

## **WEP Cloaking<sup>™</sup> – Maximizing ROI from Legacy Wireless LAN**

## WEP Cloaking™ – Maximizing ROI from Legacy Wireless LAN

Wired Equivalent Privacy (WEP) is the encryption protocol defined in the original IEEE 802.11 standard for Wireless Local Area Networks (WLANs). Several known vulnerabilities and attack tools have compromised WEP making it unsuitable for secure WLAN implementations, without additional layers of security. AirDefense’s patented WEP Cloaking™ solution is designed to make WEP virtually invulnerable to known attacks and tools, providing a robust layer of protection for legacy WLANs. The solution does not require any hardware or software modifications to the legacy WLAN infrastructure and is designed to work seamlessly through the AirDefense Enterprise Wireless Intrusion Prevention System (WIPS). WEP Cloaking™ can save large enterprises substantial capital costs by avoiding costly upgrades to their WLAN infrastructure while ensuring peace of mind from security and compliance issues.

### Wired Equivalent Privacy

The design objective of WEP, as outlined by the IEEE 802.11 standard, was to protect authorized users of a WLAN from “casual eavesdropping.” WEP was intended to provide confidentiality for the WLAN equivalent to that provided by the physical security attributes inherent to a wired medium.

Security afforded by the WEP algorithm relies on the difficulty of discovering the secret key through a brute-force attack. Figure 1 illustrates the WEP encryption process. The Secret Key (K) is a

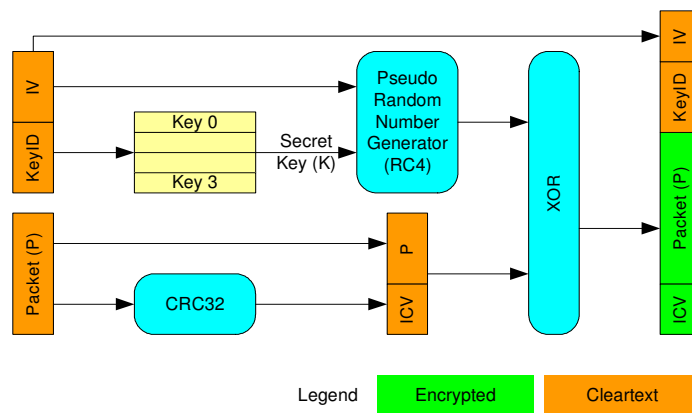


Figure 1: WEP encryption

The Secret Key (K) is a 40-bit or a 104-bit shared secret amongst all the authorized users of a given WLAN. Up to 4 keys can be specified and a 2-bit KeyID selector determines the current key. The Initialization Vector (IV) is a 24-bit random number that is “frequently changed”. The Secret Key (K) is concatenated with the IV, resulting in a 64-bit or 128-bit seed that is input to a Pseudo Random Number Generator (PRNG) based on the RC4 algorithm from RSA<sup>1</sup>. The PRNG produces random bytes, equal in length to the message to be encrypted.

<sup>1</sup> <http://www.rsa.com/rsalabs/node.asp?id=2250>

The WEP PRNG is the critical component of this process, since it transforms a relatively short secret key into an arbitrarily long key sequence. This greatly simplifies the task of key distribution, as only the Secret Key needs to be communicated between Access Points (AP) and stations. The IV extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. Each new IV results in a new seed and key sequence, thus there is a one-to-one correspondence between the pseudo random stream generated by RC4 and the (IV, K) pair. The IV may be changed as frequently as every Packet (M) and, since it travels with the message, the receiver will always be able to decipher any message. The IV is transmitted unencrypted since its value must be known by the recipient in order to perform the decryption.

