APUS Library Capstone Submission Form

This capstone has been approved for submission to and review and publication by the APUS Library.

<table>
<thead>
<tr>
<th>Student Name</th>
<th>Munoz A.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Number</td>
<td>ITCC698</td>
</tr>
<tr>
<td>Professor Name</td>
<td>Dr. Beverly JN Bowen</td>
</tr>
<tr>
<td>Program Name</td>
<td>Master of Science Information Technology</td>
</tr>
<tr>
<td>Keywords</td>
<td>Credit card, identity theft, data breach, Target, Hannaford Brothers</td>
</tr>
<tr>
<td>Passed with Distinction</td>
<td>Y</td>
</tr>
<tr>
<td>Security Sensitive Information</td>
<td>N</td>
</tr>
<tr>
<td>IRB Review Required</td>
<td>N</td>
</tr>
<tr>
<td>Turnitin Check</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Required

Capstone Approval Document

The thesis/capstone for the master’s degree submitted by the student listed (above) under this title *

COUNTERING MAN-IN-THE-MIDDLE ATTACKS IN POINT OF SALE CREDIT CARD TERMINALS

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

<table>
<thead>
<tr>
<th>Program Representatives</th>
<th>Signatures</th>
<th>Date (mm/dd/yyyy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed, 1st Reader * [capstone professor]</td>
<td>[Signature]</td>
<td>[Date]</td>
</tr>
<tr>
<td>Signed, 2nd Reader (if required by program)</td>
<td>[Signature]</td>
<td>[Date]</td>
</tr>
<tr>
<td>Recommendation accepted on behalf of the program director *</td>
<td>[Signature]</td>
<td>[Date]</td>
</tr>
<tr>
<td>Approved by academic dean *</td>
<td>[Signature]</td>
<td>[Date]</td>
</tr>
</tbody>
</table>

* Required

Send thesis submission to: ThesisCapstoneSubmission@apus.edu

Attachments must include:
- This completed form
- FINAL Thesis document as Microsoft Word file
- IRB Review docs (if applicable)
COUNTERING MAN-IN-THE-MIDDLE ATTACKS IN POINT OF SALE CREDIT

CARD TERMINALS

A Master Thesis

Submitted to the Faculty

of

American Public University

by

Alex Munoz

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

November 2014

American Public University

Charles Town, WV
The author hereby grants the American Public University System the right to display these contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by the United States copyright law for the inclusion of any materials that are not the authors’s creation or in the public domain.

© Copyright 2014 by Alex Munoz

All rights reserved.
DEDICATION

I dedicate this thesis to my wife, parents, and dog Lucy. Without their continuing support, patience, and understanding, I would not have been able to complete my studies. It is their love and encouragement which continues to push my limits, and enables me to continue my journey.
ACKNOWLEDGEMENTS

I wish to thank the faculty at the American Public University for their support, encouragement, and dedication to furthering knowledge through higher education. It is the unique approach to distance learning at this university which enabled me to get this far. Without a flexible schedule tailored to my busy lifestyle, none of this would have been possible.

I credit both Dr. Louay Karadsheh and Dr. Matthew D. Gonzalez with setting the standard for facilitating a fair, modern, and approachable learning environment. It goes without saying that it is the encouragement I found with them, that kept me motivated.
Credit and debit cards have become the preferred method of payment for many, thanks to their low cost, convenience, and limited liability. As acceptance of these payment methods has become commonplace, criminals likewise increasingly target these accounts to commit fraud. Although various initiatives over the years have aimed at reducing credit card theft by hardening, or implementing additional security features, the overall system of processing these transactions is based on outdated technology. This study examines current technologies, their vulnerabilities, known exploits, and alternatives to existing processes, for the purpose of securing credit card information and transaction processing. Various countermeasures are evaluated in a three level probability impact matrix in order to compare their effectiveness in preventing credit card theft. The researcher concludes that by implementing established technologies and extending the standards currently used for credit card transactions, backward compatibility is ensured, while also allowing the deployment of more secure systems at low cost.

*Keywords:* credit card, identity theft, data breach, Target, Hannaford Brothers, TJ Maxx, Apple Pay, man-in-the-middle attack, electronic payments
# TABLE OF CONTENTS

COPYRIGHT PAGE ........................................................................................................ ii
DECLARATION........................................................................................................ iii
ACKNOWLEDGMENTS.............................................................................................. iv
ABSTRACT.................................................................................................................... v
TABLE OF CONTENTS............................................................................................... vi
LIST OF TABLES........................................................................................................ ix
LIST OF FIGURES..................................................................................................... x
LIST OF CHARTS....................................................................................................... xi

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Statement of the Problem</td>
<td>2</td>
</tr>
<tr>
<td>Statement of the Purpose</td>
<td>3</td>
</tr>
<tr>
<td>Research Questions</td>
<td>4</td>
</tr>
<tr>
<td>Significance of the Study</td>
<td>4</td>
</tr>
<tr>
<td>Definitions of Terms</td>
<td>4</td>
</tr>
<tr>
<td>Limitations</td>
<td>5</td>
</tr>
<tr>
<td>Assumptions</td>
<td>6</td>
</tr>
<tr>
<td>Theoretical Framework</td>
<td>6</td>
</tr>
<tr>
<td>II. LITERATURE REVIEW</td>
<td>7</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Payment Processing</td>
<td>8</td>
</tr>
<tr>
<td>Security Issues</td>
<td>13</td>
</tr>
<tr>
<td>Exposure of credit card data through duplication or interception</td>
<td>16</td>
</tr>
<tr>
<td>Modification of transaction details</td>
<td>17</td>
</tr>
<tr>
<td>Malicious transactions</td>
<td>18</td>
</tr>
<tr>
<td>Malware</td>
<td>18</td>
</tr>
<tr>
<td>Man-in-the-Middle Type Attacks</td>
<td>22</td>
</tr>
<tr>
<td>Case Study-1: The TJ Maxx Data Breach</td>
<td>26</td>
</tr>
<tr>
<td>Summary</td>
<td>29</td>
</tr>
<tr>
<td>Case Study-2: The Hannaford Brothers Data Breach</td>
<td>29</td>
</tr>
<tr>
<td>Summary</td>
<td>31</td>
</tr>
<tr>
<td>Case Study-3: The Target Data Breach</td>
<td>32</td>
</tr>
<tr>
<td>Summary</td>
<td>35</td>
</tr>
<tr>
<td>Literature Review Summary</td>
<td>35</td>
</tr>
<tr>
<td>III. METHODOLOGY</td>
<td>36</td>
</tr>
<tr>
<td>Identification and Operationalization of Variables</td>
<td>36</td>
</tr>
<tr>
<td>The Target Credit Card Malware Security Breach</td>
<td>38</td>
</tr>
<tr>
<td>Hypothesis</td>
<td>39</td>
</tr>
<tr>
<td>Technical Analysis and Data Sources</td>
<td>39</td>
</tr>
<tr>
<td>Limitations</td>
<td>41</td>
</tr>
<tr>
<td>IV. RESULTS</td>
<td>41</td>
</tr>
<tr>
<td>Analysis of the TJ Maxx Breach</td>
<td>42</td>
</tr>
</tbody>
</table>
Analysis of the Hannaford Brothers Breach .................................................. 44
Analysis of the Target Breach ................................................................. 46
Effectiveness of Common Countermeasures ........................................ 48
Effectiveness of Alternative Countermeasures .................................... 51
V. DISCUSSION ......................................................................................... 54
Summary .................................................................................................. 58
Conclusion ............................................................................................. 59
Recommendations .................................................................................. 60
LIST OF REFERENCES ........................................................................... 63
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Losses Due to Fraud in Card Payments in the United States, 2009</td>
<td>9</td>
</tr>
<tr>
<td>2. Characteristics of Publicly Disclosed Data Breaches in the United States</td>
<td>14</td>
</tr>
<tr>
<td>3. Suspected TJX Data Retention Practice Compared with PCI Standards</td>
<td>28</td>
</tr>
<tr>
<td>4. TJ Maxx Data Breach Vulnerability Impact Matrix</td>
<td>43</td>
</tr>
<tr>
<td>5. Hannaford Brothers Data Breach Vulnerability Impact Matrix</td>
<td>45</td>
</tr>
<tr>
<td>6. Target Data Breach Vulnerability Impact Matrix</td>
<td>47</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initiation of Magnetic-strip Card Payments</td>
<td>10</td>
</tr>
<tr>
<td>2. Initiation of Computer-Chip Card Payments</td>
<td>12</td>
</tr>
<tr>
<td>3. Countering Code Injection Attacks</td>
<td>19</td>
</tr>
<tr>
<td>4. Type of Attack: How Keylogger Malware can Capture Data</td>
<td>21</td>
</tr>
<tr>
<td>5. A Relay Attack</td>
<td>23</td>
</tr>
<tr>
<td>6. Attacker Controlled Assets</td>
<td>33</td>
</tr>
</tbody>
</table>
# LIST OF CHARTS

<table>
<thead>
<tr>
<th>CHART</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Value of Losses due to Card Payment Fraud in the United Kingdom</td>
<td>11</td>
</tr>
<tr>
<td>2. Publicly Disclosed Data Breaches in the U.S. by Sector, Jan. ‘05 – Mar. ‘13</td>
<td>15</td>
</tr>
<tr>
<td>3. Reported POS Malware Events Over Time</td>
<td>34</td>
</tr>
</tbody>
</table>
Countering Man-In-The-Middle Attacks in Point of Sale Credit Card Terminals

Introduction

Today, credit and debit cards are commonly used to pay for anything from parking fees to groceries, and expensive products or services. In addition to mobile and various other forms of electronic payment solutions, credit and debit cards are the preferred method for payments worldwide (Schuh & Stavins, 2012). Every time the cards are swiped at a merchant, confidential credit card information is exchanged with the merchant’s credit card processor for the purpose of authorizing a charge and billing to accounts. When criminals get hold of this confidential information, they can use the credit card details to purchase goods and services, thus causing $3.3 billion in damage to banks and cardholders through fraudulent online transactions in 2009 alone (Sullivan, 2010). In general, large amounts of credit card numbers are stolen if hackers get access to locally stored databases of credit cards, or credit card terminals (Berg, Freeman, & Schneider, 2008).

There are several other ways through which credit card information can be obtained by a criminal. This includes malware installed on a computer or mobile device, credit card skimmers installed at automatic teller machines (ATM), gas stations or mail theft, for example. While mobile devices have the potential to replace credit cards as the preferred method of payment, consumers are cautious and less likely to change their habits in fear of liability related to fraudulent transactions ("Cybercrime stalls uptake of mobile payments," 2011). Therefore, criminals resort to hacking, malware, and man-in-the-middle type attacks on high volume merchants, because computers and terminals
commonly used today are vulnerable to various exploits, making them an easy target for criminals (Bodhani, 2014).

