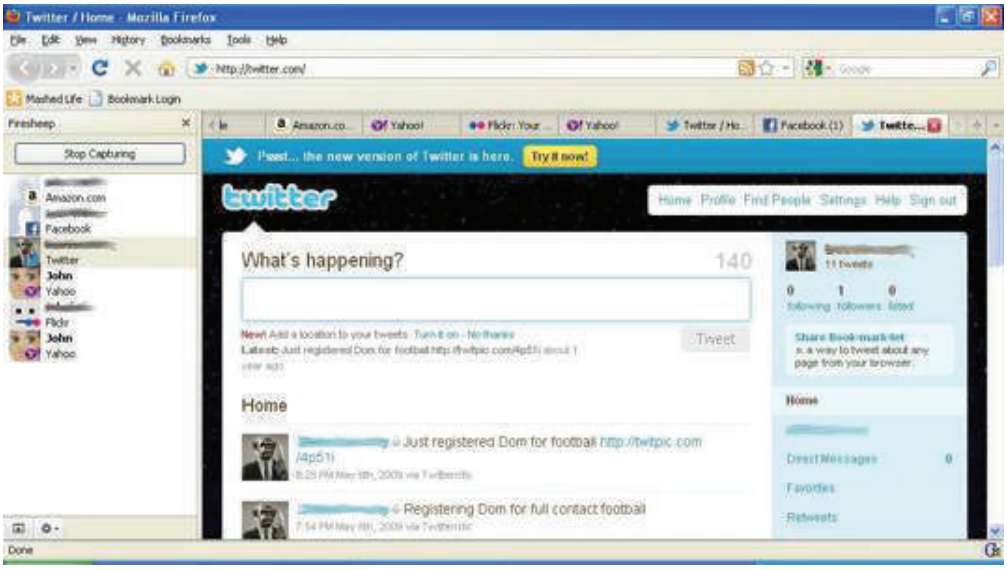
The most convenient to both deploy and to connect, open networks make sense in many scenarios. However, their acceptance to the mainstream should not connote secure access. Because the wireless network is unencrypted, all traffic sent on the network that is not already encrypted can be sniffed, including some email messages and email passwords, most VoIP sessions (not Skype), and non-HTTPS web traffic. Not all social networks encrypt traffic, and social networks that have this https feature may not have it enabled by default. Aside from being able to view traffic passively, a hacker could jump onto or "sidejack" a session – meaning that they can immediately, on their own computer, access the account of the user they are sniffing. A few years ago, this attack was made popular with a tool called "Firesheep," which places icons of persons logged into their accounts on the left sidebar of the Firefox web browser, which the user can then click on and gain live access to their account without the need for a password.

Technical Details

Wireless traffic can be passively sniffed using popular Linux distributions such as Backtrack, along with supported wireless cards. Programs such as Kismet and airodump-ng utilize "monitor" mode which captures 802.11 frames on a given channel, and saves this information in a pcap format. These files can then be analyzed in Wireshark or other packet analysis tools for the purpose of reconstructing voice audio streams, images, web pages, passwords, etc.

Figure 3

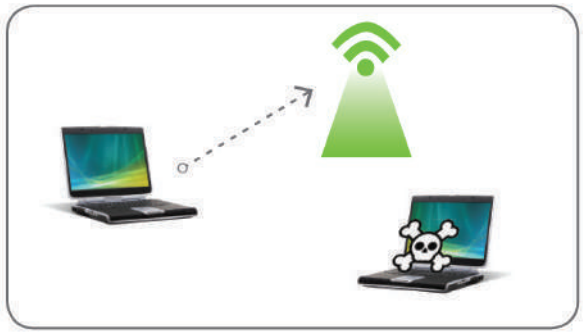
Example of hijacking an account using the "Firesheep" Firefox-plugin taken from http://beboblog. johnbe-bo.com/2010/11/11/-firesheepfailwitha-sus1005h.aspx



SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

Figure 4
Passive sniffing on an unencrypted wireless network is relatively trivial to perform



Encryption: None
Authentication: Captive web portal and/or MAC address-based
Deployment scenarios: Free Wi-fi, Paid Wi-fi, Guest networks, etc.