To protect against unauthorized data modification, an integrity algorithm based on a Cyclic Redundancy Check (CRC32) operates on Packet (P) to produce an Integrity Check Value (ICV). Encryption is accomplished by using a bitwise XOR operation between the random PRNG sequence generated by RC4 with the cleartext Packet (P) concatenated with the ICV. The WEP frame that is finally transmitted contains [(IV, KeyID), Encrypted(P, ICV)] fields where Encrypted(P, ICV) are encrypted and (IV, KeyID) are sent as cleartext.

The receiver essentially reverses the sequence of operations done at the transmitter. It uses the IV from the received frame along with the Secret Key (K) that it shares with the transmitter to re-create the pseudo random stream generated by RC4. The key stream is XORed with the encrypted payload Encrypted(P, ICV) to obtain the cleartext (P, ICV) message. The receiver then calculates the ICV based on P and verifies that it matches the ICV it received to establish data integrity.

## WEP Vulnerabilities

In 2001, Fluhrer, Mantin, and Shamir<sup>2</sup> published their famous “FMS” paper that highlighted several vulnerabilities in WEP. They were able to crack the Secret Key by exploiting weaknesses in the key scheduling algorithm used in WEP. FMS attacks rely on the fact that for certain key values it is possible for bits in the initial bytes of the random key sequence to depend on just a few bits of the encryption key (in an ideal random key sequence each bit has a 50% chance of being different from the previous one). Further, since the encryption key is composed by concatenating the Secret Key (K) with the IV, certain IV values yield weak key sequences.

These vulnerabilities were exploited by early WEP key cracking tools as AirSnort<sup>3</sup>, that sniffed encrypted frames and were able to guess the Secret Key with a large number of frames. The problem with the first generation of WEP cracking tools was the amount of time required to gather

---

<sup>2</sup> Fluhrer, S., Mantin, I., and Shamir, A., “Weaknesses in the key scheduling algorithm of RC4”, Eighth Annual Workshop on Selected Areas in Cryptography (August 2001).

<sup>3</sup> <http://airsnort.shmoo.com/>

enough frames to crack the key. While these attacks were feasible on busy networks with lots of WEP traffic, the amount of time required on intermittent networks was very long.

In August 2004, a new statistical attack called KoreK was created to crack WEP keys. The KoreK attacks do not require millions of packets or rely on certain weak IVs. They only rely on unique IVs that have been captured and can typically crack the key with a few hundred thousand packets.

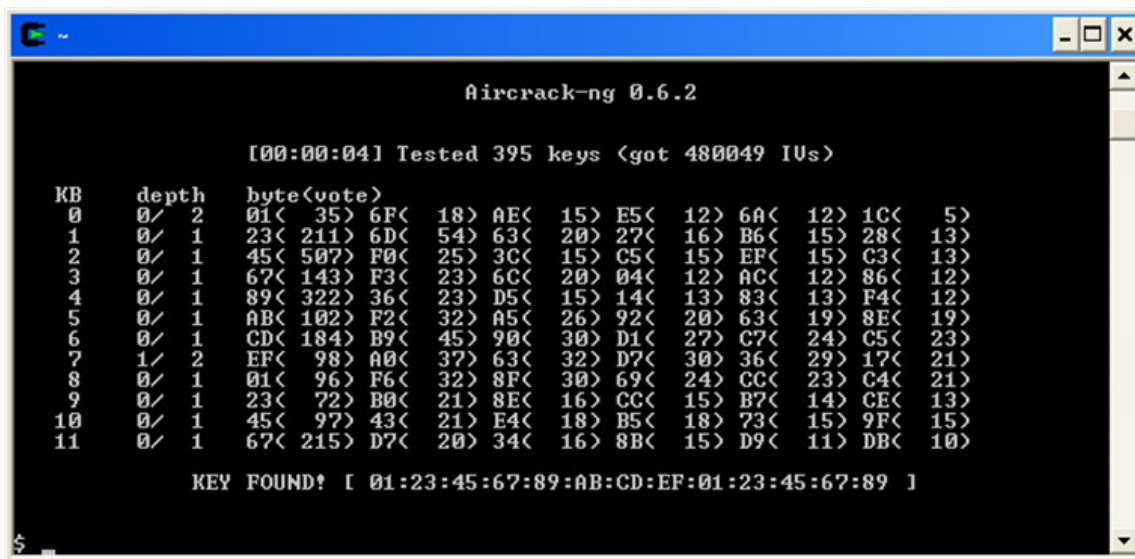


Figure 2: Screen capture of aircrack-ng breaking a 104-bit WEP key with less than 500K captured IVs