Even though not all credit card terminals are hacked, by design most of them are insecure because during a swipe, credit card information is temporarily stored in random access memory (RAM) from which malware can be used to extract personal and confidential information. Furthermore, most credit card terminals are software-based solutions running on popular operating systems. Using these off-the-shelf environments makes all software running on them vulnerable to any discovered exploit that is generally applicable. Ramachandran and Ramachandran (2012) explain that even cloud-based operating systems are not immune from vulnerabilities and exploits, although many organizations try to improve the security of information technology (IT) infrastructure by separating networks, and utilizing intrusion detection systems, but with mixed results (Bejtlich, 2004).

Statement of the Problem

By design, most credit card terminals are insecure. For example, the Target security breach in 2013, where 70 to 110 million credit card details were stolen by infecting credit card terminals with malware, is just one of many reported such incidents ("Only the beginning?" 2014). Krebs (2014b) explains that the malware used to compromise the Target credit card terminals was unsophisticated and previously used during other heists. While Krebs (2014a) acknowledges that in order to install the malware, hackers had to first gain access to a firewalled network within Target’s organization, most credit card terminals are not protected against these threats, once other
security measures have failed. Krebs (2014d) further confirms that the Target security breach occurred over several weeks, and involved compromising several systems, a fact also pointed out in a United States Senate report (United States Senate, 2014).

In general, credit card terminals are susceptible to man-in-the-middle type attacks, because credit card information is often stored without encryption in RAM, where perpetrators are able to extract that information with the help of malware. According to Friedman and Hoffman (2008), the same vulnerabilities apply to mobile payment systems, which makes them a preferred target in the future, as their acceptance continues to grow (Dewan & Lei-da, 2005). The problem discussed is; therefore, twofold, in that credit card information can be extracted, and that it is often stored locally for a given period of time.

**Statement of the Purpose**

The purpose of this study was to examine current technologies, vulnerabilities, proposed changes, and general recommendations based on research, as they apply to credit card terminals and credit card transaction processing. In particular, the study looked into commonly used standards, such as transport layer security (TLS), secure socket layer (SSL), and public key infrastructure (PKI), identified weaknesses, and recommended new or improved processes, without requiring significant changes to existing infrastructure. In addition, the proposed changes will make it very difficult for hackers to infect credit card terminals with malware; and as an added benefit, communication between merchant and card processors will be more secure and less likely to fall victim to any kind of hacking attempt in the future.
Research Questions

- Which credit card terminals are vulnerable to man-in-the-middle type attacks?
- Which credit card terminals are susceptible to malware?
- How is credit information exchanged between merchants and banks?
- How can credit card terminals and credit card transactions be secured?

Significance of the Study

Malware is responsible for one third of fraudulent transactions, and 9 out of 10 incidents involving theft of credit card information from corporate and individual computers through some type of man-in-the-middle attacks (Anonymous, 2009). In addition, any computer system or mobile device used to interact with a merchant for the purpose of payment processing poses a security risk (Sujithra & Padmavathi, 2012). Malware often takes advantage of weak security in credit card terminals, and thus, unless terminals are significantly improved they will continue to be vulnerable against similar exploits in the future (Tuttle, 2014).

Credit card theft is a global problem, and it is on the rise (Sullivan, 2010). Therefore, finding ways to reduce vulnerabilities and harden security on credit card transactions, in general, will benefit merchants, banks, and customers.

Definition of Terms

- Credit Card Terminal: A device consisting of a card reader and software for processing and authorizing transactions between customers, merchants, and banks.
• Credit or Debit Card: A contactless, or contact requiring card that is tied to a bank account for the purpose of authorizing monetary transactions, paying the merchant, and charging the customer.

• EMV: A standard developed by Europay, Mastercard, and Visa, using a chip and personal identification number (PIN) system for credit or debit cards, instead of the commonly used magnetic strip (Anderson & Murdoch, 2014).

• Malware: Software that enables access to unauthorized information, or adds unwanted and unsanctioned functionality to a system, or particular IT environment.

• Merchant: A business or entity selling goods or services.

Limitations

• This study examined processes and their vulnerabilities on terminals used for credit and debit card terminals at merchant locations within the United States.

• Findings and suggestions for improving credit card processing and associated security are universal, but may interfere with future processes that have not yet been introduced, such as the planned introduction of chip-based Europay, Mastercard, and Visa (EMV) cards in the US in 2015.

Assumptions

• Customers continue to present a credit or debit card to the merchant, and the payment transaction is carried out through the systems operated by the merchant.
• Introduction of EMV cards will only marginally contribute to reducing credit
  card fraud, because transaction processing systems have not been secured,
  changed, or otherwise improved (Anderson & Murdoch, 2014).

**Theoretical Framework**

Not all credit card terminals are hacked, but by design most of them are insecure
or operate within an insecure environment. As hackers get more sophisticated in their
attempts to circumvent these countermeasures, a combination of structured query
language (SQL) injection and memory sniffing malware is likely to allow criminals to
steal credit card information in the future (Sullivan, 2013). While the initial introduction
of EMV cards in Europe resulted in less credit card fraud, hackers have become more
sophisticated over time, and damages from fraudulent transactions are on the rise again
(Sullivan, 2008).

Systems currently in use and vulnerable to exploits are examined in order to
secure them against man-in-the-middle type attacks. Questions, such as how these
systems work; how they interact; how most recent attacks have been used to compromise
them; and what is currently done to deter, detain, or prevent more of these types of
security breaches in the future, are quantified in terms of their effectiveness in preventing
theft related to credit card information. A three-level-probability-impact matrix was used
to evaluate areas that are most vulnerable to attacks, and therefore warrant immediate
implementation of the proposed and more secure processes (Peltier, Peltier, & Blackley,
2005).
Literature Review

Introduction

In 2011, US customers used debit and credit cards to authorize transactions worth more than $3.9 trillion (Sullivan, 2013). In addition, the acceptance of mobile payment systems and other forms of electronic payments continues to grow, and is accepted by an ever increasing number of merchants (Schuh & Stavins, 2012). What all these payment methods have in common is that they are associated with accounts. To review how these systems work, and the vulnerabilities they are subjected to, this unit is divided into logical sections:

- an examination of how payment processing works,
- the security issues faced by these systems,
- how malware is able to circumvent information assurance and non-repudiation, and
- the types of man-in-the-middle attacks most often used by criminals in order to compromise credit card security.

In addition, this unit will examine three applicable case studies, namely the Target data breach, the TJ MAXX data breach, and the Hannaford Brothers data breach.

Payment Processing

Traditional cash payments involve the exchange of money for goods, where an exact amount of money is transferred between the customer and the merchant. If the customer wants more goods or services, they have to pay more cash to the merchant or
service provider. In return, if the merchant wants more cash, they have to request it in person from the customer.

Electronic payments differ in that they authorize the transfer of a limited amount of currency between the customer’s and merchant’s account. This authorization is often tied to some sort of identification, a PIN, an account number, or a physical card. The problem with this approach is that unlike with cash where a transaction is concluded between two parties, a third party, such as a bank, is used to authorize a transfer.

Criminals use this vulnerability to post as one of the parties, or impersonate a third party, for the purpose of authorizing payments to a merchant without actually owning the authorizing account. As Sullivan (2013) explains and illustrates in Table 1, criminals caused more than $3.4 billion in losses as a result of fraudulent charges in 2009 alone. Although this number seems small in comparison to the reported $3.1 trillion of processed transactions during the same year, it is significant, and partially responsible for higher credit card processing fees charged by banks and merchant payment processors alike (Sullivan, 2013).

With credit and debit cards being the most popular payment methods today, criminals have shifted away from skimming individual cards, which is the process of making a copy of the data contained on a credit card magnet strip, to large scale credit card number harvesting hacks (Tuttle, 2014). These large scale heists are made possible by the insecurity of various credit card payment systems, in particular those that rely on magnetic-strips for exchanging payment information with a merchant ("Only the beginning?," 2014). As explained by Sullivan (2010), while the chip and PIN system
favored by the EMV system is more secure than using a magnet strip for storing account information, its ability to use tokens and encryption fails to protect it from several vulnerabilities that continue to exist in those systems, and would require a change of the underlying infrastructure, if the payment industry wants to fix them.

Table 1

*Losses Due to Fraud in Card Payments in the United States, 2009*

<table>
<thead>
<tr>
<th></th>
<th>Loss per Dollar</th>
<th>Value of Transactions in millions</th>
<th>Value of Loss(^1) in millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Debit Cards</td>
<td>0.0319%</td>
<td>$563,100</td>
<td>$179.6</td>
</tr>
<tr>
<td>Signature Debit Cards</td>
<td>0.1271%</td>
<td>$857,500</td>
<td>$1,089.9</td>
</tr>
<tr>
<td>General Purpose Credit Cards</td>
<td>0.1271%(^1)</td>
<td>$1,714,000</td>
<td>$2,178.5</td>
</tr>
<tr>
<td>Prepaid Cards</td>
<td>0.0401%</td>
<td>$140</td>
<td>$0.6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>$3,134,740</td>
<td>$3,448.1</td>
</tr>
</tbody>
</table>


\(^1\)The loss rate for general-purpose credit cards is assumed to be the same as the loss rate for signature debit cards.

\(^2\)Value of loss is the product per dollar and value transactions.

Sources: Figures for loss per dollar are from Board of Governors. Figures of value of transactions are from Federal Reserve System.

In general, all magnetic-strip card payments utilize a similar process. As illustrated in Figure 1, the cardholder swipes the card through a credit card terminal, which then communicates with the merchant’s payment processor in order to authorize a charge. The merchant’s payment processor then authorizes the charge with the cardholder’s bank, at which point a hold is placed on the cardholders account for the authorized amount. In addition, an authorization code is given to the merchant, so that they can collect the payment during their daily settlement with the payment processor.
It needs to be noted that early EMV payment systems operated in a similar way, with the only difference of encrypting credit card information on a chip, in addition to making the credit account information available via the additional magnetic strip as well. Anderson and Murdoch (2014) explain that the main reason for including a backward compatibility was that not many merchants were ready to process EMV payments, because they continued to rely on the old magnetic-stripe readers instead.