Captive Portal or MAC-Based Authenticated Wireless Networks

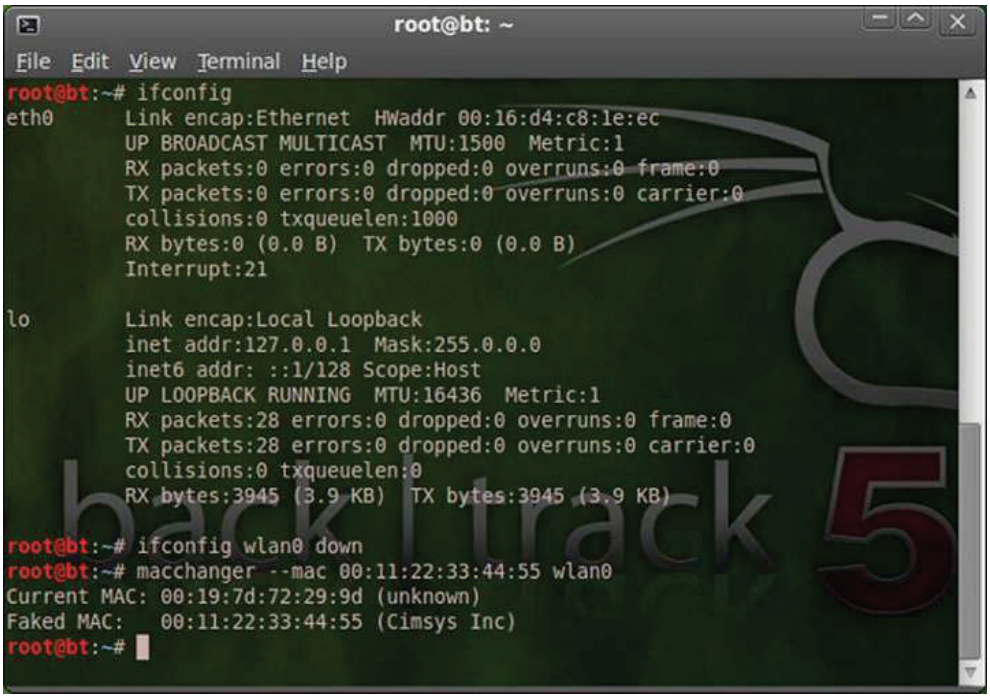
Adding slightly more security to the previously mentioned open unencrypted networks, Captive Portal, or MAC-based authentication wireless networks, usually greet the end user with a landing page as soon as they open a web browser. Here they can be led to a secure payment gateway, or perhaps click a check-box indicating that they agree to all of the terms of service for the wireless network. Some of these pages, as is the case with many hotels, require a login pass-phrase that was given to you separately. The real danger here is that secure payment gateways, passwords, or any other interaction here might give the end user a false sense of security, as it is common to associate a password with security, or a secure payment gateway with security. The reality is that many of the same attacks mentioned above can also be applied here. There is one slight twist, implied by the title, and that is when an authenticated device is granted access based on its MAC address. In order for active attacks to be performed, the MAC address of the device must be copied or spoofed by the individual attempting to breach security. While this is not an option for most users due to operating system limitations on Windows, it is trivial for a determined hacker, because MAC addresses are visible for all active wireless devices.

Technical Details

Using a Linux distribution such as Backtrack, one may analyze the MAC addresses that are present that also appear to be sending and receiving traffic – meaning that it is the MAC address of an authenticated device that may be web browsing or doing something else while authenticated. Once a target address is changed, the attacker can replace his or her MAC address to match the target and become authenticated to the network from a wireless perspective. Passive sniffing may also reveal the default gateway and IP address range used to communicate on the network, and with that information one can gain full access to the targeted network.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Figure 5
How to spoof a MAC address using Backtrack - taken from http://www.overclockedtechies.com/wp-content/uploads/2012/02/mac-changer.jpg



Encryption: WEP 64 or 128 bit
Authentication: Pre-shared Key (most common)
Deployment scenarios: Old barcode scanners/ handheld devices, older wireless networks

WEP Encrypted Wireless Networks

The security flaws associated with WEP networks were severe enough for the Payment Card Industry (PCI) standards to institute a mandatory phase out of this technology by June 2010, in order for merchants to continue using major credit cards. An attacker may gain access to a WEP-encrypted network after using one of many free cracking tools available. These tools enable one to discover the encryption key of the network, which may then be used in the connection process to gain full access to the network. Additionally, all neighboring traffic from other users can be sniffed and decrypted with the cracked key, meaning that some email passwords, VoIP conversations, etc. are visible to a hacker.

Technical Details

Using the Aircrack-ng suite, one can collect enough wireless traffic on a WEP network to run through the supplied encryption attack tools. This may be accelerated by actively causing network devices to generate response traffic, to the point that almost any WEP network key may be cracked in a few minutes.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