Aircrack<sup>4</sup>, first published by Christopher Devin, was one of the most popular WEP cracking tools that was openly released. Aircrack implemented KoreK algorithms as well as an improved version of FMS. Given the statistical nature of the attack, the number of packets required to crack the WEP key varies. However, most 40-bit keys can be cracked with 250K unique IVs and 104-bit keys can be cracked with 1M unique IVs. The aircrack-ng<sup>5</sup> suite is the premier tool of choice for WEP cracking today. It is based on the original aircrack tool, enhanced with better documentation, support for several platforms and wireless cards, and comprises of three main programs:

- airodump-ng: This is a promiscuous mode packet capture utility that enables the capturing of all wireless frames being transmitted on a given channel and writing the contents to a capture file.
- aireplay-ng: This utility is used to inject frames. The primary function is to generate traffic for cracking the WEP key. There are different attacks which can cause deauthentications,

<sup>4</sup> <http://freshmeat.net/projects/aircrack/>

<sup>5</sup> <http://www.aircrack-ng.org/>

interactive packet replay, hand-crafted Address Resolution Protocol (ARP) request injection, etc. ARP replay is a popular way of generating lots of traffic. Although ARP frames are encrypted, it is easy to recognize them based on their known frame size and the fact that they are sent to a broadcast address. Aireplay-ng can capture an encrypted ARP request and transmit it repeatedly to generate new ARP responses from a legitimate host, resulting in the same wireless messages being encrypted with new IVs. This allows the attacker to generate lots of WEP traffic with unique IVs without relying on the victim network.

- **aircrack-ng:** This is the main key cracking program that can recover the WEP key once enough encrypted packets have been captured with airodump-ng.

Figure 2 shows a screen capture of aircrack-ng running on a Windows machine. The WEP frames were generated using ARP replay injection and with less than 500K frames, the tool was able to find the 104-bit WEP key in a few seconds!

In conclusion, WEP security flaws can be summarized as follows:

- **Short IV space:** Using 24-bits IVs results in frequent IV collisions because of IV reuse. The 802.11 standard does not specify a strong random algorithm for the generation of IVs. Vendor specific implementations are typically weak.
- **RC4 weakness:** There is significant correlation between the first few bits of the key sequence and the Secret Key. Further, using a cleartext IV with the Secret Key, coupled with the existence of known weak IVs and keys, allows an attacker to effectively guess the key.
- **Known cleartext:** Almost every 802.11 data frame has a Logical Link Control (LLC) header where the first few cleartext bytes of the encrypted payload are known. This allows tools to quickly extract the first few bytes of the WEP key sequence.
- **No replay protection:** IVs can be reused allowing the attacker to capture and replay an encrypted frame, e.g. an ARP packet, and get legitimate encrypted responses.
- **Weak integrity check:** WEP does not have a cryptographically secure, key based, message integrity check. Instead it uses a linear CRC32 checksum that is traditionally used for error detection and is cryptographically weak.
- **Key rotation:** WEP does not specify a method for distributing or effectively rotating keys.
- **Shared Keys:** WEP uses one common secret shared by all users. Once a key is compromised, the whole WLAN is as good as open.
- **Optional requirement:** The default mode of operation of 802.11 is open and unencrypted. Even WEP is not mandatory.