At some point, merchant processors and banks insisted that credit card terminals had to be upgraded, because fraud continued to grow, despite the apparently more secure approach of the EMV system. As illustrated in Chart 1, after the initial introduction of EMV cards, credit card fraud continued to rise in the following years because too many merchants were still relying on magnetic-stripe based transaction processing, instead of the more secure chip and PIN system.
In particular, a change in losses related to credit card fraud was observed in the U.K. around 2008, right after more secure EMV systems offering dynamic verification codes, or so-called tokens, were introduced and enforced at merchant locations (Sullivan, 2013). In general, in a modern EMV transaction the cardholder inserts the credit or debit card into a terminal to authorize payment to a merchant. The terminal then obtains a unique token, which is only valid for one transaction. The transaction data is then transferred to the payment processor together with the token, at which point the account information, and validity of the token is being verified with the cardholder’s bank for approval as illustrated in Figure 2.
Once approved, the process is similar to that of a magnetic-stripe based transaction in that the merchant’s processor will put a hold on the cardholder’s account for the authorized amount, and provides the merchant with an approval code for later settlement and transfer of funds.

EMV has clearly been designed to address most weaknesses of traditional magnetic-stripe-based credit card processing, in that it is able to use one-time unique tokens to prevent copying, and encryption to prevent cloning. It is also a two-way communication system, where a credit card terminal is able to interact with the chip on a cardholder’s card for improved security. As illustrated in Chart 1; however, Sullivan (2013) explains that in the case of the U.K., credit and debit card fraud has declined thanks to the introduction of tokens in EMV cards, but since has leveled out, and can now be seen on the rise again. A more thorough examination of how criminals continue to circumvent security measures of both traditional magnetic-stripe-based-credit-card processing, as well as EMV-based cards is necessary, in order to identify dormant vulnerabilities and security issues in all of these systems.
Security Issues

Any processing of electronic payments is subject to various vulnerabilities and security issues. Depending on how the transaction is carried out, several primary and secondary vulnerabilities need to be addressed in order to secure communication between parties, and prevent unauthorized duplication, or collection of transaction related details. Hacking and malware present the biggest threats to credit card processing systems, because they are able to compromise the communication process from various angles, using a multitude of exploits, and several accounts at a time (Anonymous, 2009).

While mail fraud, social engineering, and other scams are difficult to prevent, as they involve a human factor, they also target individual accounts only, thus reducing potential damages to banks and merchants (Sullivan, 2010). As illustrated in Table 2, most significant and dangerous threats to credit card processing today involve outside hacking attempts and malware installed on credit card processing terminals. Sullivan (2010) explains how many of the reported data breaches go unnoticed for an extended period of time, despite the use of sophisticated intrusion detection and prevention systems.

Bodhani (2014) blames both the intrusion of, as well as, the use of Windows XP-based software terminals for the rise of successful credit card data heists. In particular, many large retailers, such as Target, Home Depot, and Nordstrom use point of sale (POS) systems running on the Windows operating system (OS). Naturally, because these payment processing systems operate on a frequently attacked OS, with new
vulnerabilities being discovered on a regular basis, any POS using the same environment is automatically exposed to the same exploits and threats (Bodhani, 2014).

Table 2

*Characteristics of Publicly Disclosed Data Breaches in the United States*

<table>
<thead>
<tr>
<th>Source</th>
<th>Outsiders</th>
<th>64%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insiders-accident</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Insiders-malicious</td>
<td>7%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>27%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Stolen laptop or computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exposure on Internet or e-mail</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>Hack</td>
<td>16%</td>
<td></td>
</tr>
<tr>
<td>Documents lost in mail or on disposal</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Scams and social engineering</td>
<td>8%</td>
<td></td>
</tr>
</tbody>
</table>

*Notes:* Statistics based on 2,318 incidents since 2000 tracked by the Open Security Foundation (datalossdb.org, accessed on March 25, 2010). The incidents compromised personally identifiable information such as credit card numbers, social security numbers, names and/or addresses, financial account information, financial information, date of birth, e-mail addresses, medical information, and miscellaneous.

Sources other than those listed above include insiders and unknown.


As explained by Tuttle (2014), electronic credit card processing is facing the following main security issues:

- exposure of credit card data through duplication or interception,
- modification of transaction details, and
- malicious transactions.

It needs to be noted that these security issues apply regardless of the payment systems used, and can even be extended to other electronic payment methods and IDs, which in general are vulnerable to similar threats (Sullivan, 2008). Furthermore, not all data is
equally valuable from a criminal’s perspective. Individual data might be of use to investigators or foreign governments, but not as valuable to hackers who are primarily interested in financial gain, rather than personal information.

As can be seen in Chart 2, amongst publicly disclosed data breaches between 2005 and 2010, payment processors, financial services, banks, and retailers combined are responsible for over 70% of compromised records. This illustrates how financial

information continues to be a main target for criminals, and any existing security measures are failing to address the situation adequately.

**Exposure of credit card data through duplication or interception.** Both magnetic-strip and EMV-based credit cards are subject to communication interception, and duplication (Bodhani, 2014). With magnetic-strip credit cards, a perpetrator only needs to obtain the data contained on track 1 and track 2 of the actual card, in order to create a duplicate (Bodhani, 2014). Furthermore, an image of the front and back of the actual card is often enough to forge a replica or use the gained information to place orders online, by phone, or by mail, as neither the account holder’s information printed on the card, nor the same information stored on tracks 1 and 2 are encrypted ("Only the beginning?," 2014).

While EMV or radio-frequency identification (RFID) based credit cards encrypt account information, and are able to communicate with the credit card terminal for the purpose of increasing security, at least early versions of EMV cards were easily duplicated due to a flaw in the authentication process (Anderson & Murdoch, 2014). First generation RFID systems are subject to similar vulnerabilities, and even though those have been addressed, criminals have found other ways to successfully compromise and intercept communication between terminals and cards (Heydt-Benjamin, Bailey, Fu, Juels, & O'Hare, 2009).

A proposed solution to the issue of interception and duplication involves the use of unique tokens, where each token is generated by the chip on the credit card, and can only be used once (Sullivan, 2013). Another approach suggests that the use of mobile
generated disposable credit card numbers is able to address the issue of duplication and interception (Buccafurri & Lax, 2011). Unfortunately, both approaches are currently vulnerable to various exploits involving modification of transaction details.

**Modification of transaction details.** If a perpetrator is able to modify the particulars of a valid transaction, then what seems to be a charge for a parking meter to the cardholder, might end up paying for a camera elsewhere (Sullivan, 2013). EMV based cards and payments initiated through mobile devices are in particular vulnerable to this threat (Friedman & Hoffman, 2008). Merchants, payment processors, and banks try to limit their exposure to these vulnerabilities by encrypting communication between each other based on industry standards for secure communication (Peltier et al., 2005). Additionally, banks, processors, and larger merchants utilize intrusion prevention and intrusion detection systems to spot malicious activity, and to get notified when secure communication between parties can no longer be assured (Bejtlich, 2004).

As explained by Sujithra and Padmavathi (2012), often the mobile device itself is compromised by criminals and information is modified before it enters the secure communication systems between the merchant and their payment processor. As such, modified transactions remain often unnoticed until it is too late, because at first look, they seem to be legitimately authorized (Anderson & Murdoch, 2014).

**Malicious transactions.** One way to prevent credit card fraud is by identifying malicious payment transactions. Greene (2009) explains that malicious transactions can be summarized as those that are out of the ordinary and unusual for a cardholder. Banks have employed malicious transaction detection algorithms for the purpose of identifying
Malicious transactions, therefore, can be summarized as transactions that seem to be legitimate at first, but upon closer inspection fail to pass scrutiny due to their deviation from the norm. Criminals try to circumvent these pattern-matching systems by carrying out fraudulent transactions in expected ways, for example a cardholder based in Los Angeles, CA, may see fraudulent charges on the next bill originating in Los Angeles as well. The bank would initially assume that these transactions are valid because of the local constraint to an area where the cardholder would normally use their card. After the cardholder notices the fraudulent transactions on their bill, the damage is already done, and criminals have successfully managed to take advantage of the card processing system and its flaws (Malphrus, 2009).

**Malware**

Malware is generally malicious software where its creators intend to access restricted data without permission, modify data without getting caught, prevent legitimate communication between parties, or add new data which does not belong there (Peltier et al., 2005). There are various types of malware, each with a specific function and threat to an organization and its IT infrastructure. Included here are worms, logic bombs, viruses, and Trojan horses, for example (Peltier et al., 2005). Commonly, malware either tricks a
user into revealing confidential information, such as login details, or it scrapes otherwise restricted data from an infected system for transmission to, and use by, a third party (Jones, 2002).


Most often, the malicious attack is aimed at modifying existing code for the purpose of crashing an application, modifying its data, or tricking a system into revealing other information than originally requested as shown in Figure 3. According to Mitropoulos, Karakoidas, Louridas, and Spinellis (2011), these types of malicious code attacks are also referred to as code injection attacks. Code injection attacks are of particular concern for the security of payment systems because they hijack authorized
applications and secure communication paths in order to modify the information that is accessed or communicated (Mitropoulos et al., 2011).

According to Savage (2013), even encrypted programs running in memory are vulnerable to malware, because a perpetrator is often able to identify patterns and deduce certain functionality just by analyzing how memory is used and allocated. Furthermore, memory encryption is of little use, if the software running the encryption has been compromised, and now runs malicious code (Savage, 2013). The threat of code injection and malware running on credit card terminals is elevated further, because many software based terminals are running Windows XP, thus making them vulnerable to exploits generally applicable to this OS (Tuttle, 2014).

Most credit card terminals infected by malware are software based terminals (Sullivan, 2013). A software based terminal simulates a physical terminal’s functionality through the use of an external keypad, a signature pad, a display, and a card reader, all of which are connected to a host computer (Anderson & Murdoch, 2014). When a credit card is swiped through the reader, the information stored on the magnetic-strip is transferred to the software terminal running on the computer. Figure 4 illustrates how malware on an infected terminal is able to scan the application memory on the host for transaction details including the data extracted from the credit card, encryption keys, keystrokes entered on the host, as well as contents from all attached screens. While some malware is able to change data that is being transmitted between the merchant and the terminal facing the customer, most malicious code running on host computers is aimed at collecting data, rather than changing it (Sullivan, 2013).
The single most dangerous threat to credit card processing, its integrity and security, is malware. Malware is able to circumvent any existing countermeasures, it is able to remain undetected, and it is able to collect and modify data that is thought of being secure (Porkess & Mason, 2012). So far, any attempts to prevent malware from accessing credit card terminals have ultimately failed, because there are a very large number of possible attack vectors, and ways to infiltrate and compromise software based merchant terminals. Intrusion prevention and intrusion detection systems have shown to be ineffective in containing threats related to malware (Rosenblum, 2014).
Man-in-the-Middle Type Attacks

Man-in-the-middle type attacks are a common threat to computer and telecommunication networks (Traynor, McDaniel, & La Porta, 2007). In a man-in-the-middle attack a perpetrator positions themselves in-between the communication of two or more parties (Comer, 2009). If the communication is not encrypted, the party listening in without authorization is effectively eavesdropping on any data that is being exchanged between all parties. Many computer networks; therefore, use standards-based encryption, such as transport layer security (TLS) or secure sockets layer (SSL), to encrypt messages exchanged between parties (Willett, 2008).