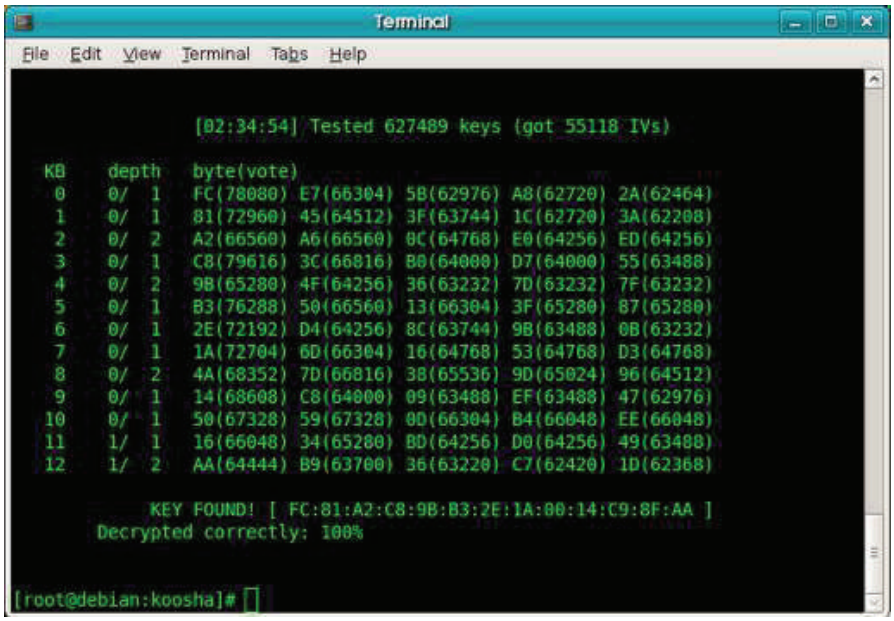


Figure 6
Example of a WEP key cracking taken from http://en.wikipedia.org/wiki/Aircrack-ng

Encryption: WPA/TKIP/WPA2/AES-CCMP
Authentication: Pre-shared Key
Deployment scenarios: Small networks, hand-held devices without advanced wireless capabilities, laptops, desktops

WPA/WPA2 Pre-shared Key Networks

With a few exceptions, WPA and WPA2 pre-shared key networks offer a similar level of security, and were a major improvement to the old WEP encrypted networks. To gain access to these networks, the attacker must crack the WPA/WPA2 key. By design, this takes considerably longer to do than WEP networks and with long, complex keys it is impractical to crack. Long, complex, identical keys however are subject to security challenges from an operational perspective. Complex keys are more prone to being emailed around to those who need access. Because the keys are universal, anyone with knowledge of the key has the ability to access the network at any time – and if you have employees whose employment is going to end, you either have to be sure that they don't have knowledge of the key, or be prepared to do a system-wide key rotation, which in many cases is impractical. Additionally any person with the key has the ability to sniff other users' traffic on the network. From a BYOD perspective, a person can apply this key to their personal mobile device to gain unauthorized access to the network.

Technical Details

There are two ways to crack a WPA/WPA2 pre-shared key. The first is by performing a dictionary attack and loading it into a program such as Aircrack-ng. The second is a bruteforce attack. Russian software company Elcomsoft, in 2008 released a GPU-based and FPGA-based WPA/WPA2 pre-shared key crack program, which brings 10-100x performance increase for a single system, which can be clustered together to divide and conquer. There are also cloud services that may be used to perform cracking for a fee.

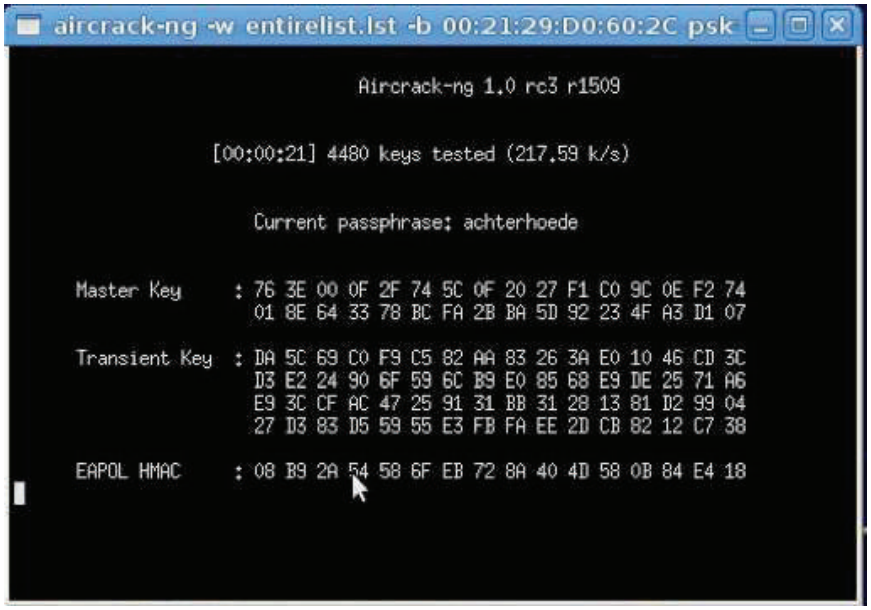


Figure 7
Example of WPA/WPA2-PSK dictionary attack with Aircrack-ng, taken from http://security-online. blogspot.com/2010/12/cracking-wpawpa2-under-linux.html

Encryption: WPA/TKIP/WPA2/AES-CCMP
Authentication: Private Pre-shared Key
Deployment scenarios: Proprietary to certain wireless vendors. Small networks, hand-helddevices without advanced wireless capabilities, laptops, desktops

Private Pre-shared Key Networks (Vendor Proprietary)

Private pre-shared key networks are an improvement from an operational security perspective because a single key is used for a given MAC address, and when a user departs the organization, it is possible to revoke the old wireless key. Aside from that, these networks are still vulnerable to the attacks that affect WPA/WPA2 networks. However in this case, in order for one to access the network after recovering the pre-shared key, he or she must spoof their MAC address to match that of the original client where the key was derived.