## Upgrading from WEP

To fix the security challenges in WEP, the IEEE standards body ratified the 802.11i standard. IEEE 802.11i provides strong authentication of wireless devices and encryption of data traffic. It

uses the IEEE 802.1X Extensible Authentication Protocol (EAP) to guarantee that only authorized devices gain access to the wireless network and uses the Advanced Encryption Standard (AES) to guarantee confidentiality and integrity of the data communications between authenticated devices. IEEE 802.11i is the basis for the WPA2 (Wi-Fi Protected Access 2) industry standard defined by the Wi-Fi Alliance.

While approving WPA2, the standards body realized that many organizations would be forced to upgrade their WLAN hardware to support the new and sophisticated security protocol. As a result, it also defined a standard called WPA that used legacy WEP hardware but addressed some of the known vulnerabilities of WEP. WPA rotated WEP keys on a per packet basis, doubled the IV to 48 bits and introduced a message integrity check. The goal of WPA was to allow legacy WEP devices to be firmware upgradeable to WPA.

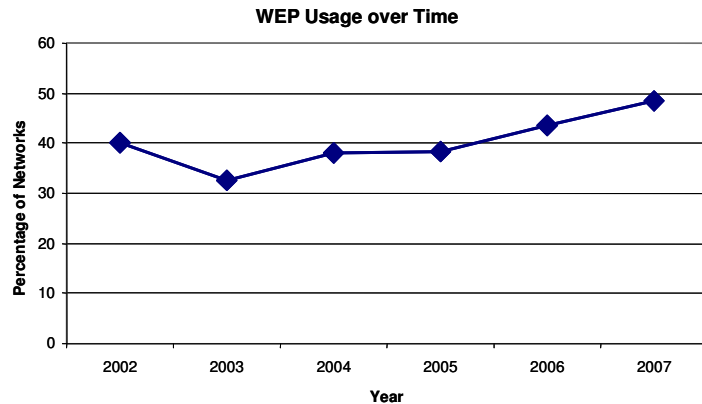


Figure 3: WEP usage over time (source: wigle.net)

While, WPA and WPA2 standards have been around for a while, their adoption has been slow. In fact, based on data from wigle.net, a popular online database of wireless networks profiled by “war drivers”, WEP usage has remained pretty flat over the last several years. Almost half of the nearly 10 million networks listed on the Wigle database continue to be open and unencrypted. This level of user indifference to wireless security has prompted several policy makers and companies to demand stricter wireless security policies, particularly when it comes to confidential information.

*“Although IEEE wireless security standard, 802.11i, was ratified in 2004, migration to 802.11i end to end hasn’t been easy as many legacy devices only support WEP. During the migration, WEP encrypted systems are vulnerable. Using a layered approach to wireless security that incorporates strong authentication and encryption in the infrastructure with wireless intrusion protection to overcome the weaker security of handsets can extend the shelf life of wireless technologies while improving security.”*

**Rachna Ahlawat, Gartner, March 2007**

### **PCI Security Standards**

The Payment Card Industry (PCI) released an updated version (version 1.1) of their Data Security Standard (DSS)<sup>6</sup> that went into effect starting September 2006. The PCI Security Standards Council is an open global forum, founded by American Express, Discover Financial Services,

<sup>6</sup> <https://www.pcisecuritystandards.org/>

JCB, MasterCard Worldwide and Visa International, for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

There has been an alarming increase in credit/debit card and identity theft in retail that has led to the creation and enforcement of stricter information security requirements. Wireless specific attacks have resulted in several known compromises of credit card and personal information in retail.

*“Merchants that have implemented or are considering using wireless technology must develop and deploy a comprehensive strategy to secure their systems from intrusion. ... It has come to Visa’s attention that some entities are not properly securing their wireless networks, which increasingly leads to the compromise of cardholder data, brand damage, and other concerns — both financial and regulatory.”*

**Visa, August 2006**

PCI DSS version 1.1<sup>7</sup> places special emphasis on WLAN security. It requires that card holder environments change wireless defaults (passwords, SSIDs, WEP keys, etc.), analyze and identify all wireless devices, restrict physical access to wireless devices, log wireless activity, define wireless usage policies, etc. The standard also mandates that WEP should not be used. If it must be used, other layers of protection should be added.

