Point-of-Sale Vulnerabilities

Dr. Neal Krawetz
Hacker Factor Solutions
White Paper

Copyright 2006-2007 Hacker Factor
All rights reserved
FOIA Exempt

Document history:
Version 1.0: Initial draft.
Version 1.1: Incorporated feedback from reviewers.
Version 1.2: Incorporated additional feedback.
Version 1.3: Limited release.
Version 2.0: Public release.

Hacker Factor
P.O. Box 270033
Fort Collins, CO
80527-0033
http://www.hackerfactor.com/

Public Release

There are many issues related to the disclosure of the vulnerabilities described in this document. Ideally this document should be quietly distributed to the impacted companies. Unfortunately, there are too many vendors and retailers impacted by these risks; a small company such as Hacker Factor Solutions does not have the resources necessary to contact each of these companies. Instead, reporting attempts were limited to a small sample of representative companies, of which, few responded.

The standard practice in the security community is to publicly release information when the vendor(s) is non-responsive. However, the vulnerabilities disclosed in this document denote a set of fundamental flaws in the point-of-sale process. Even if a solution were available today, it would take years to be fully deployed. Given that a full disclosure of these vulnerabilities would unlikely lead to a *rapid* deployment and adoption of more secure systems, this public disclosure was delayed. It was hoped that the credit card industry would respond and address some of the more significant issues. Although a few of the issues appear to have been addressed (see Section 10: Addendum), there has not been any direct response or acknowledgement from the major credit card providers and processors.

It is important to recognize that nothing in this paper is new or novel. In most cases, these risks have been known to the credit card industry for more than a decade, however little has been done to address these risks. In this paper, all exploits are discussed in high-level terms, with only specific examples offering implementation details. Generally speaking, all vendors and providers are equally vulnerable, but specific attack details may vary by vendor.

As a compromise between the need for full disclosure and desire for responsible reporting, this document was initially provided under a limited release. Only entities with a *need to know* were provided copies of this paper. The recipients included law enforcement agencies, financial institutions, card providers, credit card clearinghouses, point-of-sale manufacturers, large retailers, and related businesses. Each of the recipients had the option to discuss these issues and request that this document remain as a limited distribution. However, only one recipient had any comments on this paper (and that feedback was incorporated) and one other recipient requested a delay in the release of this paper. The delay was set for one year. Since there has been no additional discussion and no additional requests for a delay, this paper has now been released publicly.

The differences between this public release and the limited release are as follows:

1. This section, “Public Release”, has been modified. The limited release had distribution restrictions.

2. The Reporting History has been updated to reflect dates after April 2006.

3. An Addendum has been added that lists events that followed the limited release.

Because this paper is over a year old, some of the hyperlinks to references may no longer be available online. However, **no attempt** has been made to update the body of this document; **Sections 1 through 8 have not been modified**. Readers of this public release will see the same text as the limited release recipients.

This document is distributed under the following terms:

1. Only Hacker Factor Solutions may distribute this document. Public redistribution is only allowed with PRIOR WRITTEN PERMISSION from Hacker Factor Solutions.

2. Receiving a copy of this document does NOT constitute a transfer of copyright or ownership. Hacker Factor Solutions retains all rights to this document.

3. Hacker Factor Solutions recommends AGAINST the development and use of exploits described in this paper and takes NO RESPONSIBILITY for actions taken by other people. This paper is distributed under the accepted practice of Full Disclosure, 16 months after attempting to contact vendors.

Thank you for your compliance with the terms of this public distribution.

Table of Contents

1 Abstract

Point-of-Sale (POS) systems provide the initial interface for credit card transactions. While the communications between POS systems have been hardened through the use of cryptography and a variety of authentication techniques, the devices themselves provide virtually no security. Few POS systems implement best practices for handling sensitive information, such as the Visa standards for credit card management. This document describes common risks to credit card users due to POS systems.

2 Background

Between January and March 2006, many people received replacement credit cards. The replacement cards included a letter stating that the card might have been compromised. While there had not been any fraudulent charges, the credit card companies were taking a proactive step to prevent abuse by issuing new cards. One credit card provider discussed the potential compromised in a phone conversation. They could not disclose the retailer, but said that the potentially compromised information was everything on the card: name, card number, expiration date, possibly the CVV2 (number on the back of the card), and possibly the PIN code. They stated that other personal information (address, social security number, bank accounts, etc.) was not compromised.

On February 9, 2006, Bank of America announced that an unnamed retailer might have compromised 200,000 credit card numbers.[1] The media quickly speculated that the retailer might be Wal-Mart or OfficeMax.[2,3] After conducting an informal survey, it appeared that all people who remembered receiving new cards had used their cards at OfficeMax. In contrast, some of the people surveyed reported that they did not shop at Wal-Mart.

On March 17, 2006, a new theory surfaced, naming Fujitsu Transaction Services (FTS) as a possible source of the compromise.[4] FTS is the POS provider for OfficeMax, as well as many other big-box retailers. This announcement included information that matched the impact from a POS system compromise. Although the person responsible for the compromise is unknown, the retailer is inconclusive, and the details of the compromise continually change, the method for conducting the compromise is likely due to a lack of POS security. Furthermore, the unsafe storage of credit card information in POS systems is not limited to FTS or OfficeMax; it impacts nearly **every** POS vendor and retailer. This vulnerability was discussed with Verifone between 1992 and 1993 – this is a fourteen-year-old attack method.