Technical Details

There are two ways to crack a WPA/WPA2 pre-shared key. The first is by performing a dictionary attack and loading it into a program such as Aircrack-ng. The second is a bruteforce attack. Russian software company Elcomsoft, in 2008 released a GPU-based and FPGA-based WPA/WPA2 pre-shared key crack program, which brings a 10-100x performance increase for a single system, which can be clustered together to divide and conquer. There are also cloud services that may be used to perform cracking for a fee.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Encryption: WPA/T-KIP/WPA2/AES-CCMP
Authentication: LEAP
Deployment scenarios: Older enterprise networks; warehouses /hand-held scanners

LEAP Authenticated Wireless Networks

Unlike the previously mentioned "Pre-shared key" encrypted networks, which pose the operational challenge of deploying and rotating a single wireless key to all devices, LEAP networks may use a username and password (often a Windows or domain login) that can be authenticated against one's pre-existing domain credentials. Once a device is authenticated to the network, it is given a unique "non-shared" key that it uses to encrypt its traffic. The weak link in this process is the authentication action itself, which sends enough information about the user credentials for a determined hacker to derive a password. In many cases, deriving this password not only grants wireless access to the attacker, but also access to the domain, email, etc.

Technical Details

LEAP uses the Microsoft MS-CHAPv2 protocol to exchange username, challenge, and password hashes, and this transaction occurs in the clear, meaning that it can be sniffed and recorded by an attacker. Once recorded, tools such as Joshua Wright's LEAP tool may be used to launch a dictionary attack against the password hash. A brute force attack is also possible, aided by cloudcracker.com, which takes an average of half a day to crack the password under this authentication scheme.

