

14NH - HH04 - 45

PREVENTING ONLINE CREDIT CARD THEFT IN TRANSIT

An Interactive Qualifying Project Report
submitted to the Faculty of
Worcester Polytechnic Institute
in partial fulfillment of the requirements for the
Degree of Bachelor of Science

Report Submitted to:

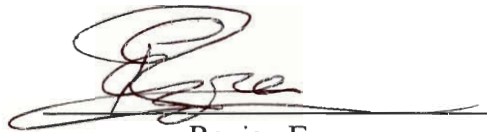
Project Advisor: Huong Higgins, Ph.D, WPI Professor



Submitted by:



Daniel Brauer



Ranjan Ezra

30 April 2003

Abstract

The goal of this project was to identify the risks of online credit card theft during transit. This included a thorough investigation of methods used by criminals to steal information online, and the technologies that have been developed to prevent such theft. The project team found that while there is a risk of theft, this risk can be diminished. This report recommends certain steps that consumer and retailers should follow in order to minimize the risk involved with online transactions.

Acknowledgements

We would like to thank the following people for their help and support throughout the duration of this project:

Huong Higgins
Rahul Bhan
Christine Nolan
Michael Demetriou
Stephen Bitar
Our Parents

Without these people, this project would never have come to such a successful conclusion.

Authorship

The authorship of all sections of this report was divided equally among the project group members: Daniel Brauer and Ranjan Ezra.

Table of Contents

| | |
|---|-----------|
| Abstract..... | 2 |
| Acknowledgements..... | 3 |
| Authorship Page..... | 4 |
| Table of Contents..... | 5 |
| Table of Figures..... | 6 |
| Chapter I: Introduction..... | 7 |
| Chapter II: Background..... | 11 |
| Risk Analysis..... | 11 |
| Cracking Methods..... | 11 |
| Antivirus Software..... | 13 |
| Encryption..... | 17 |
| Credit Card Technology..... | 25 |
| Chapter III: Procedure..... | 30 |
| Chapter IV: Results..... | 35 |
| Chapter V Analysis of Results..... | 38 |
| Chapter VI: Conclusions and Recommendations..... | 40 |
| Bibliography..... | 42 |
| Appendices..... | 47 |
| Appendix A: XML Details..... | 47 |
| Appendix B: Project Gantt Chart..... | 49 |
| Appendix C: Sample of Website SSL Providers..... | 51 |

Table of Figures

| | |
|---------------------------------|----|
| Figure 1-Postion of SSL..... | 20 |
| Figure 2- Layer SSL..... | 20 |
| Figure 3- Verified by Visa..... | 26 |

Chapter I: Introduction

Since its inception, the internet has grown into a vast arena of information. Now more than ever both retailers and consumers use the internet to conduct business. With the added convenience the internet brings, it also creates risks to all of the parties involved in the transaction. Once an internet user submits personal information such as names, addresses, phone numbers, bank account information, and even social security numbers on the internet, the user has very little control of what happens to that information. For this Interactive Qualifying Project, the project team researched what happens to this information, and examined the risks involved in online transactions. Specifically, the project team studied the risks of online credit card theft while the data is in transit, and the steps both consumers and retailers can follow to prevent it.

The project's goals are to identify the risks of online credit card theft during transit, and to suggest methods to help consumers and retailers prevent it. To achieve this goal, the team set a group of smaller goals. The first of which was to analyze the current risks involved with online credit card transactions. This included setting objectives to find figures for the percentage of online transactions that are fraudulent. The team's next goal was to research methods used by criminals to steal credit card numbers on the internet. This was done so the team could better understand how credit card numbers are stolen, and to identify areas of the transaction that may be more or less susceptible to risk. Once the team had established a risk involved with online transactions, the next goal was to reveal the current state of security technologies available to prevent credit card theft while the data is in transit. The team also set a goal to research new and forthcoming technologies that will be used for credit card theft prevention. By doing this the team

will better understand what consumers and retailers currently can do to stop online criminals, and also what they may be able to do in the near future. Finally, once the team had reached the above goals, it could then accomplish the goal of making recommendations to both consumers and retailers about the risks associated with online credit card theft. These recommendations are to be clear and concise so that normal computer users can understand and follow them without being internet security experts.