3 POS Overview

The Point-of-Sale (POS) system is comprised of components that perform credit card transactions. The main components are:

- *Card reader*. A device for reading credit cards. This device is either a standalone unit, such as the Verifone TRANZ system, or integrated into a cash register. It is most recognizable by the magnetic strip reader (MSR), numeric keypad, and receipt printer.

- *Transaction unit*. This device sends the credit card information to an authenticating source (e.g., Visa) and receives a transaction confirmation number. For Verifone, the card reader and transaction unit are integrated into an embedded device (although Verifone does sell individual components as well). The Verifone units consist of a digital display and a numeric keypad. For other devices, such as IBM SurePOS or Panasonic's POS Workstations, the card reader and transaction unit may be integrated into a cash register system.

[1] http://news.com.com/Bank+of+America+cancels+numerous+debit+cards/2100-1029_3-6037619.html
[2] http://news.com.com/Web+of+intrigue+widens+in+debit-card+theft+case/2100-1029_3-6038405.html
[3] http://attrition.org/errata/dataloss/boa05.html
[4] http://news.zdnet.com/2100-1009_22-6051261.html?tag=zdfd.newsfeed

- *Branch server*. Retailers usually network cash registers. A single computer at the store may collect all transactions for auditing purposes. The type of information collected varies by vendor, store, and location. Branch servers may be local to the particular store, regional, or national.

The network connection between the cash registers (or branch servers) and creditors usually uses strong authentication and cryptography. For example, X9.24 and X9.59 define an authentication and encryption system for financial transactions and are part of the Derived Unique Key Per Transaction (DUKPT) standard. Alternatives to DUKPT include the TDES standard and RSA's BSAFE. Regardless of the solution, traffic between the retailer and creditor is usually secure enough.

Although the communication between the retailer and the bank is protected, communications between the cash registers and branch servers are not always protected. For example, in 2005 Paul Timmins pleaded guilty to unauthorized access of a Lowe's Home Improvement store.[5] According to the legal records, Timmins and associates accessed credit cards through a wireless connection. Although this example is usually used to focus on the risks of open retail WiFi networks, it also brings up the question of network security: the case demonstrated a lack of protection for credit information on the retailer's internal network.

However, while the security of network transfers varies greatly between retailers, the end points in the POS architecture are very vulnerable. The two places that are most vulnerable for exposing customer credit card information are the *POS terminal* (card reader, transaction unit, and/or cash register) and the branch server (local, regional, and national).

Compromising these systems requires physical access – usually leading to a low risk profile. But with POS terminals, every employee and most customers have physical access. For branch servers, access may be more restrictive, depending on the retailer. Offsetting any deterrence from physical access is the sheer volume of cards that can be compromised. The large volume of information is a highly attractive target. Combining the volume with the amount of damage from a single compromise makes this a high risk. Finally, as suggested by the February 9, 2006 announcement, this type of compromise is likely more than theoretical.

4 Existing Security Measures

POS vendors seem to take a reactive approach to security. Security measures are generally not initiated until after credit card providers require them. The PCI DSS is one example of a reactive approach to security. In late 2004 Visa, MasterCard, Discover, and American Express addressed the issue of large credit card compromises by releasing the Payment Card Industry Data Security Standard (PCI DSS). This standard lists twelve major points for evaluating security risks[6]:

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

While the PCI DSS is definitely a step in the right direction, it has many significant limitations:

[5] http://www.securityfocus.com/news/9281
[6] https://sdp.mastercardintl.com/pdf/pcd_manual.pdf and
http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

- **Too late**. The industry has known about the risks with credit card storage for more than 10 years. Yet they did not develop a unified solution until after a series of large credit card compromises.[7]
- **Best practices**. Many of the PCI items follow established best practices for maintaining a secure environment. For example, using firewalls, changing default passwords, and assigning all users unique identifiers have been best practices for network security for decades. One should question why this was not a standard procedure for the credit card industry until December 2004.
- **Missing scope**. While the PCI does focus on storage and information transfer, it does not address information flow or security concepts such as least-privilege. As a result, information may be stored in an encrypted form but remain easily recalled.

Adding to the limitations of the PCI DSS, many POS vendors appear to be slow at adopting these standards. Since the release of the PCI, there have been many credit card compromises.[8] A sample of this list includes:

- 9-Feb-2006: Breach of 200,000 credit cards, possibly involving OfficeMax and Fujitsu Transaction Services.
- 6-Feb-2006: Regions Bank cancels 100,00 credit cards following an unnamed compromise. (Note: This may be the same compromise as 9-Feb-2006, bringing the total to more than 300,000 cards.)
- 28-Jan-2006: The State of Rhode Island announces 4,118 credit cards were possibly compromised.
- 28-Dec-2005: Marriott International Inc. announces missing backup tapes containing 206,000 credit cards and social security numbers.
- 19-Dec-2005: A remote attack at Guidance Software compromises 3,800 credit cards. The breach likely occurred in November 2005.
- 12-Dec-2005: A breach at two Iowa State University computers compromised 2,500 credit cards.