*“For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.”*

**PCI DSS 1.1, Section 4.1.1**

Several retailers and other organizations that handle card holder data are struggling with PCI compliance with the new wireless requirements. Many of them have legacy WEP wireless networks in stores and distribution centers with data collection terminals, wireless Point of Sale (POS) terminals, Manager’s workstations, VoIP phones, wireless printers, and other WLAN devices that simply cannot be firmware upgraded to WPA. These devices often do not have sufficient processing capabilities to allow them to implement the enhanced computational requirements of WPA. Some devices such as VoIP phones have a longer battery life with legacy 802.11b WEP radios. In fact, according to the Wi-Fi Alliance<sup>8</sup>, as of March 2007, only 47% of the 3384 Wi-Fi certified devices are capable of WPA and only 22% are capable of WPA2 as shown in Figure 4. This implies that over half of all Wi-Fi devices are only capable of WEP. A lot of these legacy WEP devices are present in retail environments and will fail PCI compliance.

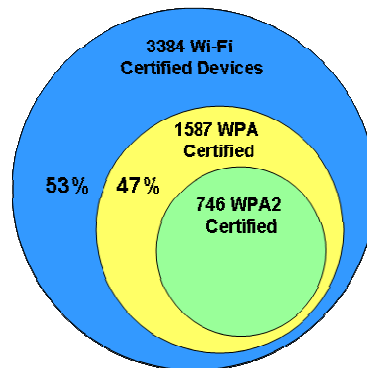


Figure 4: Wi-Fi certified devices that support WPA or WPA2 (source: Wi-Fi Alliance)

<sup>7</sup> [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

<sup>8</sup> [http://certifications.wi-fi.org/wbcs\\_certified\\_products.php](http://certifications.wi-fi.org/wbcs_certified_products.php)

## AirDefense WEP Cloaking™

AirDefense Enterprise is the industry's most comprehensive and widely deployed WLAN protection platform used to enforce policy and verify compliance, log forensic records of wireless activity, and provide real-time notification/mitigation of wireless intrusions. The addition of WEP Cloaking™ provides an entirely new dimension of protection that can act as the security supplement for WEP encryption.

AirDefense Enterprise uses a dedicated network of WLAN sensors that continuously monitor the RF environment 24/7 over a given spatial location for threats, attacks and performance issues. Sensors use AP hardware with special firmware that allows them to listen to and analyze all packets picked up by the antenna. In addition, the sensors use an intelligent channel scanning algorithm to detect traffic