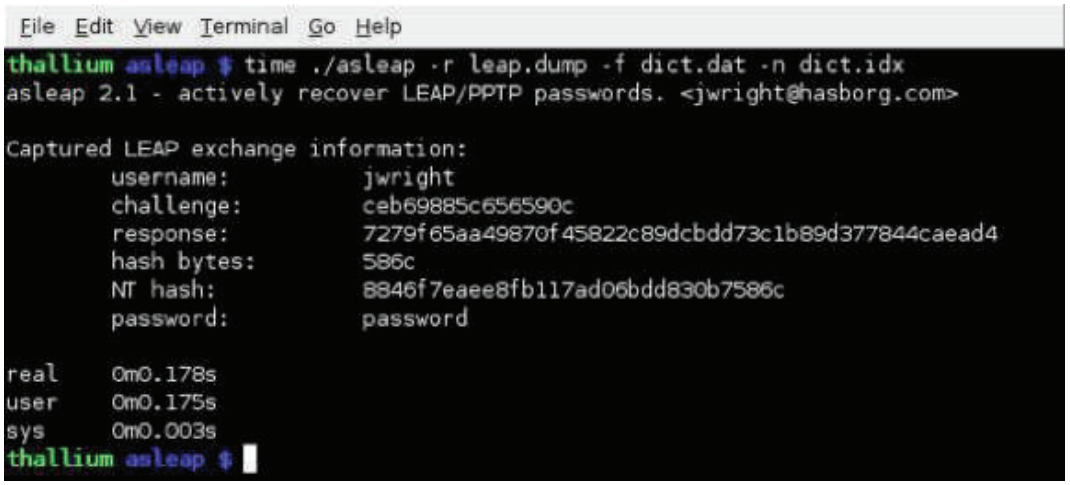


Figure 8

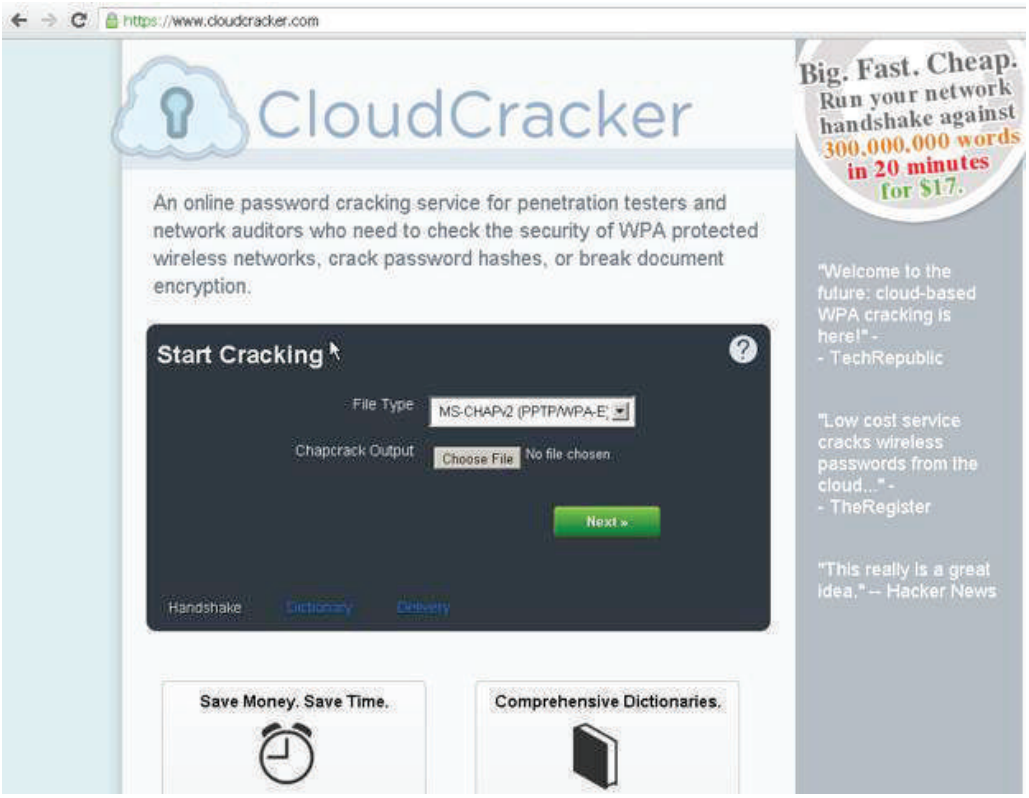
Username and MSCAHPv2 challenge/response cracking performed by asLEAP offline dictionary attack.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

Figure 9

Brute force attack of wireless credentials is available online at cloudcracker.com.



Encryption: WPA/T-KIP/WPA2/AES-CCMP
Authentication: EAP-FAST
Deployment scenarios: Older networks; often upgraded from LEAP

EAP-FAST Authenticated Wireless Networks

EAP-FAST was the response to the weaknesses discovered in the LEAP protocol. The weakness lies in the deployment, which can either be convenient, or secure, but not both. The convenient, over-the-air deployment method, while only intended to occur once, can be sniffed, which minimizes the risk exposure to exist only when connecting new devices to the network for the first time. The impact of this attack is to bring EAP-FAST networks back to the same level of security as LEAP authenticated networks.

Technical Details

When the protected access credentials (PAC) is deployed in automatic mode during "phase 0," the PAC, which is used for securing all subsequent authentication with a client, can be sniffed and captured. Phase 2 authentication credentials (MS-CHAPv2) are susceptible to offline dictionary attack. At the time of this writing there is not automated attack tool to exploit this, however it theoretically could be done using both Wireshark and asLEAP.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Encryption: WPA/T-KIP/WPA2/AES-CCMP
Authentication: PEAP
Deployment scenarios: Most enterprise environments today – desktops, tablets, laptops, and smartphones

PEAP Authenticated Wireless Networks

PEAP is perhaps the most common enterprise wireless deployment, yet the client devices – particularly iOS and Android devices - are often configured in such a way that makes it vulnerable to the same attacks that threaten the security of LEAP wireless networks. This is a common but serious flaw in wireless deployments today. Its popularity is derived from the fact that one's domain credentials can also be used to enable a device to access the wireless network, which means that there is less intervention from IT in order to manage wireless provisioning.

Additionally, wireless access is naturally revoked when one's domain credentials are revoked. The problem is that it is either expensive, or impossible to restrict the wireless device to only interact with the correct wireless network when it attempts to access the network. Meaning that if an attacker attempts to impersonate the correct network, and the wireless device does not validate a certificate presented to it by the hacker, it will assume that it is interacting with the valid network. In this moment, the attacker collects just enough credential information to mount an attack and discover full access credentials. Now the hacker has access to the wireless network. Additionally, this attack does not need to be performed on site, but wherever another wireless device is present that is configured to connect to the valid network. A CEO walking through the airport in proximity to a hacker's laptop is all that is required for the attack to occur, and the attacker could later arrive on company site to access the wireless network. Using cloud services at a nominal fee, the credentials can be extracted within 24 hours.

