

# Breaching Wireless POS Networks

By Ryan Sherstobitoff

This article describes the vulnerabilities and strategies for mitigation as it pertains to protecting wireless point-of-sale systems.

Wireless networks and endpoints offer convenience and connectivity. Unless properly secured, they also offer a means of ingress into the network. This article will describe the vulnerabilities and strategies for mitigation as it pertains to protecting wireless point-of-sale systems.

In the wake of undiscovered data breaches and subsequent public exposure, hackers have begun to turn their eyes towards breaching wireless networks and taking advantage of their many weaknesses. Furthermore, we are seeing a trend towards stealing cardholder information from retailers through much publicized breaches such as TJ Maxx and Hannaford Brothers. According to the *2008 Data Breach Investigations Report* by the Verizon Business Risk Team,<sup>1</sup> 84% of the data compromised in documented breaches pertained to card holder information.

The use of wireless networks is not an uncommon way of providing access for employees anywhere, anytime throughout the corporate campus. However, wireless networks come with often ignored dangers:

- Exploitation of WEP encryption: exploiting WEP can allow an intruder to gain connectivity to a network, thus, giving the hacker the means of exploiting a specific system (e.g., the point-of-sale terminals)
- Access points being deployed with little or no security enabled

These vulnerabilities can eventually lead to the exposure of private information if not properly secured and accounted

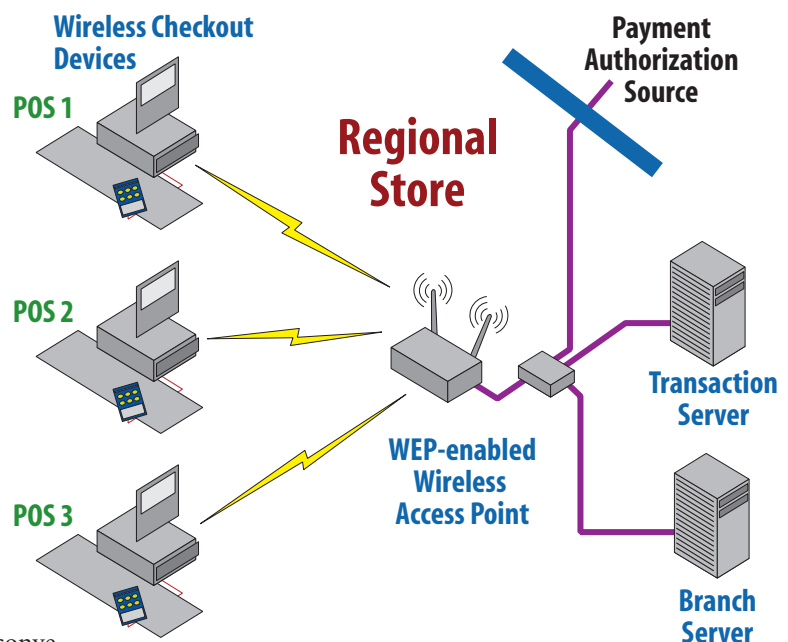


Figure 1 – Retail Point-of-Sale System

for when implementing a data security policy. The weaknesses of a wireless environment can often lead to violations of PCI-DSS, HIPAA and SOX if an exposure were to occur through one of those vulnerabilities. For example, the protection of cardholder information as covered under PCI-DSS includes a number of guidelines to aide in the development of policy that (a) protects cardholder information stored on servers, and (b) protects cardholder information that may be in transit via transactions that occur between front-end wireless point-of-sale terminals and the external authorization source.<sup>2</sup>

## The wireless point-of-sale (POS)

The wireless POS system consists of one or more networked wireless POS end-points located at check-out stands and the internal on-site transaction server which connects the system to the payment authorization source (Figure 1). The transaction server also interfaces with the branch server for transaction storage and inventory control system. The basic steps are as follows:

- Transaction initiated at wireless POS checkout stand
- Transaction information sent to wireless access point, to transaction server, to authorization source
- Transaction authorization returns to POS checkout terminal to complete transaction

1 <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>.