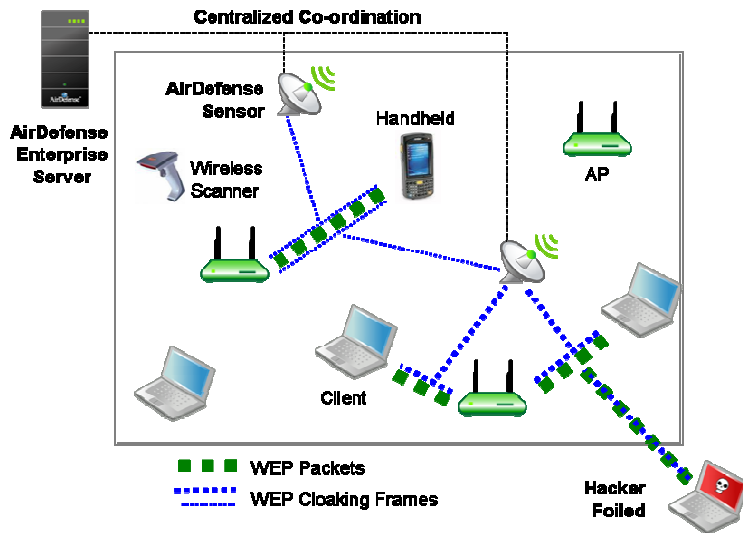


Figure 5: AirDefense Enterprise's WEP Cloaking™ operation

across the RF spectrum. The sensors locally analyze all the received packets, collect several statistics and events of interest and use a bandwidth efficient secure TCP/IP communication link to aggregate information in a centralized server. The AirDefense Enterprise server provides a centralized repository of all current and historical information, management and troubleshooting dashboards, policy definition wizards as well as reporting and compliance modules.

AirDefense's WEP Cloaking™ is the first and only patented<sup>9</sup> technology to protect enterprises using WEP from common attempts used to crack the WEP key. Leveraging the AirDefense Enterprise platform, the WEP Cloaking™ module uses the same AirDefense Enterprise sensors to constantly protect APs, laptops and handheld devices, by intelligently injecting chaff WEP frames designed to confuse WEP attack tools.

AirDefense sensors communicate with the Enterprise server to co-ordinate cloaking operation. The server can be configured to instruct a group of sensors to cloak authorized devices in a given location. Sensors are designed to intelligently adjust their frequency scanning patterns to maximize cloaking effectiveness while performing regular wireless IPS scanning on other

<sup>9</sup> US Patent No. 7,058,796, "Method and system for actively defending a wireless LAN against attacks"

channels. More than one sensor can cloak a single device depending on spatial coverage. In the event of a wired network outage, if sensors lose connection with the centralized server, they will continue to cloak once enabled. The sensors use several countermeasures, correlation through the server and mutual co-ordination over the air to maximize the effectiveness of cloaking with nominal wired and wireless bandwidth consumption.

Once configured for cloaking, sensors intelligently analyze local traffic and insert carefully timed cloaking frames as shown in Figure 5. These cloaking frames appear as legitimate WEP traffic between authorized devices to someone who does not have the Secret Key. Authorized users with access to the Secret Key automatically ignore the cloaking frames as their ICV integrity test fails. An attacker sniffing traffic will not be able to distinguish cloaking frames from the legitimate frames. When statistical WEP cracking tools are run on the captured data, key cracking will fail. Figure 6 depicts a screenshot of aircrack-ng where the same scenario from Figure 2 was repeated, except in this instance WEP Cloaking™ was enabled. WEP cracking tools simply fail to decode the key when cloaking is enabled.