Technical Details

Wireless clients susceptible to this attack are configured to not validate the server certificate of the authentication server it is interacting with during its connection to the wireless network (this is the most seamless way to deploy). Android devices automatically accept invalid certificates, and iOS devices prompt the user to accept the invalid certificate (When does anyone ever say "no" to that question, if it means that they get access?). In order for Windows laptops or desktops be configured otherwise, so that it can validate this server certificate, it must either have a server certificate deployed on the device (not the easiest operation to be performed by IT on EVERY wireless device), or IT must subscribe to a public certificate authority, just as websites subscribe to authorities like Verisign, Thawte, DigiCert, etc., in order to appear as authentic to the end user device.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Once the attack is successful, the hacker will have obtained the MD4 hash of the password, which is all that is required to authenticate to the network, provided that they have modified their WPA supplicant to submit this hash in place submitting the hash of a given password. Additionally, this MD4 hash is vulnerable to further rainbow table or dictionary attacks, which could yield to the hacker the domain credentials of the victim.

Figure 10

Use of freeradius-wpe on a laptop masquerading as a valid access point. Username and MSCHAPv2 challenge/response are captured. Taken from http://www.willhackforsushi. com/?page_id=37

Encryption: WPA/T-KIP/WPA2/AES-CCMP
Authentication: EAP/TLS
Deployment scenarios: Large enterprise, internal PKI structure

EAP/TLS Authenticated Wireless Networks

EAP/TLS networks are considered the most secure wireless networks to deploy. Their adoption is stalled due to the complexity required to deploy and manage the network. Certificates must be installed on both the servers and clients in the wireless network. The only way for an attacker to gain access to this type of network is to have the client digital certificate and passphrase used to protect it, or to have obtained a lost/stolen device. In the case that a hacker is able to copy the digital certificate from one device to another device, the wireless network would have no way of knowing that the hacker's device was impersonating a valid device.

Overall Observations

Wireless security encryption and authentication mechanisms, with the exception of MAC authentication and EAP-TLS, are based on the paradigm of trusting end users by way of a pre-shared key, or by a username and password. When devices were controlled, managed, and secured by the same organizations, it was generally assumed that trusted users operated trusted devices, and thus the end user trust mechanisms were sufficient to be applied to device trust as well. EAP-TLS, while offering device-based authentication, is not widely deployed because of the impractical nature of its deployment. One might argue that the underlying mechanism for trusting a device based on the MAC or EAP-TLS methods is also based on user trust as well in many cases.

RISKS

Created by Wireless Threats

The following heat map represents our view of the risk that a given WLAN configuration presents to internal network security. Based on this, BYOD devices that are untrusted by IT have a certain likelihood of accessing the internal network. For example, there is a high risk that an employee with knowledge of the organization's WPA2 pre-shared key will be able to apply the same key to their personally owned device, which has not yet been trusted by IT. Hackers do not have this knowledge by default, but are able to exploit weaknesses in wireless configurations. Doing so enables them access to the network and in some cases the ability to passively decrypt data, and so this was also included in the table.

Heat Map of Risks Without NetSHIELD

High Risk | Medium Risk | Low Risk

Threat	Open	MAC Auth	WEP PSK	WPA/WPA2 PSK	WPA2 PRIVATE PSK	LEAP	EAP FAST	PEAP	TLS
Hacker decrypting data									
Hacker assessing network									
Untrusted BYOD accessing network									

Heat Map of Risks With NetSHIELD

High Risk | Medium Risk | Low Risk

Threat	Open	MAC Auth	WEP PSK	WPA/WPA2 PSK	WPA2 PRIVATE PSK	LEAP	EAP FAST	PEAP	TLS
Hacker decrypting data									
Hacker assessing network									
Untrusted BYOD accessing network									

Figure 11

Adding NetSHIELD to an internal network provides an immediate layer of defense against untrusted devices, and directly impacts the likelihood of an untrusted device gaining access to the network.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