5 POS Terminal Weaknesses

The POS terminal reads the credit card information, performs the credit transaction, receives the confirmation code, and stores information for audits. The type of information collected and stored varies by vendor and configuration. In general, this includes the information found on the credit card: name, card number, and expiration date. Some terminals also require manual entry of CVV2 or PIN codes; these may be stored as well. Other information, such as address, phone, or social security number are not stored on the credit card and therefore not stored on the POS terminal. The information collected matches the information reported as compromised by the February 9, 2006 announcement. It is likely safe to assume that the compromise concerned information collected by POS terminals.

5.1 POS Storage Volume

A single POS terminal may store hundreds of credit card numbers. The numbers are usually cleared out when the cash register is closed (at the end of the day or end of the shift) and when transactions are tallied, but not always. Exploiting a POS terminal requires physical or network access. Since POS terminals are almost never directly accessible by the Internet, the only consistently exploitable route is physical access. Fortunately, POS terminals are located in plain view. An attacker attempting to open a POS terminal with a screwdriver, or typing in long numeric sequences, will appear suspicious.

In contrast to subtle compromises, there is little to stop a smash-and-grab. Depending on the retailer, cash registers may not be anchored to the counter. In addition, most small retailers do not secure standalone POS terminals. An attacker armed with nothing more than wire cutters can disconnect the terminal and dash out the door. Even if the money drawer is not taken, credit card information stored in the terminal can be stolen.

The degree of a storage compromise primarily depends on the storage medium used by the POS terminal. Different terminals use different storage systems. The three most common systems are static RAM, compact flash memory, and hard drives.

[7] Keith Reid, "Defeat the Hacker", *National Petroleum News*; Jan. 2006, Vol. 98 Issue 1, p 40-44.
[8] http://attrition.org/errata/dataloss/

5.1.1 Static RAM Devices

Many POS devices use static RAM for storing credit card information. The information is kept in memory, providing an audit trail, until either the device's memory is cleared (using a specific command code), or the memory fills and older records are overwritten. Removing power from the device usually does not clear the memory.

Verifone is a POS market leader that provides devices with static RAM, or memory with a battery backup. Normally a card is swiped at the POS device, and a PIN or CVV2 number may be entered. A modem associated with the device calls a Verifone central office for card validation and acquisition of a confirmation number. The information stored in the POS device can be accessed through a set of key combinations and numeric passwords. An attacker only needs to know the key combinations for accessing the information. Different Verifone models use different key combinations.

Some Verifone key combinations list specific information (e.g., recall last transaction, show last confirmation number, show/set the telephone number it dials). There is also a combination (different for every model) that shows the last set of transactions – all information. If the POS device has 16 Megs of RAM, then it can recall up to 16 Megs of data. Verifone terminals have a minimal amount of memory, usually up to 512K, reducing the impact of a system compromise to a few hundred credit cards at best.

For example:
http://www.emdeon.com/documents/UserManuals/MassachusettsPayers/POS_Basics_Guide_Massachusetts_Multipayer.pdf
This manual describes the Verifone TRANZ 380 and 380x2 Point of Sale terminal. Pressing "FUNC/ENTER and 2" displays "a complete list of current payers on the POS device."

Similarly, the Verifone TRANZ 330 allows printing a batch report of all transactions in memory. At the keypad, a user can type "[enter] 31 [enter] 0 [enter]" to generate a batch report. Details of each transaction can also be recovered:

- Press BLUE Function key, then the 5 key.
- Terminal will display "Print Option?"
- Press the 3 key for reprint.
- Terminal will display "Enter Item #".
- Type in the transaction number listed in the batch report and press enter.

By entering the appropriate information, a duplicate receipt will be printed. Duplicate receipts include credit card information. Although some Verifone devices can be configured to not display the full card number, this setting can be changed if the master passcode is known (see "5.2 POS Authentication" for resetting the master passcode).

5.1.2 Compact Flash Devices

Static or battery powered RAM can be expensive to upgrade and is not easily removable, leading to higher service requirements for upgrades and maintenance. As an alternative, many POS vendors use Compact Flash (CF) memory for transaction storage. This allows the retailer to upgrade quickly or perform backups by swapping out CF memory.

Panasonic's 7900 POS workstation[9] is an example of a POS terminal that uses CF memory. The product guide for this device clearly describes the storage of credit card information within the CF: "Rest easy, your valuable store data is dually maintained in your 7900 and back-office PC, allowing easy data restoration when necessary." The guide also mentions that the CF memory is removable: "A field replaceable Compact Flash (CF) card allows you to easily maintain your workstation and save money on costly service visits." From an attacker's viewpoint, this is an invitation since the CF contains credit card information and is removable. The only deterrent is the difficulty related to removing the CF memory – this differs between terminal models.

Panasonic is not the only vendor with this vulnerability. IBM, NCR, and other POS providers that use CF memory are equally vulnerable.

[9] http://www.panasonic.com/business/pos/front_counter_cat.asp

5.1.3 Hard Drive Storage

Larger POS terminals are essentially a personal computer with a cash register in place of a keyboard. These devices usually run a variant of the Microsoft Windows operating system (Windows 2000 and XP are common), but Linux and custom operating systems, such as Windows Embedded for Point of Service (WEPOS), are occasionally provided. Rather than storing transaction history in memory or to CF, these devices store information on hard drives.