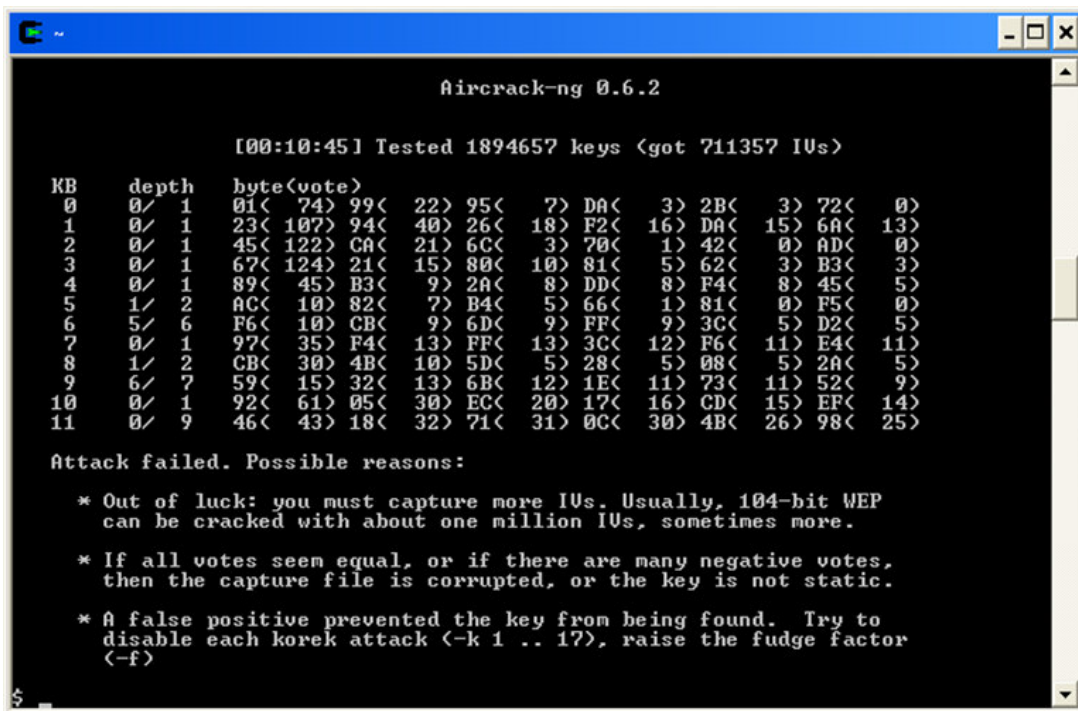


Figure 6: Screen capture of aircrack-ng failing with WEP Cloaking™

## Expert Opinion—Trustwave

*“The Payment Card Industry Data Security Standard requires that WEP-encrypted networks either be upgraded or supplemented with additional security. AirDefense’s WEP Cloaking solution offers a new, cost-effective avenue for compliance.”*

**Robert McCullen, CEO of Trustwave**

Trustwave provides data security and compliance management solutions—including Secure Sockets Layer (SSL) certificates—to organizations throughout the world. Trustwave assists thousands of organizations—financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies—secure their critical data and manage industry and regulatory compliance initiatives.

In addition, Trustwave is trusted by all the payment card brands to investigate security incidents involving payment card data and as a result has performed over 300 forensic investigations of payment card breaches.

### ***Wireless Devices and the Payment Card Industry Data Security Standard (PCI DSS)***

As wireless technology continues to evolve and implementation costs continue to decrease, many organizations leverage wireless LANs to increase efficiency in their operations. However, along with wireless technology’s usability and cost-effectiveness comes responsibility to perform due diligence and secure wireless systems including the detection, identification and neutralization of rogue wireless devices. A number of payment card compromises investigated by Trustwave arose from the exploitation of an insecure wireless infrastructure.

Trustwave defines a payment card compromise (or breach) as an unauthorized individual taking advantage of a flaw in a system that processes, transmits or stores cardholder data to steal payment card numbers, expiration dates validation codes and other information. Thieves then sell the stolen information on the black market or use it themselves to make fraudulent purchases. The payment card brands developed the Payment Card Industry Data Security Standard (PCI DSS) specifically to combat these occurrences.

All of the payment card brands require any entity that processes, transmits, or stores cardholder data to comply with all 12 requirements of the PCI DSS.

Of the payment card breaches that resulted from the penetration of a wireless network, Trustwave found that in the majority of the cases, the compromised organization relied solely upon WEP encryption. As previously discussed, an organization cannot depend upon WEP encryption alone to secure their wireless network. In fact, using only WEP encryption without additional security measures violates the PCI DSS.

As stated in the Payment Card Industry Data Security Standard (PCI DSS):

***4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC***

*VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:*

- *Use with a minimum 104-bit encryption key and 24 bit-initialization value*
- *Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS*
- *Rotate shared WEP keys quarterly (or automatically if the technology permits)*
- *Rotate shared WEP keys whenever there are changes in personnel with access to keys*
- *Restrict access based on media access code (MAC) address.*

WEP began its life as part of the IEEE 802.11 standard that was ratified in 1999. The many inherent and fundamental shortcomings that abounded have, for the past 8 years, been leveraged by attackers and researchers alike to continually find newer, better, and faster ways of breaking it.