What makes credit card payment processing vulnerable to man-in-the-middle attacks is that magnetic-strip based cards offer no encryptions, and EMV based cards have several vulnerabilities that allow a perpetrator to extract valuable credit account information (Sullivan, 2013). Furthermore, some of the currently known man-in-the-middle-attacks on credit card payment processing systems amend existing transactions in a way that a valid authorization is given for a fraudulent transaction (Bodhani, 2014). While encrypted messages are difficult to decrypt without keys, criminals focus on the weakest link instead, that is, they focus on extracting unencrypted credit card details stored in RAM when a card is swiped, or they try to partially change the contents of a transaction for the purpose of obtaining authorization for an unauthorized charge (Bodhani, 2014).

Using an existing system to trick both the processor and the cardholder in believing they authorize a different charge is a trick that has not yet been deployed on a
large scale basis, but it seems feasible, and a possible target for criminals, once EMV cards become more common (Sullivan, 2013). This particular form of man-in-the-middle attack is often referred to as a relay attack (Anderson & Murdoch, 2014). In a relay attack, the perpetrator sets up a fake terminal or uses malware to compromise an existing terminal. What seems to be a transaction for one item to both the merchant and the cardholder, will then authorize an entirely different charge for a different item, and for the sole benefit of the criminal only as shown in Figure 5.


This particular threat to transaction security is applicable to both magnetic-strip, and EMV based cards, and can be particularly devastating to both the merchant, as well as the cardholder. As explained by Anderson and Murdoch (2014), often credit card issuers do not honor fraud protection agreements with cardholders and merchants because the transaction seems to be legitimately authorized. In particular in the case of EMV cards, if the card was presented at the time of purchase, and the charge authorized with a valid PIN number. While the relay attack is a smart way to compromise otherwise secure
payment systems, the more commonly found man-in-the-middle type attack on credit card payment and processing systems is one utilizing RAM scraping malware.

RAM scraping malware often infects a host system for the purpose of extracting credit card, or other valuable data. In the case of credit card processing, extracting this information becomes difficult because once a transaction leaves the local network, a secure and standards based communication is established with the merchant’s processor (Wright, 2002). Anything that goes out and comes in as part of the transaction is now encrypted using a combination of TLS/SSL, and thus makes it difficult for a criminal to extract valuable information, should they be able to intercept any of that communication. To avoid having to deal with encrypted data, malware often looks for pattern associated with track 1 and track 2 of a swiped credit card (Sullivan, 2013). This data can be found in at least two points during a credit card transaction.

The first time a magnetic-strip’s Track 1 and Track 2 data becomes accessible is during the initial swipe at a credit card terminal. A perpetrator can tamper with the actual card reader by installing additional hardware, enabling the criminal to read the data at the same time the card is being swiped. Alternatively, they may use an insider to create a copy, once a cardholder has handed over their card for processing a transaction (Bhatla, Prabhu, & Dua, 2003). In both cases, a cardholder may not be able to immediately notice that their credit card details have been recorded. This approach puts the criminal at risk of getting caught in the act because they either need an insider they can trust or physical access to the credit card terminals. In any case, where credit card processing terminals are self-contained, such as they are often at smaller merchants, automated teller machines
(ATM), and restaurants, skimming with or without an insider may be the only way to carry out a man-in-the-middle attack in these environments (Bhatla et al., 2003).

For a large scale and more anonymous approach criminals have resorted to infecting software-based terminals with malware (Tuttle, 2014). In this scenario, an external card reader is used to transfer the credit card details from the card into the POS system. While most POS software encrypts data that is stored or processed further, the credit card information captured from the external card reader is generally raw, meaning that EMV data and magnetic-strip data is at least temporarily stored in the POS system’s RAM, while it is being acquired and often during the subsequent processing of the transaction (Sullivan, 2013).

This major vulnerability has been exploited successfully over the years with criminals gaining access to hundreds of millions of credit card information through the use of RAM scraping malware ("Only the beginning?," 2014). This approach is similar to eavesdropping on a conversation, where the communicating parties are unaware that someone else is listening in on them. Instead of securing terminals, merchants and banks have resorted to strengthening their networks against malicious traffic and hacks (Bodhani, 2014). The assumption often is, if an intrusion can be prevented through intrusion prevention and intrusion detection systems, no valuable information can be extracted beyond a corporate network, thus leaving the perpetrator with data that they cannot collect, or otherwise use (Bejtlich, 2004).

As explained in a United States Senate (2014) report, man-in-the-middle type attacks utilizing malware infected credit card terminals rely on four major variables:
COUNTERING MAN-IN-THE-MIDDLE ATTACKS

- data extraction to a location outside of the corporate host network,
- network intrusion,
- unnoticed collection of data, and
- vulnerability and infection of credit card terminals.

This form of man-in-the-middle type attacks is particularly devastating for an organization and credit card issuers, because criminals are able to gain access to a large number of credit cards in a very short period of time, while remaining anonymous during the heist (Riley, Elgin, Lawrence, & Matlack, 2014). Hackers prefer this approach, because they do not have to physically modify terminals, rely on third parties, or even live in the same country (Bodhani, 2014).

**Case Study-1: The TJ Maxx Data Breach**

The TJ Maxx (TJX) Data Breach was first reported in 2007 and is said to have exposed at least 94 million Visa and Mastercard accounts, resulting in a projected loss of $4.5 billion, or more (Berg et al., 2008). Hackers first gained access to internal networks through an inadequately secured local wireless access point at a TJX store location (Berg et al., 2008). As Berg et al. (2008) continue to explain, the criminals then used this access to further compromise accounts and machines on the corporate network until they were able to find credit card transaction records stored in files, containing full credit card information of customers who had recently used their credit cards at one of TJX’s locations.

Criminals were able to successfully carry out their heist, because TJX was not in full compliance with the latest payment card industry’s (PCI) standards, which requires...
discarding most credit card information after the transaction has been completed; for any
data that is retained strong encryption has to be used (Berg et al., 2008). The PCI data
security standards (DSS) 3.5 and 3.6 also require an organization to keep keys, used for
encryption and decryption of stored credit card information, separate and secure from
encrypted customer data (Berg et al., 2008). Table 3 illustrates how TJX only partially
complied with the PCI DSS, and where it did not, hackers were able to take advantage,
and extract valuable customer information.

The TJX case is in particular troubling because in addition to ignoring data
retention and data security requirements set forth by the PCI, TJX did also not follow
general IT best practices for data storage and information assurance (Schou &
Shoemaker, 2007). From a risk management perspective, TJX solely relied on the
security of its internal network, completely discounting the possibility that its network
can be compromised and that locally stored information is then exposed, without another
line of defense (Bodin, Gordon, & Loeb, 2008). Berg et al. (2008) suggest that TJX may
have failed to identify the locally stored credit card data as an asset, and therefore,
internal audits did not reveal any vulnerability. The argument is, that because TJX is
mostly concerned with securing the transaction and that credit cards are of no value to
them unless a charge is authorized by a customer, storing credit card information was
merely seen as a convenience factor, rather than an asset that needs protection (Berg et
al., 2008).

Generally applicable best practices and audits commonly used for information
assurance are aimed at identifying risks, threats, and vulnerabilities similar to the ones
that allowed criminals to infiltrate TJX’s internal network, and manage compliance with countermeasures effectively, in order ensure security and confidentiality (Layton, 2007). Berg et al. (2008) suggest that both the lack of appropriate audits and the lack of PCI compliance have enabled the TJX data breach, but also that inadequate and inconsistent security policies at TJX were a contributing factor for making this breach possible in the first place.

Table 3

Suspected TJX Data Retention Practice Compared with PCI Standards

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Data Retained by TJX</th>
<th>PCI Retention Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Service Code*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiration Date*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sensitive Authentication Data†</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

* Must be protected if stored in conjunction with PAN.
† Sensitive authentication data must not be stored after authorization (even if encrypted).

Note. Adapted from “Analyzing the TJ Maxx data security fiasco” by Berg et al., 2008, CPA Journal, 78(8), p. 36.

Summary. In 2007, at least 94 million Visa and Mastercard accounts were exposed to criminals in a data breach at TJX (Berg et al., 2008). Hackers gained access to local networks by infiltrating a wireless access point at one of TJX’s store locations. Once in the private network, the perpetrators then found several files containing credit
card information. These files included account numbers, expiration dates, card security codes (CSC), entire magnetic-strip data contents, as well as PINs (Berg et al., 2008). In this particular incident, hackers did not compromise credit card terminals but rather file systems containing copies of transaction details. The resulting data available to the criminals is similar in scope and content to what they would have been able to obtain through a man-in-the-middle type attack, utilizing a physical connection or malware.

The TJ Maxx case illustrates the importance of data encryption at any given point during the process of charging a credit card and subsequent storage of related data, as well as the need to delete any unnecessary transaction details after a transaction has been completed.

**Case Study-2: The Hannaford Brothers Data Breach**

In 2008, the Hannaford Brothers grocery chain fell victim to a targeted data breach at their nearly 300 stores, allowing criminals to collect over 4.2 million credit card details (Clapper, 2010). As explained by Clapper (2010), malware installed on credit card terminals was used to extract primary account holder names, account numbers, and card verification value CVV2 codes at the company’s locations in Vermont, Maine, New Hampshire, Florida, Massachusetts, and New York. The perpetrators then used the stolen account details for fraudulent charges in at least 1800 cases in the US, as well as in other countries (Clapper, 2010).

What makes this case unique are the number of collected credit card details, and the fact that all POS systems at the Hanford Brothers’ locations had recently been updated to comply with PCI standards. Unlike with other breaches before this,
hackers focused on extracting credit card information that is in transit, rather than data stored in local files, as for example happened with the TJ Maxx data breach (Berg et al., 2008).

The PCI DSS specifies that cardholder data needs to be protected, and that transmissions over public networks need to be encrypted (Clapper, 2010). It is unclear whether the Hannaford Brothers encrypted locally stored credit card information or whether they even stored this data past the charge and authorization process, but it took a team of 30 experts over a week to find the malware responsible for leaking credit card information to criminals (Clapper, 2010). What the researchers found was unlike any other large scale breach they had encountered before.