The IBM SurePOS and Panasonic JS930 are just two examples of POS terminals that contain hard drives. The problem with hard drive storage is that deleted files (including temporary files) are not always securely deleted. By default, most operating systems – including those used in POS devices – do not securely delete information. As a result, credit card information that is many years old may be recoverable from a single POS terminal.

5.1.4 Storage Security

To defend against the smash-and-grab and related attack vectors, the credit card companies developed the Payment Card Industry Pin Entry Device (PCI PED) certification. The PCI PED provides an extended checklist for securing information at the POS terminal. The requirements range from physical to logical.

Newer POS devices, such as the Verifone V* series, are PCI PED approved. For terminals such as the V*750, information is encrypted and a remote key is usually required for cryptography. When the POS terminal is removed, the key is no longer accessible and the data remains encrypted. Unfortunately, the PCI PED was not released until 2005[10] and the V* series were not released until January 2006[11]. As a result, PCI PED compliant terminals are not widely deployed.

5.2 POS Authentication

To prevent unauthorized access to the transaction information stored on a POS terminal, authentication codes are used. These passcodes attempt to restrict access to different functions on the terminal. Unfortunately, most codes can be bypassed or are set to default values.

Verifone provides many POS terminals that include a simple passcode system and backdoor code. Verifone TRANZ systems use a master code for accessing hidden functionality, and a backdoor code in case the master code is accidentally lost.

For example:
http://www.binrev.com/forums/index.php?showtopic=3761&pid=31908&mode=threaded&show=&st=&
In 2003, the user "Ozlo" was amazed that the Verifone terminals at Wal-Mart saved information and used a master passcode. Quoting Ozlo:

> "Press [ENTER] + the top left button (usually unlabeled) simultaneously on the device. This will bring up a password prompt. The default for some Verifones is supposed to be 166816, and I've also seen 166831 to be a default as well."

Each model of Verifone POS terminal has a *default* master passcode (e.g. 166816 or 166831). The client should set this code. The client's passcode may vary by company or location (e.g., Wal-Mart or a specific Wal-Mart store). In fact, every Verifone terminal at a single store could have a different passcode, but that complicates management. Usually there is one passcode per store or region.

5.2.1 Backdoor Options

Most Verifone POS devices also have a backdoor key sequence that is intended only for Verifone. If an administrator knows the right key combination then he can get into every POS device of the same model. This allows an administrator at Verifone to reset or reconfigured the device in the event that a master passcode is lost. An attacker who knows these key sequences can also gain access to the POS device.

[10] A variation of the PCI PED was developed by Visa in 2002 but not universally supported by other credit card providers. The Visa POS PED was later incorporated into the PCI PED.
[11] http://www.verifone.com/news/releases/release.cfm?contentType=newsReleases&contentId=126975

As an example, to reset the master passcode on a Verifone TRANZ 330[12]:

1. Press and hold the "*" and clear key at the same time.
2. At the "Enter Password" prompt, type "800 [alpha] 3 [alpha] 684 [alpha] 35 [alpha] 3 [Enter]".
3. The screen will display "Successful" indicating that the password has been reset.

Other systems have less complex methods for bypassing passcodes. For example, the IBM SurePOS has a jumper on the motherboard that is used to clear any CMOS password settings. Beyond the CMOS protection is the user login. For the SurePOS 500, the default master passcode is "12345" and there is no passcode set for operator accounts.[13] While it is recommended to change the default passcodes, it is not required.

Most POS operating systems use adequate methods to prevent unauthorized logins at the terminal. For example, there is no known backdoor login for Microsoft XP or Novell Linux (both are operating systems used by NCR terminals). However, even if the login passcode is unknown, an attacker with physical access to the hard drive (or CF memory) can easily bypass the authentication.

5.2.2 Lax Security Processes

It is important to recognize that the Verifone TRANZ series is based on 1990 technology. Although the Verifone Omni has replaced the TRANZ, TRANZ terminals are still widely used by many retailers. Newer models do incorporate some security features. For example, if the system password on a Verifone Omni 3750 is lost, then it cannot be recovered. Unfortunately, some third-party providers view this as a limitation. In July 2004, Electronic Data Systems Corporation (EDS) provided a manual for the Omni 3750 to the Idaho Medicaid system. In this manual EDS wrote[14]:

> You can enter Eligibility Verification mode without using a password. System Device Setup mode does require a password that you received with your new POS device. The default Terminal Password is 000000 (six zeros). **It is strongly recommended that you do not change the default password.** This will eliminate issues regarding forgotten passwords.

The EDS manual also includes a sample Medicaid receipt, showing that the device stores social security numbers.

5.2.3 Impact of an Authentication Compromise

Beyond the initial authentication is the actual information stored on the terminal. While there are encrypted file systems for Windows and Linux, these do not appear to be used by any POS terminal. In particular, none of the manuals or documents for these devices discuss setting, resetting, or changing the password information for an encrypted file system. In other words, the initial authentication can be bypassed, and after bypassing the authentication an attacker is given direct access to financial transaction information.

Adding to this vulnerability, many POS terminals do not log all functions. For example, the Verifone TRANZ terminals do not log that a receipt was reprinted. An attacker can use this knowledge to compromise credit card information without leaving a transaction history.

5.3 Security Up For Auction

Although standing at a checkout counter and punching codes into a Verifone device (or opening up an NCR cash register to access the hard drive) is likely to raise suspicion, there are other ways to access this information. For example, a less-than-trustworthy employee may be left unsupervised. Similarly, spare equipment may exist in a back room and contain information residing from the last use. For many retailers, POS terminals are readily available and employee access may not be suspicious.