Use Network Access Control to Secure Your Wireless Networks

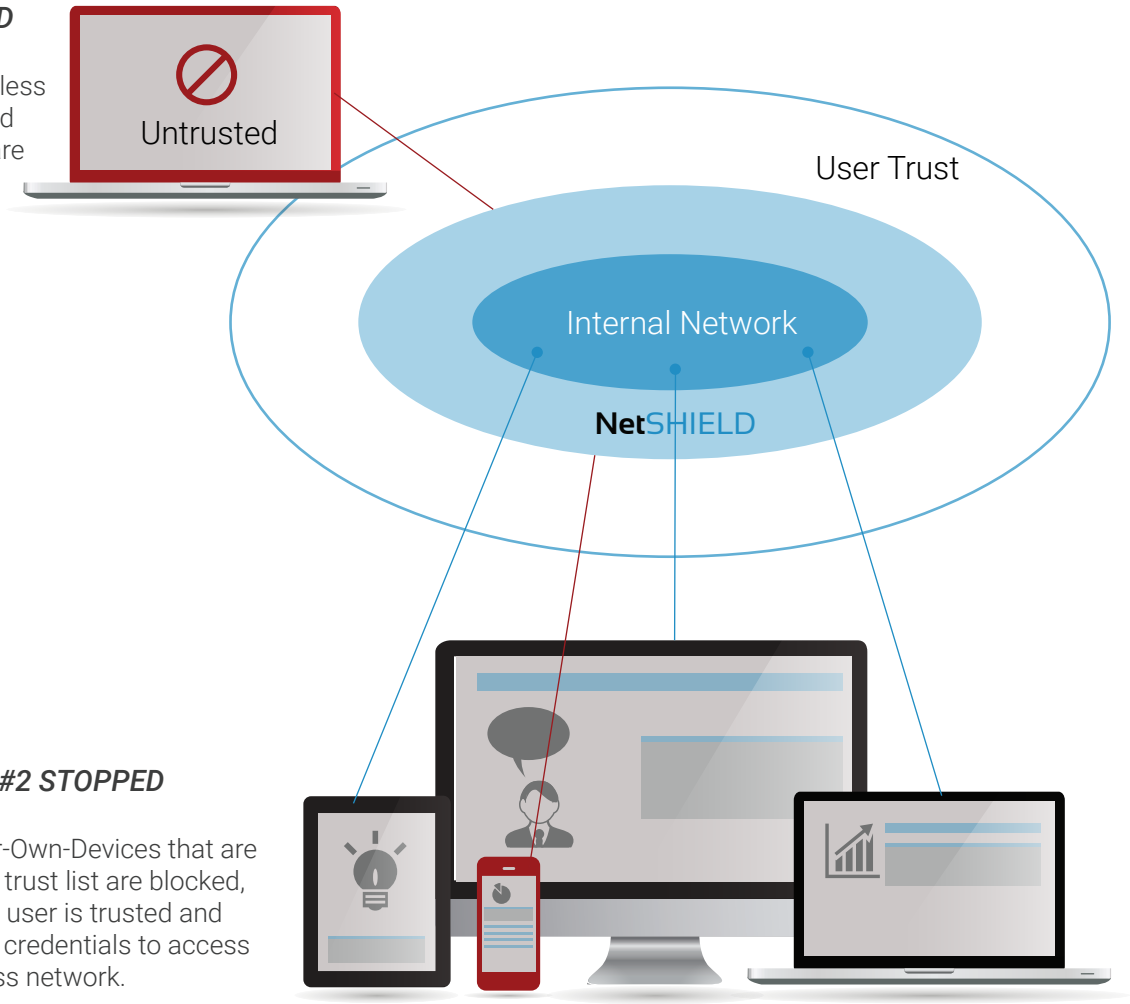
NetSHIELD

Significantly Reduce Wireless Risks

Deploying a wireless network (like EAP-TLS/WPA2) that is relatively safe from hackers is often not practical, because of the complexities involved in deploying certificates on endpoints. For this reason, a complementary solution to the wireless network such as NetSHIELD can provide an additional and immediate defense layer once the wireless layer is breached. Each of the previous wireless network configuration descriptions outline the methods needed for an attacker to breach the security of the wireless network. NetSHIELD provides visibility to all devices attempting to access trusted networks – including those that have circumvented wireless security. All untrusted devices are blocked within milliseconds of connecting to the network, provided that this is the desired policy.

BREACH #1 STOPPED

Hackers exploiting wireless weaknesses are blocked because their devices are untrusted.



BREACH #2 STOPPED

Bring-Your-Own-Devices that are not on the trust list are blocked, even if the user is trusted and used valid credentials to access the wireless network.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871

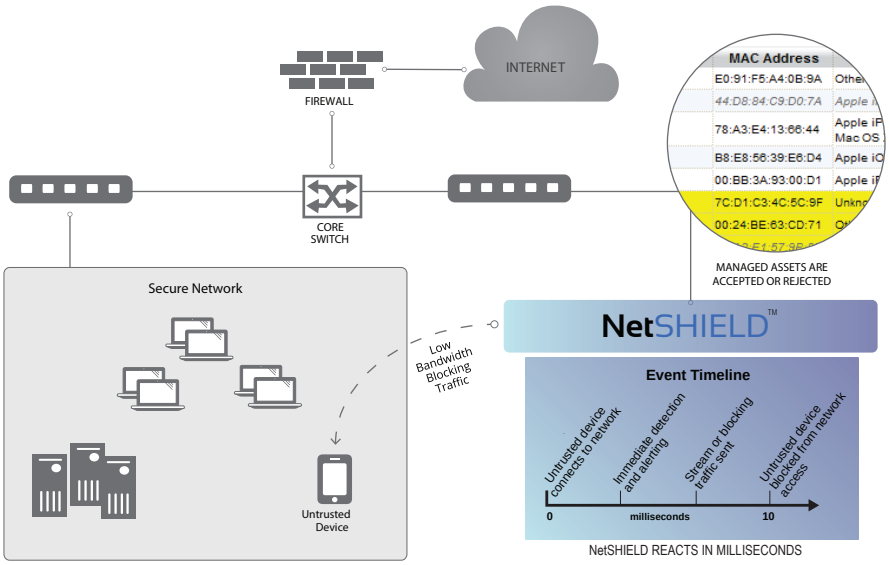
Use Network Access Control to Secure Your Wireless Networks