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

From an architectural perspective a POS end-point runs an operating system, either a version of Windows or Linux designed to limit functionality with not all OS functions being available to the logged-in user. These devices are physically divided into two different components:

- **Card Reader** – system that reads the card as it is swiped
- **Transaction Unit** – system that sends the card information to an authorization source

The information read at the POS is sent to the authorization source (e.g., Amex) through the transaction unit. In addition the purchase information (payment, item, quantity, etc.) is sent over the network to a branch server for inventory control and auditing purposes.

Normally the information sent between the retailer and the authorization source will use strong encryption to protect the information; however, network security between the POS and the internal branch/transaction servers may or may not be encrypted and really depends on the configuration at each location.

Assuming that the retailer does encrypt the information sent between the POS device and the branch/transaction server, the real vulnerabilities then exist at the POS end-point, the wireless access point, and the server itself.

Because a POS terminal reads the card information, performs the transactions, and receives the authorization code, information may be stored for short periods either in flash memory, static RAM or the hard drive (e.g., a few hours until close of register, etc). Malware could be installed directly on the POS to intercept the transaction data as it is being sent to the authorization source or the internal branch server for storage.

Branch servers are normally used to collect information from multiple POS terminals, thus, they often will be running a database of some form or another. A hacker wishing to obtain access to this information would have to compromise the server first, and would then likely exploit database encryption vulnerabilities.

Because the target is often cardholder information, hackers are developing strategies that involve breaching wireless networks – wireless POS systems in particular – because they are easier to penetrate than cracking the corporate firewall and obtaining access via the external gateway.

## Cracking the wireless POS

Wireless hacks attributed to around 9% of the security incidents documented in the Verizon Business Risk Team investigation. This is likely due to the following:

- Incorrect access point configuration
- WEP encryption
- No security enabled

## Incorrect access point configuration

A wireless access point is vulnerable to attack if the device is not configured correctly from a security perspective:

- Using default administrative passwords
- Broadcasting the SSID (service set identifier)
- Not using encryption
- Using weak authentication such as WEP to validate users

Networks that are openly broadcasting their SSID can be discovered quite easily by placing a laptop with a wireless card in the vicinity. Furthermore, the only security that some of these networks are using is WEP to prevent unauthorized connections unless a valid key is provided.

## WEP encryption

WEP (wired equivalent privacy) can be a stumbling block in terms of preventing intruders from connecting to wireless networks located throughout regional locations. WEP has a number of vulnerabilities<sup>3</sup> that should not be ignored.

The number one vulnerability with WEP is that the encryption algorithm can easily be cracked in a matter of minutes using commercially available tools, thereby, providing the hacker with the WEP validation key. The sad truth is that recent surveys show that there are many retailers still using WEP to encrypt their traffic, exposing them nonetheless.<sup>4</sup>

For the networks that do have WEP enabled and have been configured not to broadcast their SSID, they can still be discovered and compromised quite easily. Using tools such as Netstumbler provides the hacker invaluable information concerning what networks exist despite whether the SSID is visible or not. Once the network has been discovered through listening for RF signals, the hacker can employ a number of methods in attempt to penetrate and gain access.

The first step in breaching any wireless network will require the hacker to gain basic connectivity. Gaining illicit access can be accomplished through two different approaches depending on how complex the attack is – the later is obviously much easier to conduct than crafting specific exploits (though many exploits can be found in the underground hacker marketplace):

1. Exploiting specific encryption vulnerabilities, including offline dictionary attacks, using brute force, and cracking the encryption algorithm or the supporting protocols.
2. Using tools such as AirSnort and AirCrack to aide in discovery of the WEP key from packets obtained through passive monitoring.<sup>5</sup> The idea is to reassemble packets and compute the encryption key by capturing the RF traffic for an extended period of time.

3 <http://www.xlogs.net/?p=211>, <http://www.securityfocus.com/infocus/1824>.

4 [http://findarticles.com/p/articles/mi\\_m0EIN/is\\_2008\\_Jan\\_14/ai\\_n24229173](http://findarticles.com/p/articles/mi_m0EIN/is_2008_Jan_14/ai_n24229173).

5 <http://airsnort.shmoo.com>.