---

[12] http://www.arjaydata.com/support/download.htm
[13] http://www.collegeid.com/SurePOS%20500%20Manual.pdf
[14] Quote, including the bold emphasis, are from page 1-12 in
http://www.healthandwelfare.idaho.gov/_rainbow/documents/medical/Provider%20Handbooks/POS_handbook.pdf

For non-employees, auctions are a very viable option. Auctions are where companies sell off assets including POS terminals and cash registers. While the theft or tampering of a POS terminal could lead to the reporting of a potential compromise, a legitimate sale would have no reason to be reported.

Searching Google for "verifone", "bankruptcy", and "auction" brings up thousands of sites, including eBay, where Verifone POS terminals are being auctioned off. There is no assurance that the card information was wiped before the auction. Considering that every POS model has a different reset sequence, it becomes unlikely that the auction house cleared the memory before the sale. In addition, while many organizations recycle or destroy computer hard drives prior to auction, hard drives in cash registers are usually overlooked and are sold with POS terminals.

Consumers should be cautious when using credit cards during "going out of business" sales. The cash register and POS terminal may become part of an auction, along with any credit card information residing in the device.

6 Branch Server Vulnerabilities

A single POS terminal may contain hundreds or thousands of credit cards, but a compromise only impacts people who used that particular terminal. In contrast, branch servers allow for much larger compromises.

Branch servers collect information from multiple cash registers. They may be local (existing within the store), regional, or national. A local server may store tens of thousands of credit cards. In contrast, a regional or national system can store hundreds of thousands, or millions, of credit cards.

Branch servers are effectively networked PCs with a database of transactions. As with the POS terminal operating systems, these devices usually run some version of Windows or Linux, and offer no protection beyond the initial (bypassable) authentication. The only true protection comes from restrictive physical access. For small merchants, the server may be located in a back room. Larger companies may have more restrictive access.

The compromise announced on February 9, 2006, was likely a regional or national branch server. While the compromised information matches the information collected by POS terminals, the impacted scope spanned the entire United States. Similarly, the volume (200,000 credit cards) implies a central collection system, and the inability to specify the actual cause suggests the lack of an audit trail. These all match the symptoms of a branch server compromise.

6.1 Convenience versus Security

Having a system that saves credit card information for a region benefits merchants by offering convenience to customers. For example, Target (Target Corporation), BestBuy, and Circuit City only require a receipt for customer product returns. A customer can purchase a product with a credit card at one Circuit City, and return it at any other Circuit City without providing the original credit card; only the receipt is required. The receipt contains a transaction code that is matched with a regional (or national) database where the credit card information is stored.

Unfortunately, this type of convenience requires the merchant to save credit card information. This appears to be a direct violation of the PCI policies on credit card management. If the merchant has a return policy of 30 days, then the credit card information is stored for at least 30 days. In the case of Target, some items can be returned within 90 days – that means credit card information is saved at a branch server for at least three months.

6.2 Impact of a Branch Server Compromise

Branch servers offer a single point for a very large credit card compromise. Although the vulnerability is restricted to physical or network access, this does not provide sufficient protection. As shown by Timmins, et al., network access to the branch server may be vulnerable. Similarly, one news report suggests that the compromise announced on February 9, 2006 was due to an open WiFi network involving a Fujitsu Transaction Systems branch server.[15] Without adequate logging, the compromise could have occurred anywhere and would be untraceable.

[15] http://www.msnbc.msn.com/id/11963088/

Additional news reports have associated the compromise with a Tracer Utility program provided by many POS vendors including Fujitsu Transaction Systems.[16] This program was intended for diagnostics but may have saved information (including data and encryption keys) to a hard drive. Unfortunately, there are problems with this explanation:

1. A diagnostic program used at an individual outlet would not lead to a massive, nation wide compromise. Yet replacement cards were issued to people all across the nation.

2. If the program were used at a national branch server, then the data should be protected by physical and network security. However, the announcement indicates a breach. This means the attacker had system access. An attacker with system access should be able to retrieve stored information, run existing software, or install hostile software. As a result, the particular "tracer utility" would not be essential to the exploit.

While the diagnostics program may have been present and assisted with the compromise, it was unlikely the source of the compromise. The "tracer utility" theory is more likely an effort to shift blame than to address the true cause.

Internal, corporate networks can expose information stored at a branch server. But the risk is not only network based. Given enough incentive, an insider with physical access can easily compromise a national branch server. The core risk is **not** that someone could possibly compromise a branch server; the risk is that the information is stored on the branch server in the first place. An attacker cannot steal information that does not exist.

6.3 Additional Customer Information

In most cases, a compromised branch server will only disclose information collected from credit cards, but in some situations, there may be additional information available. For example, many grocery stores and retailers use frequent shopper cards. The registration for these cards includes name, address, phone number, and birthday (or year of birth). Since receipts includes both the frequent shopper number and credit card number, the branch server may associate credit cards with shopper information. A breach of the branch server could compromise more personal information than strictly found on the credit card.

6.4 Scale of a Large Compromise

Although there have been large compromises, resulting in millions of stolen credit cards[17], these are relatively small with regards to a potential compromise from a large retailer. Consider the hypothetical impact from a national branch server compromise at a large retailer such as Target.