As Clapper (2010) states, unlike most POS systems that are based on a Windows OS, the Hanford Brothers picked a POS system based on Linux when they modernized affiliate and store IT in 2005. Linux is a common OS used for many web applications, as well as data storage servers and other server clusters, but it is not often found as the basis for a POS system (Clapper, 2010). Clapper (2010) revealed that the security team investigating the Hannaford Brothers data breach was convinced that the malware was custom designed for the purpose of working with this particular POS and extracting credit card information that is in transit.

The security researchers continued to be intrigued by how the perpetrators managed to circumvent network security and infect nearly 300 servers (Clapper, 2010). The way the POS system was set up at the Hannaford Brothers locations is that a credit card reader connected to the register would transmit credit card information, once a
customer swiped their card. This information is then sent from the terminal to a central
server on the same local network. The server is responsible for obtaining authorization,
initializing the charge, and complete the settlement process with the merchant’s processor
(Clapper, 2010). While this approach seems to be efficient from a merchant’s
perspective, because all operations are controlled and managed from within just a single
machine, it also enabled the criminals to compromise only one system in order to get
access to all credit card data acquired at any one of the nearly 300 Hannaford Brothers’
locations (Clapper, 2010).

Once the server was successfully compromised, the hackers intercepted all credit
card information, and stored it in local files. According to Clapper (2010), the criminals
then sent batches of credit card information to an overseas server from where they were
collected for future use.

**Summary.** The Hanford Brothers Data Breach illustrates the power of man-in-
the middle type attacks, and how external security is secondary to internal security.
While the data leaving the Hanford Brothers’ stores was encrypted, the locally exchanged
data was not. This allowed the perpetrators to collect the information for which they
were looking, without the hassle of finding keys or cracking any encryption (Clapper,
2010). This case also illustrated that the PCI DSS is of little use for protecting an
organization against malware attacks commonly utilized to compromise software based
POS systems at various merchant locations. It can be argued that the PCI DSS needs to
be revised to address these frequently exploited vulnerabilities, but the bigger lesson to be
learned from this particular case is that regardless of OS system and regardless of
whether individual terminals or central servers are compromised, malware presents the biggest threat to credit card confidentiality at the POS.

**Case Study-3: The Target Data Breach**

In November and December 2013, criminals managed to infiltrate Target’s internal network and install malware on its software based terminals, leading to the exposure and loss of data connected with nearly 110 million Target customers (United States Senate, 2014). Target is one of the largest retail companies in the US, and as reported by Riley et al. (2014), at least 40 million credit card details, in addition to other personal data, was stolen during the heist.

As explained by Krebs (2014a), the Target breach started out as a phishing and malware attack on one of Target’s vendors. It is unclear at this point whether the vendor was specifically selected or whether the email attack was rather random, and the hackers got lucky in a way with the information they were able to retrieve from the compromised vendor (United States Senate, 2014). However, once the perpetrators obtained login credentials to Target’s external billing system called Ariba, they continued to probe the environment until they were able to isolate a network computer using the name/domain `ttcopscli3acs` (Krebs, 2014b). The malware installed on the software terminals connected to the registers at target locations did then utilize this name/domain to locally dump and store credit card information for later collection (Krebs, 2014d).

On an almost daily basis, the perpetrators then collected batches of personal information from their local storage for export to an off-site international location through the use of port 80 communications (Rosenblum, 2014). Port 80 is commonly
used for hypertext transfer protocol (HTTP), or web browsing content, such as internet websites, and therefore, is often exempt or less monitored than ports usually not associated with legitimate use of Internet services (Bejtlich, 2004). Once the criminals were able to secure communication, infiltrate software terminals with malware, and solve the issue of local temporary storage to prevent suspicion about continuous data transfer, they were able to collect customer information on autopilot and past any firewalls or intrusion detection systems as illustrated in Figure 6. As Krebs (2014d) explains, the hackers used various malware to infiltrate and compromise the internal network on several levels, before extracting information to a drop site.

![Figure 6](image-url)  
*Figure 6. Attacker controlled assets. From New Clues in the target breach, B. Krebs, (2014d).*

Tuttle (2014) points out that Target’s IT was PCI DSS compliant and had passed an audit to that extent not long before the data breach was first noticed. As reported by Krebs (2014b), the target malware was not particularly sophisticated. Several intrusion detection alerts were issued while the hackers were trying to setup their base; however, all of which were subsequently ignored (United States Senate, 2014). As part of the case
COUNTERING MAN-IN-THE-MIDDLE ATTACKS

analysis presented by Krebs (2014d), and as illustrated in Chart 3, similar malware had been used previously to successfully breach security at other retailers. One might assume that associated vulnerabilities should have been addressed and fixed before the Target breach had occurred, effectively preventing the re-use of already known malware.


As with most other reported high profile malware related data breaches, Target was also operating its POS and most of its internal network on computers and servers running on a Microsoft OS (Bodhani, 2014). This is insofar relevant to this case, as it allowed the perpetrators to use readily available off-the-shelf malware, instead of having to engineer a custom solution, as was apparently necessary to compromise the Hannaford Brothers’ POS (Clapper, 2010).

**Summary.** The Target Data Breach illustrates again how internal security is as important, or even more so, than external security, when it comes to credit card and
customer data. It can no longer be assumed that internally connected systems can be trusted, just because they are on an isolated network without direct internet access. This case is exemplary in detailing how gateways can be created or repurposed, so that they function as offloading servers to an off-site location for internally connected data. Furthermore, relying on intrusion prevention and detection systems is still largely dependent on human action, and as explained by Bejtlich (2004), automatic systems rely on predefined pattern detection, and thus will never be effective against or able to prevent all attacks and intrusions. These systems only detect what they know or deviations from the norm, but if an attacker derives a novel way to bypass the expected pattern and conceal their actions so that they look normal, they become rather ineffective tools for securing a network against intruders.

**Literature Review Summary**

Credit card fraud is big business for criminals, banks, and merchants. The majority of fraudulent transactions today are the result of magnetic-strip credit card information theft. While other payment systems have been gradually introduced, such as the chip and PIN based EMV, acceptance is not yet universal, and may be limited to certain countries or merchants only. Even though EMV provides a greater level of security and protection against cloning or theft of account information, criminals have quickly adopted and found other vulnerabilities.

The three case studies evaluated as part of this study illustrate how encrypted communication between the merchant and the processor, as well as intrusion prevention and detection systems installed at merchant locations, are ineffective in the fight against
credit card theft. The weakest link, as shown in all three presented cases, is any communication, data access, or storage thereof without encryption at any given point. In order to prevent man-in-the-middle type attacks on existing and future payment systems, the way payment data is acquired, processed, stored, and shared has to be re-evaluated and adjusted, making RAM-scraping malware or traditional hacking attempts impossible to succeed.

**Methodology**

**Identification and Operationalization of Variables**

The study focused on identifying dependent variables with impact on overall security when processing credit card payments over Point of Sale (POS) terminals, for the purpose of influencing independent variables, those that reduce credit card fraud, and a merchant’s vulnerability to malware. Krebs (2014b) explains that random access memory (RAM) scraping malware is primarily to be blamed for the loss of up to 110 million credit card details during a security breach at Target in 2013. More recently, a similar malware was used to potentially extract even more credit card information from Home Depot stores (Krebs, 2014c).

In both cases, the malware was installed on credit card terminals and used to scrape RAM for credit card details, such as account numbers, expiration dates, and other information. While other systems have to be compromised as well in order to allow the perpetrators to export their collected data to a location from where it can be retrieved easily, the fact that data is unencrypted when captured, makes this hack a particularly valuable approach for any criminal (Tuttle, 2014).
The biggest influential factor on credit card security, and the loss of credit card data then is the fact that credit card information is stored without encryption on cards, but also without encryption, at least temporarily, when read for payment processing (Bodhani, 2014). This study therefore evaluated the influence of credit card information encryption, both at the card level and when extracted during payment authorization, for the purpose of identifying a potential reduction in credit card theft.

While most credit card terminals do not encrypt credit card information, in general, as it is extracted from the card, there have been indications that when the chip and PIN standard was introduced in Europe, credit card fraud initially dropped significantly (Anderson & Murdoch, 2014). Despite this early success, credit card fraud is on the rise again, thanks to the fact that most processors rely on old technology and most credit card terminals remain insecure (Greene, 2009). The variables examined in this study; therefore, included encryption technologies, terminal systems, as well as overall payment transaction processing, with a focus on how improvements can be used to reduce credit card theft, and in particular the possibility for terminals to fall victim to RAM scraping malware.

**The Target Credit Card Malware Security Breach**

The Target credit card malware hack is used as a case study because it is recent, much better documented than other cases, and despite the identification of vulnerabilities, most recently a similar approach has been used to hack terminals at Home Depot as well (Krebs, 2014c). The Target hack is in particular of interest, because Target was following industry standards for securing payment information, had a modern intrusion
detection and prevention system in place, and yet failed to contain the malware or prevent the successful heist altogether.

Target is therefore a prime example of vulnerabilities in credit card processing systems, and indicative of a best case scenario faced by many other merchants. While improvements are made continuously and new payment processing systems are introduced regularly, so far most of them have failed to reach critical mass or relied on old systems by only partially fixing some vulnerabilities (Clover, 2014). Even the latest near field communication (NFC) based payment systems are vulnerable to fraud (Wagstaff, 2012).

The Target security breach illustrates the larger issues at hand in regard to capturing and processing credit card information at POS terminals, and presents itself as an ideal candidate for an in depth examination. By analyzing the Target malware attack, this study was able to identify universally applicable vulnerabilities, and evaluate potential improvements for their ability to reduce credit card theft by preventing man-in-the-middle attacks at credit card terminals.

**Hypothesis**

Research shows, credit card theft is possible because of the lack of encryption of credit card data on the physical card, as well as when it is captured for payment processing (Savage, 2013). As a result, the following research questions were addressed:

- Which credit card terminals are vulnerable to man-in-the-middle type attacks?
- Which credit card terminals are susceptible to malware?
- How is credit information exchanged between merchants and banks?
How can credit card terminals and credit card transactions be secured?

The hypothesis is that if magnet strip or EMV readouts are encrypted through hardware before the data is submitted for processing, large scale credit card theft through malware infected terminals is prevented.