## Targeted malware extracts credit card information and other sensitive data directly from the wireless POS.

### Exploiting the breach

Penetrating a wireless network and planting targeted malware only recently emerged on the scene and is expected to increase. Once the intruder has accessed the wireless network, the next challenge would be to compromise the POS or the branch server. There are a number of ways and vectors in which this can be accomplished in a relatively short period of time:

- **Privilege escalation:** Elevating user privileges is a method that hackers use to gain access to other parts of the system that may require a higher level of validation. Vulnerabilities that allow this condition to occur are often the culprit behind most escalation attacks.
- **Hacking specific Windows services (IIS, SQL, Apache, etc):** Gaining access via Windows services by exploiting specific vulnerabilities that allow remote arbitrary code execution.
- **Buffer overflow attacks:** Overflowing the buffer of an application will cause a condition to occur that in some cases will allow for arbitrary code to execute with remote shell-binding capabilities.

One popular method currently being exploited is the development of targeted malware to extract credit card information and other sensitive data directly from the wireless POS, AP, or branch server.<sup>6</sup> Some recent breaches have led to malware being physically installed on key servers and the avenue for attack was through a wireless network at a field office.

Malware could capture the sensitive information in real time by installing Trojans that directly interact with the application on the POS terminal, thus, capturing the customer's information as it is sent to the authorization source or the branch server (Figure 2).

Once the malware has captured the necessary data, it can open a channel with a command and control server and upload the stolen information. It is often found that the C&C server will also be connected to thousands of compromised PCs, subsequently distributing the stolen data to be

stored on a consumer's PC. The chilling part is anyone's PC can instantly become a drop-box for stolen corporate information once it has been compromised by hackers.

### Hiding the evidence

A next step for the attacker after compromising the POS would be to hide the obvious signs that the system had been tampered with by installing a root-kit. Full kernel mode persistent root-kits are the hardest form to detect. Now the hacker has completely eliminated the possibility of detection by the means of security scanners, antivirus applications or any other security tool focused on finding vulnerabilities. This way the breach can remain hidden for as long as possible before anyone considers the possibility a POS is breached.

### Discovery and prevention

Determining if a wireless POS and network has been breached is somewhat difficult as the intruders have likely covered their initial entry by hiding any physical traces (deleting or hiding audit logs, installing root-kits, etc.). Therefore, the best approach is to adopt a strategy for detecting and mitigating the effects of a breach with the following steps:

- **Database monitoring:** Technologies exist to monitor SQL and Oracle databases for suspicious activity (access from unauthorized users, insertion of scripts, execution of SQL statements, etc.). Monitoring is only part of the equation to detecting an actual breach in