- Target allows a 90-day return policy on items and a credit card is not required for refund processing. This implies that Target holds credit card information for a minimum of 90 days.

- Without knowing the exact statistics, we can assume that each store handles an average of 2,000 credit cards per day. This is likely an underestimate.

- According to the corporate information at www.target.com, there are at least 1,300 stores operated by Target Corporation.

These assumptions result in an estimated 234 million credit cards stored in the Target Corporation national branch server.

$$90\,days \times 1{,}300\,stores \times 2{,}000\,cards = 234{,}000{,}000\,total\,cards$$

This estimated total number of cards is likely a gross overestimate. Many people revisit the same store in a 90-day period. Assuming that 75% of the cards are from repeat customers, this still results in 58.5 million unique credit

[16] http://www.eweek.com/article2/0,1895,1939846,00.asp
[17] http://attrition.org/errata/dataloss/

cards. That is more than the 40 million cards included in the CardSystems compromise of May 2005.[18,19] In actuality, the estimated 58 million cards at the branch server is likely an underestimate for large retailers such as Target.

7 Mitigation Options

While not using credit cards does prevent exposure, it is not a practical option. It has been reported that the financial industry has been aware of these risks for years, yet their actions show little effort until very recently to address this problem. There are questions that should be asked by consumer advocates and retailers in order to understand the customer credit risk exposure.

7.1 Questions For POS Terminal Vendors

Retailers and consumer advocates should ask the following questions to POS terminal vendors:

Is the credit card information lost when power is removed?
If the answer is "no" then the information is stored in a relatively permanent location. The information could be accessed by a potential attacker, or remain in memory when the POS terminal is resold.

How many transactions can be retained in the device's permanent storage?
This allows an estimate for the impact of a compromise. If only one credit card is held at a time, then this is a low risk. If hundreds can be retained, then this becomes a high risk.

How often is the information purged from the POS terminal?
Frequent purges (hourly or every few hours) lowers the risk profile. There is a high risk of a compromise if any part of the POS terminal holds information indefinitely. For example, if the card reader holds information after the cash register is cleared, then the card reader poses a threat to consumer credit information.

What is needed to purge information from the POS terminal?
It can be a high risk if a human must remember to enter a code to clear the information. Automated clearing, such as on a timed schedule or when the register is closed out, is much more secure. Information should not be stored if there is no method to purge the data.

Is the permanent storage medium removable? What effort is needed?
A locked metal case that is anchored to a counter is a stronger deterrent than a Compact Flash card that can be removed with a thumbnail or screwdriver.

Is the permanent storage encrypted?
Many laptop vendors uniquely lock the hard drive to the motherboard. This prevents data on a stolen hard drive from being access by any other system. Similarly, encrypted file systems cannot be accessed without a unique key. If the POS terminal's permanent storage is not encrypted, then an attacker can easily access it. The PCI PED also attempts to address this issue: if the cryptographic key is not stored on the POS device, then the impact from a storage compromise is reduced.

When deleting information from permanent storage, is a secure erase used?
Simply deleting (or unlinking) a file can leave recoverable information. At minimum, overwriting the file with zeros will clear the disk space. More secure deletion options include overwriting with a set of random data.

Does the system require changing the default authorization code?
Secure systems require setting or changing the default password during the initial configuration. For example, current Linux and BSD systems cannot be installed without setting an initial password. (Even if the password is set to a blank password, it is still a required setting.) Similarly, POS terminals should not allow use with default

[18] http://www.usatoday.com/tech/techinvestor/corporatenews/2005-07-20-visa-amex-cut-ties_x.htm
[19] http://www.greensheet.com/PriorIssues-/060302-/7.htm

passcodes. The PCI DSS does state that the default settings should be changed, but POS terminal software does not enforce the requirement.

Is there a backdoor code for bypassing or resetting authentication?
If a backdoor exists, then it can be use by an administrator or an attacker.

Does resetting the authentication also clear stored records?
If a reset allows access to stored records *and* an attacker can perform an authentication reset, then an attacker can access stored records. Ideally, resetting the authentication should also reset all stored information. This prevents an attacker from gaining unauthorized access.

Is an administrative code needed to reprint receipts or view transactions?
If no code is needed, then anyone with access to the POS terminal can view transaction information.

Are all actions logged and associated with a specific operator account?
Creating, modifying, or viewing transaction information should be logged. The logs should indicate the unique operator performing the action.

7.2 Questions For POS Branch Server Vendors

Retailers and consumer advocates should ask the following questions to POS branch server vendors:

How long is credit card transaction information held?
Storing confirmation codes is generally not a risk, but storing full credit card information is a very high risk. The longer it is held, the bigger the risk of being compromised.

Can consumers opt-out of credit card storage?
If a consumer does not wish to have credit card information held indefinitely by a retailer, then a process needs to exist for requesting and removing the information.

Does the branch server ever send credit card information back to the POS terminal?
A high risk of exploitation exists any time the answer is “yes”. Information in a secure environment should not easily pass from a level of high security to a level of less security. For example, military information may be unclassified, secret, or top secret. Information can be easily passed to a more secure environment (e.g., from secret to top secret), but cannot be easily passed to a less secure environment (e.g., from secret to unclassified). Branch servers should follow a similar classification model. In addition, transaction IDs can be used to reference classified information without needing to pass credit card information back to the POS terminals.