In testing WEP Cloaking™, Trustwave has found that AirDefense has not made an attempt to perpetuate an inherently flawed protocol. They have added an additional layer of security that can be used for legacy WEP networks to mitigate statistical analysis attacks to recover WEP keys.

AirDefense's WEP Cloaking™ seems to provide a significant impediment to attacks that rely on statistical analysis to decode the WEP key such as FMS and the KoreK attacks.

WEP Cloaking™ is not a substitute for more robust security protocols such as WPA, VPN, or SSL, and WEP Cloaking™ itself does not address all of the flaws inherent in WEP. Therefore WEP Cloaking™ alone will not address all of the PCI DSS requirements for wireless but a properly configured implementation of WEP Cloaking™ may serve as a component of a compensating control strategy for a portion of the PCI DSS Section 4.1.1 requirements.

When WEP Cloaking™ is used in conjunction with AirDefense Enterprise, and careful attention to wireless best practices for security, it can provide fairly robust security for legacy networks.

### ***Common Wireless Security Gaps***

Trustwave's numerous forensic investigations and experience helping over 30,000 businesses manage their PCI DSS compliance provides insight into what areas of the PCI DSS organizations find particularly challenging. One of those areas specifically is the proper configuration of wireless technologies. In many instances, a merchant fails to change the default settings on their device (e.g., log-in credentials, WEP keys, SSID, and SNMP community strings on access points). Another challenge is the cost of upgrading a large wireless infrastructure as discussed in the section above titled "Upgrading from WEP". The failure to change default settings or implement additional security measures if only WEP is used can leave a wireless network vulnerable to attack techniques such as replay based attacks, CRC based attacks, IV collisions, eavesdropping, statistical analysis, and inverse induction decryption, and these are just some of the published attack vectors against WEP. Many of these have been employed in many of the recent, high profile payment card breaches.

## ***Using WEP Cloaking to Secure Legacy Wireless Technology***

Trustwave's tests of the AirDefense product finds that the technology provides an effective layer of security to WEP that can be used with legacy WLAN to mitigate some WEP attacks, such as FMS and KoreK, used to recover WEP keys and decrypt WEP encrypted wireless communications.

AirDefense's WEP Cloaking™ is not a substitute for more robust wireless security protocols such as WPA or WPA2. However, when upgrading to these newer security protocols is not immediately feasible, a properly configured AirDefense WEP Cloaking™ system could be used as an effective component of an entity's compensating control strategy. . Under the compensating control provision defined by PCI, <sup>10</sup> compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must

1. Meet the intent and rigor of the original stated PCI DSS requirement
2. Repel a compromise attempt with similar force
3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements)
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

---

<sup>10</sup> <https://www.pcisecuritystandards.org/tech/glossary.htm#c>

## Conclusions

The AirDefense WEP Cloaking™ solution extends the shelf-life of existing and future WLAN infrastructure deployments. There are millions of legacy WEP devices already deployed, such as wireless scanners, barcode readers, Wi-Fi phones, and embedded Wi-Fi clients and many may not be firmware upgradeable to stronger encryption protocols. Although wireless security professionals have long known of the need to use technologies stronger than WEP, organizations may require months or years before such a change can be fully implemented. The cost of such upgrades can be substantial. AirDefense's WEP Cloaking™ technology enables companies to preserve their existing and often considerable investment in legacy WEP wireless devices even after their security life-span has seemingly expired and provides a cost-effective option for PCI compliance.

## ***About AirDefense***

**AirDefense**, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among Red Herring's Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

**AirDefense Enterprise**, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

**AirDefense Personal**, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

**The AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: AirDefense Mobile, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. AirDefense Architect provides complete design and 3D RF simulation of WLANs based on building-specific environments. AirDefense Survey provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact [info@airdefense.net](mailto:info@airdefense.net) or call us at 770.663.8115. All trademarks are the property of their respective owners.