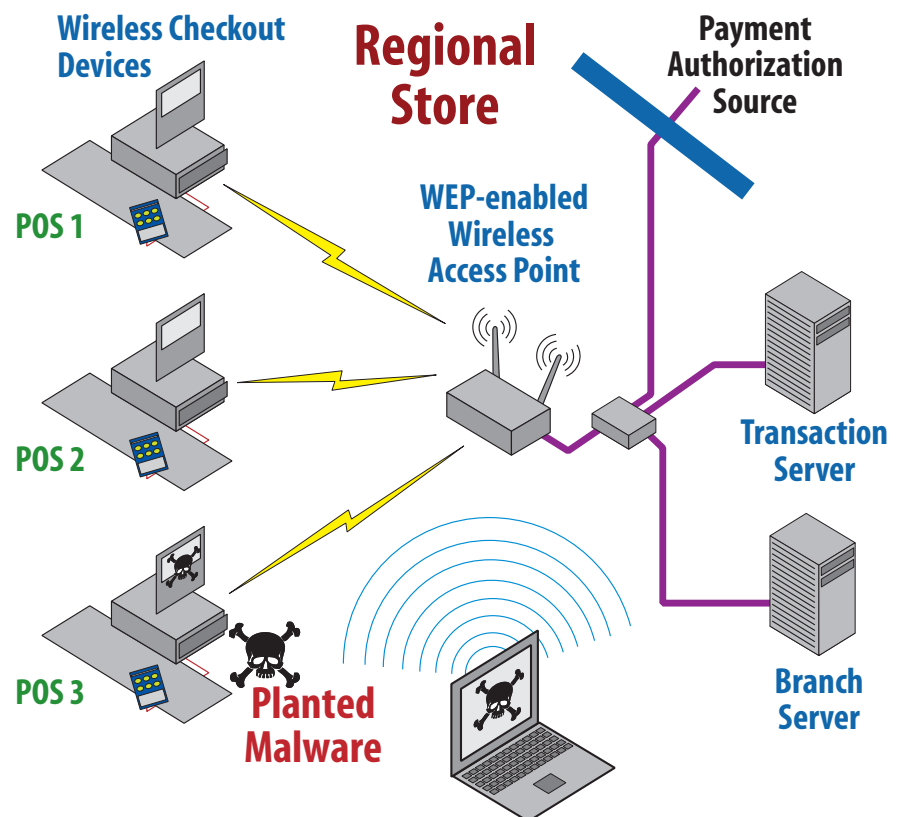


Figure 2 – Malware placed on wireless POS to steal cardholder information from a live transaction

<sup>6</sup> [http://www.infoworld.com/article/08/03/28/Hannaford-Malware-planted-on-store-servers-stole-card-data\\_1.html](http://www.infoworld.com/article/08/03/28/Hannaford-Malware-planted-on-store-servers-stole-card-data_1.html).

progress. If hackers subsequently decide to access cardholder information stored in your databases in addition to extracting the data in real time, database monitoring will increase the odds of discovering unauthorized access.

- **Network intrusion detection:** Intrusion detection technologies in addition to other methods can be used to detect anomalous traffic and behavior that might be associated with an attack.
- **Hardening critical assets:** You can minimize your exposure and risk by hardening critical assets (in this case the wireless POS terminal) by removing and disabling non-essential functionality such as services, applications, and ports that not only add to the complexity but introduce additional risks.
- **Integrity checking:** Integrity checking can be used to recognize unauthorized modification of sensitive information.

Organizations mandated to protect cardholder information must ensure that proper measures are implemented to avoid becoming the next victim of a data breach. Part of this on-going process is adopting a security policy framework designed to not only avoid common threats but also unseen deficiencies that wireless networks may have:

- Knowing where the wireless networks are and what they are connected to. In an ad hoc, de-centralized environment (i.e., regional offices, stores, etc.), understanding all wireless networks and access points, what encryption methods are being implemented, and what they are connected to is crucial, especially when containing sensitive information.
- Adopting stronger wireless encryption by using WPA2-EAP or WPA2-AES-128 instead of WEP. It is often found that WEP is still used despite the well-known deficiencies within its encryption algorithm. According to a 2007 survey conducted in London England, 30% of the wireless networks discovered were still using default settings inherent to the wire-

less access point.<sup>7</sup> Furthermore a study conducted in November 2007 concerning retail wireless networks revealed that 25% were using WEP for encryption.<sup>8</sup>

## Mitigation and understanding your risk

Having a good understanding of what and where your risks are is important to on-going strategy to ensuring successful mitigation.

- Understand where your data is flowing to and from
- Incorporate stronger authentication for wireless networks
- If you are in the retail business, encrypt payment information between POS terminals and branch servers
- Regularly assess critical assets with a multitude of technologies – anti-root-kit, anti-virus and vulnerability assessment tools

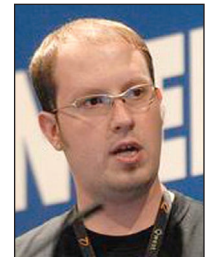
## Conclusion

Like any other device on the network the wireless POS has a number of vulnerabilities that should not be ignored; thus, administrators should adopt strong policies in an effort to minimize these risks by protecting the end-points and all components involved in the system.

It's also important that administrators be aware of the dangers that are inherent to a wireless environment and the strategies used by hackers to get access. Therefore, it is important to understand what the implications are when deploying various technologies and what their associated risks are.

## About the author

Ryan Sherstobitoff, Chief Corporate Evangelist at Panda Security USA ([www.pandasecurity.com](http://www.pandasecurity.com)), is a widely recognized security expert and lectures audiences across the U.S. on cybercrime trends. He can be reached at [ryans@us.pandasecurity.com](mailto:ryans@us.pandasecurity.com) or through his blog at <http://pandasecurity.us.wordpress.com>.



<sup>7</sup> [http://www.rsa.com/solutions/wireless/survey/wireless\\_security\\_survey\\_london\\_2007.pdf](http://www.rsa.com/solutions/wireless/survey/wireless_security_survey_london_2007.pdf).

<sup>8</sup> <http://www.net-security.org/secworld.php?id=5618>.