Are there publicly accessible POS terminals?
Circuit City, for example, has terminals located all throughout the store. An unmonitored terminal is an open invitation to attackers.

Can the POS terminal be used to browse credit card information stored on the branch server?
While browsing or listing transactions can be useful for auditing information, it can also be exploited by allowing an attacker to list sensitive information. This should never be allowed from a POS terminal.

7.3 Questions For Retailers

Consumer advocates should ask the following questions to retailers:

Where are the POS branch servers?
A remote branch server is more secure because it limits physical accessibility.

Who has physical access to the branch server?
A server located in a locked room is less risky than one stored under the front counter or in an unlocked storage area.

How long is full credit card information stored at the branch server?
Cryptography is not part of this question; as long as information is stored somewhere, it can be stolen.

How is information transferred from the POS terminal to the branch server?
If data is transferred unencrypted across the retailer's network, then it is vulnerable to interception.

Is the retailer's WiFi network linked to the POS system?
Even with encryption enabled, wireless networks are vulnerable to attack. In general, wireless networks are accessible by anyone who can receive the radio signal. Wireless networks with cryptography only limit the time needed for an attacker to access the network. In addition, encrypted wireless networks do not protect information from other nodes on the encrypted network.

Are demonstration systems on the same network as the POS terminals or branch servers?
There are regular reports of retailer floor systems with access to corporate networks. For example, BestBuy has been reported as having customer-accessible demonstration computers on the corporate backbone.[20] This wired connection can allow an attacker to compromise sensitive information.

Are there multiple layers of network security and remote authentication?
A strategy of defense-in-depth, where there are multiple protection steps, lowers the risk profile by increasing the difficulty of a compromise.

What steps have been taken to address known security risks?
After each public compromise, consumers should ask if other vendors are vulnerable. For example, following the alleged OfficeMax compromise through a Fujitsu Transaction Systems POS solution, other FTS-based retailers should have established solutions that address the same risk. For example, Kroger and Home Depot use FTS. Are they vulnerable to the same type of compromise? If they are not vulnerable, then why are they not vulnerable?

Security-by-obscurity only works against people who do not know the exploit. In the reported case of FTS, there is clearly *some* attacker who knows an exploit.

8 Conclusion

On February 9, 2006 a massive credit card compromise was publicly disclosed. An estimated 200,000 credit cards were potentially compromised. Although (1) the retailer has not been officially named, (2) the method of exploitation has not been confirmed, and (3) the culprits behind the exploit have not been identified, the fundamental mechanism that enabled the compromise is likely known. Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly every POS provider is vulnerable, including Verifone, Fujitsu Transaction Solutions, Retalix, Hypercom, AutoStar, Innovax, JDA, JPMA, NCR, StoreNext, IBM, and Systech. Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, Target, Wal-Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product can be returned at any store, then the retailer likely has a serious vulnerability.

The vulnerable aspects of the POS architecture are summarized as follows:

- **POS Terminal**. These devices store credit card information. The security is primarily limited to physical access and initial authentication. An attacker with physical access can bypass most authentication requirements.

- **Transaction Security**. The connection between the cash register and the bank, for authorizing the transaction, is relatively secure and has a low risk of exploitation.

[20] W1nt3rmut3, "Best Buy Insecurities", *2600 The Hacker Quarterly*, Vol. 20.1, Spring 2003, p. 21-22.

- **Network Security**. The connection between the POS terminal and the branch server varies greatly. Some retailers have virtually no security, while others may be very secure. But an attacker who gains physical access to the network may be able to bypass security measures; the vulnerability varies between retailer configurations.

- **Branch Server**. These systems save information for specific stores and wide regions. The primary security options come from network security (preventing unauthorized remote access) and restrictive physical security. An attacker who is able to overcome either of these limitations can potentially compromise hundreds of thousands, or millions, of credit cards.

Even though other sightings have occasionally surfaced, the February 9th announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. It is only a matter of time before a national branch server at a large retailer is compromised.

9 Reporting History

The following information details the reporting history of this vulnerability.

1992-1993: Worked with a startup company on a modified POS system. Identified initial flaw with Verifone system. Disclosed risk (in person) to Verifone and verbally told not to be concerned. At the time, this type of identity theft was considered rare and this was a very low risk.

January 2006: A 200,000 credit card compromise was announced and many people were issued new cards. One card provider stated that an unnamed retailer might have compromised the credit card number. There were no fraudulent charges, but they were replacing the card just in case. The card company said that the following information might have been compromised: name, card number, expiration, CVV, possibly the CVV2. Other information, such as phone, address, and SSN were not compromised.

January - February 2006: Many associates who used credit cards at the local OfficeMax have received new cards. This primarily impacted Visa, but also included some Discover cards. At the time, nobody reported a new-assigned MasterCard or American Express (although it may have happened). By February 2006, news reports disclosed that the 200,000 card compromise that might be linked to OfficeMax or Wal-Mart.

17-March-2006: *http://news.zdnet.com/2100-1009_22-6051261.html?tag=zdfd.newsfeed.* ZDnet article describing how "cash-register software made by Fujitsu Transaction Solutions" may have exposed customer credit information at BestBuy, OfficeMax, and other retailers.