Technical Analysis and Data Sources

The study focused on the analysis of various documented large scale credit card theft cases, including the TJMAXX case, the Target malware, as well as the most recent Home Depot incident. In addition, the analysis examined generally documented vulnerabilities in credit card processing, as well as popular countermeasures recommended as industry standards, and those that are currently used by most organizations, to secure financial transactions at the POS.

Each countermeasure and incident is evaluated with a three level probability impact matrix for the purpose of identifying the most and least effective approaches for reducing credit card theft. While this study had to largely rely on secondary sources, there have been many well documented and different incidents, ensuring validity and reliability of the findings. Furthermore, using a probability impact matrix for both effects and countermeasures, allows to evaluate both cause and effect on a similar scale by assigning values, including likely, neutral, and unlikely, to all data points.

This approach illustrated the correlation between countermeasures and their impact on the likelihood of credit card data theft in general. As shown by the Target incident, perpetrators use multiple attack vectors and vulnerabilities to successfully carry out their heist (Krebs, 2014a). Therefore, each countermeasure needed to be evaluated
for how likely it would have been able to prevent the security breach altogether, assuming that other vulnerabilities still exist. As explained by Bodin et al. (2008), while systems can be secured against known vulnerabilities, it is the unknown that will likely allow an attacker to successfully carry out an attack.

Focusing on individual threats and vulnerabilities as a means to evaluating overall credit card processing system security is therefore unable to adequately address the root cause of the security weaknesses, as this approach only fixes issues related to the symptoms of a breach. The use of a probability impact matrix is aimed at identifying a single modification that will render credit card information useless, even if other vulnerabilities exist, and remain unfixed.

Limitations

This study examined processes and their vulnerabilities of terminals used for credit and debit card terminals at merchant locations within the United States. Findings and suggestions for improving credit card processing and associated security are universal, but may interfere with future processes that have not yet been introduced, such as the general introduction of EMV cards in the US for example. In addition, while newly introduced payment systems may not be vulnerable to the same exploits used with magnetic-stripped based transaction processing, they are largely based on standards that have been developed many years ago (Clover, 2014). Therefore, this study was exclusively aimed at examining known processes currently used for processing credit card payments. All findings may still apply to future payment systems, at least if these still rely partially on the evaluated methods and systems. Without explicit knowledge of how these future
systems operate, no default statement can be made as to how they might be affected by the findings of this study, and to what extent.

**Results**

A three-level-probability-impact matrix scale of likely, possibly, and unlikely is used to evaluate various approaches for identified vulnerabilities and their ability to stop, or prevent, a given data breach scenario. Likely means that by removing this vulnerability without additional intervention, a hack could not have succeeded. Unlikely means that even if this vulnerability can be addressed in the future, it will have no impact on the outcome of a potential hack. Possibly refers to the case where a vulnerability is dependent on other factors in order to prevent a breach, meaning that addressing this vulnerability alone will not secure a system and prevent similar attacks from happening.

**Analysis of the TJ Maxx Breach**

According to Berg et al. (2008), TJ Maxx was the victim of a data breach in 2007, which had given hackers access to customer credit card information for at least 18 months prior to when it was first discovered. During that time, the perpetrators were able to obtain at least 94 million Visa and Mastercard account details collected from various store locations across the United States (Berg et al., 2008). Despite the PCI DSS requirements for encrypting customer account information and the use of strong encryption for remote access, the perpetrators were able to compromise a weakly secured wireless network at one of the TJ Maxx store locations (Berg et al., 2008). Once they gained access to the local network, they were able to further infiltrate other systems until they successfully hacked their way into the corporate headquarters. The following
reconnaissance led the hackers to discover server hosted files, which contained copies of customer credit card account information, including all magnetic-strip data, expiration dates, card verification codes (CVC), PINs, and other personal identifiable data (Berg et al., 2008).

Table 4

*TJ Maxx Data Breach Vulnerability Impact Matrix*

<table>
<thead>
<tr>
<th>Vulnerability exploited during the Target data breach</th>
<th>Ability to stop the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure local WiFi access with strong encryption, Mac filters</td>
<td>possibly</td>
</tr>
<tr>
<td>Encrypt all locally stored credit account information</td>
<td>possibly</td>
</tr>
<tr>
<td>Prevent access to payment processing systems from external hosts</td>
<td>likely</td>
</tr>
<tr>
<td>Do not aggregate and store credit account information from branches</td>
<td>likely</td>
</tr>
<tr>
<td>Install intrusion prevention and detection systems</td>
<td>possibly</td>
</tr>
<tr>
<td>Prevent installation of RAM-scraping malware on terminals</td>
<td>likely</td>
</tr>
<tr>
<td>Encrypt all credit card information at any given time</td>
<td>likely</td>
</tr>
<tr>
<td>Use EMV-based cards exclusively</td>
<td>possibly</td>
</tr>
</tbody>
</table>

Unlike with other recently reported incidents, where credit card information was compromised, the perpetrators did not have to install malware on the cashier terminals in order to obtain customer credit account information, because TJ Maxx stored everything for which they were looking in server hosted files without any encryption (Berg et al., 2008). Once the initial intrusion was successful, this breach is unique because of two factors: the credit card information awaiting retrieval was already stored locally by the
organization, and the overall weak security of the external wireless as well as local and corporate networks.

Table 4 illustrates the impact of addressing various vulnerabilities on how likely they would have stopped or prevented the data breach, as it had occurred at TJ Maxx. It needs to be noted that because best practices for network security were not followed in this case, it cannot be assessed if another data breach would have happened regardless, even if some known vulnerabilities would have been addressed beforehand.

**Analysis of the Hannaford Brothers Breach**

The Hannaford Brothers data breach is unique in many ways, although hackers used a familiar approach successfully employed in other breaches. Hannaford Brothers operates a chain of nearly 300 grocery stores, most of them located on the east coast of the United States. In 2008 it was discovered that at least 4.2 million credit and debit card numbers were compromised, originating from a hack targeting credit card terminals at Hannaford Brothers grocery store locations (Clapper, 2010). Somehow perpetrators had managed to install RAM-scraping malware at all Hannaford Brothers locations, allowing them to create locally stored backup files of all payment information exchanged between the store and the merchant’s card processor (Clapper, 2010). The local files were then regularly offloaded to servers located overseas from where the perpetrators could retrieve them safely without creating further suspicion.

Clapper (2010) explains that the Hannaford Brothers data breach is unique for several reasons. The terminals used at the Hannaford Brothers were upgraded and based on the Linux OS prior to the incident. Instead of using RAM-scraping malware on each
terminal, the hackers took advantage of the fact that each local terminal sends payment data to a local server, thus aggregating all credit information at a single location. A custom written software was used to compromise these local payment processing servers, therefore collecting all credit card information in one location without the need to infiltrate multiple systems. According to Clapper (2010), no publicly released information is available as to how the perpetrators were able to infiltrate the payment servers at all Hannaford Brothers locations, or whether encryption was used between local terminals and the local payment server.

What is known, is that this breach resulted in the loss of Track 2 data from the magnetic-strip on each card that was swiped at a cashier’s terminal during the heist (Clapper, 2010). While Track 2 data does not allow a perpetrator to duplicate a credit card, it contains both the primary account number (PAN), and the expiration date, which is sufficient information to carry out many types of fraudulent transactions (Clapper, 2010). With many unanswered questions about why perpetrators chose to infiltrate the central servers rather than individual terminals, how they managed to compromise all Hannaford Brothers’ locations, and why no intrusion was detected or prevented, potential vulnerabilities are far from just a few.

Table 5 lists the vulnerabilities that might have been exploited during the Hannaford Brothers data breach, and the impact of a potential fix on the overall success of the hackers in their attempt to extract customer credit card information.
Table 5

*Hanaford Borthers Data Breach Vulnerability Impact Matrix*

<table>
<thead>
<tr>
<th>Vulnerability exploited during the Target data breach</th>
<th>Ability to stop the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use anti-malware software to prevent infiltration of servers</td>
<td>possibly</td>
</tr>
<tr>
<td>Encrypt all locally stored credit account information</td>
<td>possibly</td>
</tr>
<tr>
<td>Encrypt credit card data at the terminal</td>
<td>likely</td>
</tr>
<tr>
<td>Only exchange encrypted credit card information internally</td>
<td>likely</td>
</tr>
<tr>
<td>Install intrusion prevention and detection systems</td>
<td>possibly</td>
</tr>
<tr>
<td>Secure company networks and prevent external access</td>
<td>possibly</td>
</tr>
<tr>
<td>Encrypt all credit card information at any given time</td>
<td>likely</td>
</tr>
<tr>
<td>Use EMV-based cards exclusively</td>
<td>possibly</td>
</tr>
</tbody>
</table>

**Analysis of the Target Breach**

According to a United States Senate (2014) report on the Target data breach in 2013, attackers compromised Target’s intrusion prevention systems on many levels. Initially, the perpetrators sent malicious emails to various vendors in order to gain access to Target’s supplier portal. This crucial first step in compromising Target’s IT was only possible because at least one vendor was not using realtime malware protection (United States Senate, 2014). Once passwords to Target’s systems were extracted, the perpetrators were able to access the vendor portal and other more sensitive systems from thereon (Krebs, 2014a). The United States Senate (2014) report claims that simple two-
factor authentication, as required by the PCI DSS for accessing payment processing systems remotely, could have prevented further intrusion.

Two-factor authentication relies on two forms of authentication with one most often being a password, and another a generated one-time code or biometric identifier such as a fingerprint, for example (Schou & Shoemaker, 2007). The United States Senate (2014) report; however, failed to mention that two-factor authentication would have only prevented access from a third party, but not access with the help of malware running on a system used to authenticate with proper credentials. In this case, the malware would piggyback and execute commands in addition, or modify existing commands with the help of the infected system, in a man-in-the-middle type attack, achieving likely similar results (Mitropoulos et al., 2011).