How NetSHIELD Works

NetSHIELD appliances determine trust based on MAC address, and this is the foundation of the trust list that it maintains and protects. However, unlike the MAC authenticated wireless networks listed above, NetSHIELD is protected against hackers changing their MAC address to match that of an authenticated wireless device (MAC spoofing). While the specifics are proprietary, the NetSHIELD collects more information about a wireless device than just its MAC address. It is able to use this information to detect MAC spoofing events. If policy allows, these events can be defended against using NetSHIELD NAC blocking technology.

Figure 12

NetSHIELD can begin blocking untrusted devices within minutes of being attached to the network. It could literally be plugged in under one's desk and function as a NAC on that network.



NetSHIELD is Practical Security

Many are skeptical of our claims that we are the world's only plug 'n play NAC appliance. The process for setting up an appliance is as follows.

Step 1: Build your trust list. This can be accomplished via automatic discovery or via CSV import.

Step 2: Enable blocking. Our "EasyNAC" blocking technology "snowblinds" any untrusted asset with an IP and MAC address, which means it cannot communicate with other devices on the network. This protects the trusted internal network from interacting with untrusted devices.

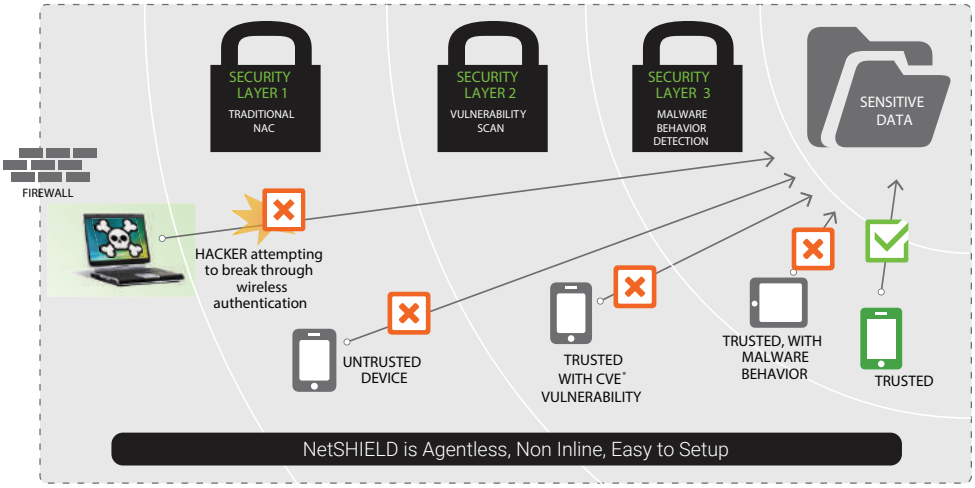
Use Network Access Control to Secure Your Wireless Networks

We also include an optional “SmartSwitch” integration feature, similar to the core functionality offered by other NAC vendors, enabling you to reassign physical ports to quarantine VLANs, but this has the drawback of shutting down all devices that are attached to a given port. Because this is an undesired consequence in many instances, EasyNAC blocking provides an immediate, sniper-rifle block to the untrusted devices only, and is unique to NetSHIELD

Beyond this core NAC functionality, NetSHIELD appliances can enumerate vulnerabilities present on the devices accessing your network in a non-intrusive way similar to how hackerswould, so that you can be proactive about remediating vulnerabilities. Appliances are also equipped with a malware detection feature designed to identify outbound “command and control” traffic destined toward known malware sites, and this is integrated with the blocking engine to provide millisecond response time to contain this type of malware threats.

Figure 13

NetSHIELD provides defense-in-depth through multiple security layers.



About SnoopWall

SnoopWall is the world's first Counterveillance security company delivering a suite of products from the enterprise to the endpoint, protecting all computing devices from prying eyes and new threats through patented cloaking technology. SnoopWall secures mission critical and highly valuable confidential information behind and beyond firewalls and on mobile devices with next generation technology that detects and blocks all rogue network access, remote control, eavesdropping and spying. SnoopWall was recognized by CIO magazine as one of 10 Cloud Security Startups to Watch as well as being ranked 1st among mobile device security companies by Cybersecurity 500. SnoopWall’s software products and hardware appliances are all proudly made in the U.S.A and sold through channel partners throughout the globe. Learn more at http://www.snoopwall.com.

SnoopWall, Inc. | Ten Tara Boulevard, Suite 140, Nashua NH - 03062 | support@snoopwall.com | 1-800-991-3871