18-March-2006: Realized that this is the same flaw reported to Verifone back in 1992. Realized that there were too many vendors and retailers to contact. Sought assistance for contacting vendors and selected a few large vendors to contact directly.

19-March-2006: Disclosed summary to a security response organization (no reply).

21-March-2006: Disclosed to US government agency that investigates related exploits. Disclosed to iDefense VCP for independent verification, contacting specific vendors, and optional public disclosure. Attempted to contact Verifone.

22-March-2006: iDefense rejected the submission. Their reply: "Thanks for the submission. It certainly looks like an interesting piece of information." and "These days we adhere pretty strictly to a software vendor list (which I have attached). We still encourage you to help get this issue addressed. Good luck dealing with all of those vendors :)"

23-March-2006: Revised report to separate the three identified parts: POS device storage, POS auction exploitation, and POS centralized collection.

24-March-2006: Disclosed to a security company for potentially contacting retailers. They had no response from their retailer contacts.

27-March-2006: Attempted to contact Visa, but received no reply.

28-March-2006: Second attempt to contact Verifone.

5-April-2006: Advice from an independent security expert confirmed the decision to go public.

8-April-2006: Created formal write-up for public disclosure.

14-April-2006: Incorporated feedback from reviewers.

19-April-2006: Second attempt to contact Visa. No reply.

25-April-2006: Limited release. Between May 2006 and August 2007, the limited release versions were sent to various financial institutions, large retailers, credit card processors, and point-of-sale system manufacturers.

27-Aug-2007: Public release.

10 Addendum

In the 16 months following the limited release of this paper, many events occurred that appear related to the contents of this paper. In some cases, the events are clearly attributed to this paper reaching the "right" people. In other cases, the events may not be directly attributed to this paper, but the timing and details appear to be more than coincidental. The following events occurred:

- Between April 2006 and May 2006, Visa was provided with three copies of the limited release paper: one passed to Visa through a financial institution, one through a government agency, and one through a security company. Unfortunately, nobody at Visa ever contacted Hacker Factor Solutions nor acknowledged receipt. However, less than two months after receiving it, Visa released three security advisories related to topics detailed in this paper, including one advisory in June 2006 that appears to use questions taken directly from this paper:
  http://www.paymentech.com/pdf/Visa_Security_Alert_June2006.pdf
  http://www.chasepaymentech.com/pdf/Alerts_VisaDataSecurity_2006July31.pdf
  http://www.chasepaymentech.com/pdf/Alerts_VisaDataSecurity_2006August30.pdf

- In September 2006, Visa updated the PCI DSS to include some issues mentioned in this paper.

- Three months after receiving this paper, Visa reclassified their merchant security requirements.[21] Failure to comply would result in strict penalties or limited access. Unfortunately, in August 2007 Visa softened their strict stance.[22,23]

- Between March 2006 and August 2007, a few financial services companies, retailers, and law enforcement agencies received copies of the limited distribution. One financial institution said they planned to use it in a training exercise, and a big-box retailer agreed with many of the issues covered in this paper, but was not at liberty to discuss details.

- It has been observed that nearly every Verifone POS device is now either locked down or moved away from an open counter. This change happened very suddenly in July 2006, although no advisory saying to take this precaution has been identified. In particular, nearly all TRANZ 330 units were replaced with more secure units, locked down, or moved away from open counters. This matches the explicit examples from Sections 5.1.1 and 5.2.1, and the mitigation option mentioned in Section 7.1, question #5. However, few of the fast-food POS merchants seem to have taken preventative measures. In addition, a May 2007 news

[21] http://usa.visa.com/about_visa/press_resources/news/press_releases/nr332.html
[22] http://www.eweek.com/article2/0,1759,2171641,00.asp
[23] http://usa.visa.com/about_visa/press_resources/news/press_releases/nr419.html

report identified that thieves are using physical access to compromise point-of-sale devices in order to steal credit card numbers.[24] This exploit is explicitly discussed in this Section 5: POS Terminal Weaknesses.

- An anonymous and unverified tip claimed that this paper led to an audit that resulted in the discovery of the TJX credit-card compromise. (It was attributed to Section 3: POS Overview.) In particular, the tip mentioned that the compromise came through a wireless connection. The tip was received a month before this detail became public knowledge.[25] Later reports[26] indicate a series of compromises including attacks to the wireless network, physical access exploits to the local network, theft by skimming, and a failure to follow PCI security standards. It is also worth noting that the size of the TJX compromise (45.6 million credit cards) closely resembles the estimate compromise size from a big-box retailer (58.5 million cards) found in Section 6.4: Scale of a Large Compromise.

At the DEF CON 15 security conference (August 2007), Brendan O'Connor gave an excellent presentation about vulnerabilities in online banking. His presentation focused on client-side risks due to poor authentication systems. These risks easily extend to online retail shopping. Between O'Connor's presentation (risks from banking online) and this paper (risks from credit card storage), the financial infrastructure is being exposed as having nothing more than a security façade. Due to the reactive nature of the credit card industry, it is no wonder that credit card theft is growing at an exponential rate.[27]

[24] http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051800060_pf.html
[25] http://weblog.infoworld.com/zeroday/archives/2007/05/wardriving_may.html
[26] http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201400171
[27] http://www.iht.com/articles/2007/05/11/news/mcredit.php