Once Target’s systems were compromised, the attackers installed RAM-scraping malware on Target’s terminals, as well as exfiltration software, allowing them to collect credit card information and then extract those recordings in regular intervals (United States Senate, 2014). It needs to be noted that both Target’s intrusion prevention and intrusion detection systems failed to contain, or prevent, this breach (Krebs, 2014d). Although the report by the United States Senate (2014) confirms that the FireEye software used to detect intrusions on Target’s network managed to identify unusual traffic, the analysts in charge of acting on these automatically generated alerts failed to address the issue.
Table 6

**Target Data Breach Vulnerability Impact Matrix**

<table>
<thead>
<tr>
<th>Vulnerability exploited during the Target data breach</th>
<th>Ability to stop the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Target’s systems by malware infected Vendors</td>
<td>possibly</td>
</tr>
<tr>
<td>Implement 2-factor authentication when accessing Target’s systems</td>
<td>possibly</td>
</tr>
<tr>
<td>Prevent internal access from less secure systems to more secure systems within Target’s network</td>
<td>likely</td>
</tr>
<tr>
<td>Prevent outgoing network traffic necessary for exfiltration</td>
<td>possibly</td>
</tr>
<tr>
<td>Act on intrusion prevention and detection alerts</td>
<td>possibly</td>
</tr>
<tr>
<td>Prevent installation of RAM-scraping malware on terminals</td>
<td>likely</td>
</tr>
<tr>
<td>Encrypt all credit card information at any given time</td>
<td>likely</td>
</tr>
<tr>
<td>Use EMV-based cards exclusively</td>
<td>possibly</td>
</tr>
</tbody>
</table>

At first look it might seem that in the case of the Target data breach the perpetrators got lucky, because various systems were not fully secured, or working in the designed manner. It needs to be acknowledged however, that even in a best case scenario, relying on intrusion prevention and detection systems puts an organization at risk and significant disadvantage against criminals (United States Senate, 2014).

Intrusion prevention systems are always one step behind adversaries, as they rely on pattern recognition based on known approaches and vulnerabilities (Bejtlich, 2004). Table 6 illustrates a possible fix for each major vulnerability used during the Target data breach, and its ability to stop the criminals in their tracks or prevent them from causing damage.
Effectiveness of Common Countermeasures

Bejtlich (2004) explains that common countermeasures used to prevent hacking include intrusion detection and prevention systems, firewalls, authentication and authorization, encryption, logging, and physical security. The cases examined in this study all employed a combination of several of these countermeasures, and although this might suggest greater protection against malicious attacks, ultimately they all failed to be an effective defense.

Traynor et al. (2007) state that intrusion detection systems notify administrators if an event occurs that matches a predefined pattern, which are also known as signatures. These signatures may include activity on various ports, amount of data sent, unusual traffic, and other recognizable behavior, but always require to be defined in the first place (Traynor et al., 2007). Commonly used intrusion detection systems are antivirus and antimalware tools, which scan a host and look for known signatures of viruses, and other malware. Intrusion detection systems; therefore, are only as effective as the defined signatures for which they look or the administrators that act on automatically generated intrusion notifications (Schou & Shoemaker, 2007).

To address this problem, intrusion prevention systems were developed. Intrusion prevention usually works in combination with intrusion detection, but instead of looking for pattern to create alarms, prevention aims to distract potential intruders, often with a technique called honeypot (Bejtlich, 2004). A honeypot leads an intruder on a wrong path of no value, thus preventing them from finding confidential information. This
distraction gives administrators time to identify the breach and act on it before the hacker was able to steal valuable information.

The purpose of firewalls is to actively prevent intrusion by limiting access to networks protected by a firewall (Bejtlich, 2004). A firewall is used to block all unwanted traffic, and ideally prevents the use of ports or tools that would allow unauthorized extraction of data. These firewalls often work in conjunction with authentication and authorization systems, ensuring that only authorized users have access to secured networks and terminals.

Physical security is concerned with preventing access to networks or terminals by locking appliances away from public access (Schou & Shoemaker, 2007). Measures to physically secure assets involve locked doors, fences, and security guards, for example. Physical security is concerned with access control that would involve physical interaction with individuals or technology, and thus can be considered a preventative measure.

While encryption does not prevent intrusion, its primary intention is to prevent a third party from gaining useful intel in case of unauthorized access (Comer, 2009). A perpetrator may successfully gain access to a secure network, but the data they may obtain is useless unless it can be decrypted or was not encrypted in the first place. Encryption can therefore serve a dual purpose as deterrent and last line of defense.

Logging is not concerned with deterring or defending adversaries, but rather with documenting intrusions and data exchange for the purpose of learning from mistakes and prosecution. Logging is essential for training intrusion detection systems, as evaluating
access and transfer logs allows an administrator to identify patterns for future recognition of similar intrusion attempts.

Each of the discussed countermeasures addresses a certain problem, suggesting that combining many of those approaches in a security policy will prevent intrusions and loss of confidential data. As the three discussed case studies illustrate, in reality, this is not the case. None of the commonly used countermeasures are able to prevent network intrusions, whether they are used alone or in combination with other tools. Both intrusion detection and intrusion prevention systems have been circumvented by hackers, and authentication or authorization often falls victim to fishing scams, exposing entire networks to criminals (Krebs, 2014a).

Physical security has been circumvented in the case of the TJ Maxx breach, where hackers used local wireless networks at a store location to gain access to corporate headquarters (Berg et al., 2008); encryption either failed or was otherwise circumvented in the Hannaford Brothers data breach (Clapper, 2010). All three cases supposedly used firewalls, intrusion detection and prevention systems, as well as access control to some extent. In no case did those countermeasures prevent the perpetrators from gaining control over various systems, and extract confidential credit card account numbers.

Furthermore, in the case of the Hannaford Brothers and the Target data breach, the criminals successfully used man-in-the-middle type attacks to eavesdrop on credit card transactions, rendering any of the discussed countermeasures ineffective. This indicates that these commonly used approaches for defending and securing networks are ineffective in deterring criminals or preventing data breaches. Most recently Home
Depot was the victim of a breach very similar to the one executed on Target, further suggesting that none of the current approaches is efficient enough in preventing these, or similar, heists (Krebs, 2014c).

**Effectiveness of Alternative Countermeasures**

As explained by Peltier et al. (2005), strong encryption while in transit, as well as when stored, is one of the recommended best business practices for securing confidential data. Encryption makes it difficult for an adversary to make use of any data they may obtain, unless they have access to keys, or are otherwise able to break the cipher used to encrypt the information (Jones, 2002). There is no indication in any of the three cases examined in this study that hackers were forced to break encryption. If any encryption was indeed used, the criminals were either able to get the key to decrypt data, or access information through a man-in-the-middle type attack, and in a state where it was not encrypted.

The fact that the perpetrators were able to gain access to secured networks suggests two-factor authentication was not used. Two-factor authentication adds additional authentication to passwords in order to access networks through the use of smart cards, magnetic-strip cards, hardware or software tokens, fingerprints, retina patterns, hand geometry, or palm prints, for example (Peltier et al., 2005). The initial breach at Target for example, where perpetrators used phishing to obtain login credentials from a vendor would not have been possible, if two-factor authentication was used (United States Senate, 2014). Similarly, the breach at TJ Maxx would most likely have been avoided as well, although the same cannot be said for the Hannaford Brothers
incident, because information on how the hackers were initially able to compromise the internal network has not been released (Clapper, 2010).

Additionally, if two-factor authentication is only used for accessing corporate networks remotely, perpetrators may still be able to infiltrate systems, if weak wireless security for example allows a perpetrator to become part of a local network, as it has happened during the TJ Maxx incident (Berg et al., 2008). This suggests that rigorous enforcement of two-factor authentication for any and all access control can be an effective deterrent and protect local networks from unauthorized access. However, should a perpetrator gain access regardless, only strong encryption of all data at any given time will be able to stop an intrusion or prevent confidential data from being stolen.

The cost associated with breaking through two-factor authentication, as well as decrypting data is likely too high for most adversaries other than government and nation-state sponsored hackers with access to tremendous resources (Jones, 2002). An additional layer of security can be provided by using some sort of contextual firewalls and database access (Mitropoulos et al., 2011). Hardware based signatures can be used in firewalls to prevent code execution other than the one that has been authorized. Furthermore, this approach also allows an organization to prevent data extraction because firewalls can be trained to accept traffic only from specific hosts, but also only to specific hosts in the context of an expected transaction (Mitropoulos et al., 2011).

For example, a host tasked with processing credit card transactions will only be able to communicate with the merchant’s bank, only one or more specific servers, and only transaction related data, as defined by a framework. Additional security can be
provided by implementing transaction signatures in addition to encryption for systems that need to be able to communicate with a wider variety of servers (Bisht, Madhusudan, & Venkatakrishnan, 2010). A hacker would then have to work around the firewall restricting the outgoing traffic based on origin and destination, the content of the data packets, a unique application specific signature, then possibly decrypt the data stream; if they were successful in intercepting any communication between the merchant and their bank.

Forcing encryption on any and all data being accessed, in transit, acquired, or during processing, can be an effective deterrent and protection against hacks similar to those examined in this study. Furthermore, using two-factor authentication for any access, as well as context aware firewalls and application specific signatures, will make it less likely for hackers to be able to extract any data they might be able to find or would want to collect for further examination. While two-factor authentication and encryption are both recommended as a best business practice for securing networks, content aware and signature based firewalls are not yet used for most applications (Bodin et al., 2008). It needs to be noted that many recommendations on how to use encryption and two-factor authentication in corporate networks are limited to remote access and data exchange, or storage (Peltier et al., 2005). In order for these two countermeasures to be effective in the fight against data breaches, they need to be implemented for any access to a corporate network, and encryption needs to be used for any interaction with data throughout the entire process.
Discussion

As criminals adjust their approaches in order to steal large numbers of credit cards, Credit Card fraud has become a serious issue that severely threatens traditional commerce and affects profit margins (Riley et al., 2014). Hacks exposing millions of credit card account details have become common, and despite more secure corporate networks, criminals seem to find ways to use the same exploits over and over again, as evidenced by the latest hack at Home Depot (Krebs, 2014c). While some experts believe that the problem can be controlled by switching from magnetic-strip based credit cards to those utilizing EMV, the statistics available from select markets, where chip and PIN are more common, suggest otherwise (Anderson & Murdoch, 2014).

As illustrated by the three discussed cases, the Hannaford Brothers, the Target, and the TJ Maxx breach, the criminals were able to obtain credit card information because they were able to join a non-public corporate network, and the data they stole was not encrypted. As was evident in all cases, security measures such as intrusion detection, intrusion prevention, firewalls, closed networks and authentication were all useless in preventing the hackers from finishing their heist. Furthermore, the simple existence of these countermeasures did not deter the intruders, and possibly only served to slow down the hacks temporarily.

Although the PCI DSS requires the use of all of these countermeasures for payment processing systems, the actual reported cases suggest that they are ineffective tools for securing networks, and preventing hackers from stealing credit card information. As shown earlier in the results section of this study, only two-factor authentication and
encryption at any given time offers the potential to prevent criminals from executing similar heists in the future. While magnetic-strip based terminals can be compromised, for example by adding a card skimmer on top, which requires physical access to all terminals, it is unlikely that criminals will be able to accomplish such a task on hundreds or even thousands of locations, especially when in public and under supervision (Bhatla et al., 2003).

Instead of closing these vulnerabilities and preventing them from being exploited, the payment processing industry has relied on a patchwork consisting mostly of detection and deception, rather than addressing the core issues (Tuttle, 2014). For example, many card issuers use neural networks and artificial intelligence software to analyze purchase pattern and spot abnormal transactions (Bhatla et al., 2003). This approach has been proven successful in detecting fraudulent transactions; however, it addresses the issue of using stolen credit card numbers and not the actual theft in the first place.

In order to address the inherent insecurity of magnetic-strip based credit cards, the card issuers have developed new systems, such as EMV and NFC. While both are far more secure than magnetic-strip cards, they have built-in vulnerabilities, which are already exploited on a larger scale (Anderson & Murdoch, 2014). For example, Apple Pay, a solution where NFC is used to transfer a token between a cell phone and a merchant’s terminal instead of a credit or debit card account number, is based in principle on the same technology that has been around for several years and has already been shown to be vulnerable to various attacks (Clover, 2014). Although Brandon (2014) suggests that Apple Pay may not be susceptible to the same vulnerabilities as regular
NFC payments, the fact that it is based on known industry standards suggests otherwise. In particular, Apple Pay, which is functional similar to google wallet, uses a technique where tokens are used to authorize payments; however, both the token generating algorithms, as well as payment details have already been hacked in the past, in what is known as a relay attack (Heydt-Benjamin et al., 2009).

Additionally, Apple Pay information is validated on the local network level, as well as with the merchant’s payment processor for authorizing payments, thus suggesting the need for decryption by both the merchant, as well as the bank (Brandon, 2014). If hackers get access and infiltrate this communication chain, what keeps them from modifying payment terms, or generating additional tokens as is now common with various EMV-based cards in the U.K. (Tuttle, 2014)?

This observation suggests that even with systems like EMV, or Apple Pay for example, the payment processing systems used during the transaction remain vulnerable to attacks for the foreseeable future. Clearly, these newer systems offer significant advantages over magnetic-strip cards, but it will be only a matter of time, until criminals adopt their approach and focus on different exploits instead. Regardless of the inefficiency of these systems to fully protect electronic payment transactions, the White House (2014) has just released an executive order signed by the President of the United States of America, to further accelerate the use and installation of EMV capable cards and terminals as quickly as possible.

As mentioned, EMV cards will prevent hackers from collecting bulk credit card numbers, but it will not prevent them from hacking tokens, or executing relay attacks in
the future. In this context, this study was aimed at answering the following research questions:

- Which credit card terminals are vulnerable to man-in-the-middle type attacks?
- Which credit card terminals are susceptible to malware?
- How is credit information exchanged between merchants and banks?
- How can credit card terminals and credit card transactions be secured?

In that regard, and as shown both by the Target and Hannaford Brothers breaches, all credit card terminals are susceptible to man-in-the-middle type attacks. Especially software based terminals are susceptible to malware, because they often run as part of other POS software on a rather insecure OS. Although not particularly discussed as part of the three case studies, especially in the U.K. hackers were able to infiltrate stand-alone terminals as well, and it cannot be ruled out that those are similarly vulnerable to malware (Tuttle, 2014).

Regardless of whether an EMV or magnetic-strip card is used to initiate a transaction, payment information is always exchanged with a merchant first, then with the merchant’s processor and a bank. This approach exposes several potential entry points where a perpetrator can execute a man-in-the-middle type attack by either building a relay or capturing transaction data, as seen in the case of the Hannaford Brothers data breach (Clapper, 2010). Therefore, credit card terminals and transactions can only be secured, if encryption between the source and destination is guaranteed. Allowing parts of the transaction to be verified or decrypted during the transaction at various points will provide a possible attack vector for criminals to inject or extract code.
In addition, the hypothesis that large scale credit card theft through malware infected terminals is prevented, if magnetic-strip or EMV readouts are encrypted through hardware before the data is submitted for processing cannot be confirmed. Even newer systems, such as Apple Pay for example, allow partial decryption or token verification while the transaction data is in transit between the customer and the authorizing bank, thus opening the door for relay or other man-in-the-middle type attacks.

**Summary**

The study has illustrated that all credit card transactions are vulnerable to man-in-the-middle type attacks, because all currently used processes allow attackers to inject or extract transaction related information at some point during the communication. In addition, some merchants do not follow best practices for securing their networks against intruders, further exposing them to additional exploits. Best practices include two-factor authentication for remote access, as well as strong encryption (Peltier et al., 2005). Commonly used countermeasures, such as intrusion prevention and detection systems, for example, have little impact on preventing sophisticated heists, and thus provide a false sense of security to administrators and IT professionals.

Although two-factor authentication could likely have avoided all of the three cases examined in this study, other vulnerabilities still exists. These include partial encryption of transaction data, as well as, a lack of non-repudiation during credit card transaction processing, thus making relay attacks possible. The incidents at Target, the Hannaford Brothers, and TJ Maxx illustrate how criminals were able to obtain a large
number of credit account information through three different approaches, suggesting that
the overall system for processing credit card payments is flawed in general.

**Conclusion**

In conclusion, this study sought to identify one or more approaches for securing
credit card terminals, and preventing man-in-the-middle type attacks in the future. While
both two-factor authentication for any login and persistent and permanent encryption of
all transaction related data was identified to offer significant improvements in restricting
unauthorized network access, inherent vulnerabilities present in current payment
processing systems make it nearly impossible to provide consistent protection. While
tokenization is a step in the right direction, both the creation of tokens, as well as
compromising transaction details have been proven to be effective targets for criminals to
continue with fraudulent transactions (Tuttle, 2014).

As it stands, only a system that completely encrypts transaction related data, and
then ensures that data will only be exchanged directly between the customer and the
bank, would provide far greater security for these transactions than possible today, even
with encryption of existing systems, and two-factor authentication for network access.
Putting a better lock on the front door helps little, if all windows are wide open.

**Recommendations**

This study makes two major recommendations. In order to provide the best
possible security for payment transactions while retaining compatibility with current
systems in the market, credit card readers, whether attached to software terminals, or
operated as stand-alone units, need to encrypt data in hardware with the help of a
dedicated chip, and no software access from the outside. Square Inc. (2014) already uses this approach in their cellphone connected card readers, thus ensuring that any data that is sent to the software terminal on the mobile device is already encrypted. The software terminal itself does not have access to transaction related account information, which is only available to the payment processor. Thus, a man-in-the-middle type attack would be unsuccessful, unless the perpetrator is also able to get hold of the keys used for encryption and decryption of the data stream. Using such an approach, and making it mandatory for all terminals used to process credit cards, would make it next to impossible for any attempt similar to the examined cases within this study to succeed in the future.

In addition, instead of processing transactions through the merchant, meaning that the merchant is acting as a mediator during the transaction, a simple modification of the process would significantly secure the transaction, and prevent relay attacks, as well as man-in-the-middle type attacks in the future. When a merchant wants to charge a customer for goods and services, he notifies the processor about the transaction total. In return, the processor issues an encrypted token only to be decrypted by the card-reading terminal. The merchant’s POS forwards the transaction total, as well processor’s unique to the card reader, which then displays both transaction details to the customer, if they match. The customer can be sure that they will only be charged for what has already been requested by the merchant.

During the following step, the terminal will read the customer’s card and issue an encrypted token unique to both the card and the terminal. The merchant then forwards the token to the processor for final approval. This approach has several advantages over
the current system in that the merchant never gets hold of any decrypted account information, and because the merchant does not actually create the charge request for the terminal directly, man-in-the-middle type relay attacks can be avoided. The token issued by the processor will reflect the total charge, and no other charge can be requested during this pre-authorized transaction. A different amount would require a different token, which then again would be unique to both the merchant, as well as coming back from the terminal. With this approach, a perpetrator would have to infiltrate the credit card terminal, the merchant’s POS system, and the merchant’s processor, making this a very unlikely event due the complexity involved.

While the latter recommendation would require a change in how payments are processed, existing cards based on EMV, or even magnet strips could still be used for this new approach without requiring issuers to replace their cards. POS systems would need to be updated, but this change is transparent to the merchant’s employees, as well as the customers using their cards. The added benefit; however, is that in the case of a data breach, criminals will be unable to directly obtain any useful data, as no useful data is stored or decrypted at the merchant’s location. Furthermore, man-in-the-middle type attacks are successfully prevented because keys used for encryption at terminals will be unique. Even if hackers are able to obtain the key to one terminal, they will be unlikely able to do so for another, thus limiting their ability to compromise a secure system. This approach combined with two-factor authentication for secure network access will make heists with millions of stolen credit card account numbers extremely unlikely.
Further investigation into how payment processors could integrate this approach into their legacy systems and encourage existing merchants to switch is warranted. Without making a change to the transaction process itself, existing credit card systems cannot be fully secured.
References


probably-wouldnt-work-with-apple-pay.html#tk.rss_all?utm_medium=referral&utm_source=pulsenews


Only the beginning? (2014). *Quality Progress, 47*(2), 10-12.


Date ___________________________

I (we) _______________________________________________________________
owner(s) of the copyright to the work known as ______________________________

______________________________________________ _______________________

hereby authorize _______________________________________________________ to
use the following material as part of his/her thesis to be submitted to American Public
University System.

Page        Line Numbers or Other Identification

________________________________________

Signature
School of Science, Technology, Engineering, and Math
MS in Information Technology

The thesis for the master’s degree submitted by

Alex Munoz

under the title

Countering Man-In-The-Middle Attacks in Point of Sale Credit Card Terminals

has been read by the undersigned. It is hereby recommended for acceptance by the faculty

with credit to the amount of 3 semester hours.

(Signed, first reader) _Dr. Beverly JN Bowen___ (Date) __11/30/14____

(Signed, second reader, if required) _______________________ (Date) ______________

Recommend for approval on behalf of the program

(Signed) ______________________________ (Date) _______________

Recommendation accepted on behalf of the program director

(Signed) ______________________________ (Date) _______________

Approved by academic dean
This capstone has been approved by Dr. Beverly JN Bowen, PhD for submission, review, and publication by the Online Library.

Author’s name: Alex Munoz

Title: Countering Man-In-The-Middle Attacks in Point of Sale Credit Card Terminals

Professor: Dr. Beverly JN Bowen, PhD

Second reader, if required:

Program: Master’s of Science in Information Technology with a concentration in Information Assurance and Security

Pass with Distinction:  X  YES

Keywords/Descriptive Terms: credit card, identity theft, data breach, Target, Hannaford Brothers, TJ Maxx, Apple Pay, man-in-the-middle attack, electronic payments

[ ] Contains Security-Sensitive Information