The purpose of this project is to inform both consumers and retailers of the current risks of credit card theft online, and the technologies available to prevent it. Currently many internet users are making online purchases while not being aware of the risks involved, and not taking proper action to secure themselves. Many others are avoiding making online purchases because of fears for their personal security. The team hopes to help both of these groups of people by informing them of what the actual risks are, and letting them know what they can do to minimize those risks.

In order to be a suitable Interactive Qualifying Project, the project must meet the objectives set by the Zwiebel Committee. This project creates awareness of socially related technological interactions by revealing the aspects involved with online credit card transactions, and the inherent risks involved. The project also identifies socio-technological systems and their subsystems. The systems involved with the project include the internet, credit card use, as well as e-commerce and e-security. Subsystems include security technologies such as from “smart” credit cards and encryption keys, policies that can be enacted to minimize online theft, and the trends of internet use. The project also cultivates a habit of questioning social values and structures by encouraging consumers and retailers to question online security. If internet users continue to do this,

technologies will continue to advance and evolve according to new threats as they arrive. This is an important aspect of the project, because if society fails to continue questioning online security, it will inevitably lose the battle with internet criminals. Lastly, the project encourages the recommendation of policy for consumers and retailers to follow to help ensure secure online credit card transfers.

The project's target audience is both consumers and retailers that currently or will conduct online transactions. More specifically, the project targets consumers who have or have considered making purchases online. These consumers will likely have a credit card, and may or may not use the credit card for online purchasing. The project is also targeted at retailers that currently or will offer sales using online credit card transfers. Both of these groups of people will be able to utilize the project's results by examining and following the given recommendations. The audience also includes people who have a general interest in the internet, e-commerce, or e-security.

The project's results will be presented in easy to follow guides for consumers and retailers to allow them to understand the risks to credit card transactions, and the methods available to diminish those risks.

Chapter II of this report, Background, covers all of the different aspects of the project that the team researched. It includes data on the risks involved with credit card transactions online, including figures for the rate at which credit card numbers are stolen. It also includes information describing methods used by criminals to steal credit card data while it is in transit. In addition, this section details many different security technologies available to help prevent online credit card theft, including SSL, SET, XML, and anti-

virus software. This chapter supplies technical background to help fully explain the results and conclusions of the project.

Chapter III, Procedure, details the steps the project team took to complete the project. It describes the methodology used by the group to reach its conclusions. This chapter explains what research procedures were employed, and why. It clearly lists major tasks, along with their sub-tasks, and the methods used to achieve the project's goals. In addition, it lists the sources used to gather information for the project, including indexes, websites, and correspondence.

The following three chapters, Results, Analysis of Results, and Conclusions and Recommendations, lay out the project team's findings. Chapter IV, Results, summarizes the groups results found in Chapter II. It clearly shows the findings of online credit card theft rates, methods used by thieves, and technologies and policies available to prevent theft during transit. The analysis of these results is shown in Chapter V. Here the team evaluates the actual risk involved with online credit card transactions, and the factors that can affect this risk. The team also connects security technologies and policies to direct threats by methods used by criminals. Finally, in Chapter VI, Conclusions and Recommendations, the project team combines the analysis with the project goals to draw conclusions about the state of online credit card theft. The project team also makes a series of recommendations for both retailers and consumers to follow to help eliminate the threat of online credit card theft while the data is in transit. There is a list of simple recommendations that all retailers and consumers should be able to follow to help reduce their risk. Lastly, the team suggests further studies in areas of internet security to ensure safe internet use.

Chapter II: Background

Risk Analysis

The internet is quickly becoming a popular place to conduct business transactions. According to International Data Corp., worldwide online retail sales are expected to grow from \$112 billion in 2001 to \$807 billion in 2006.¹ Credit card transactions account for nearly 90% of those sales. With such a large amount of money being transferred, the internet has quickly become a hotbed of criminal activity.

While there are relatively few cases of online credit card theft while the data is in transit,² there is still a risk. According to the Australian National Office for the Information Economy (NOIE), MasterCard has reported online fraud rates of 0.08%, while Visa reported similar figures.³ This rate can vary widely, however, depending on both the consumer and retailer involved in the transaction. If both are exercising caution when conducting the transaction, the rates can significantly decrease. Inversely, if either the retailer or the consumer neglects using all of the security features available to them, the threat of theft can increase dramatically.

Cracking Methods

Crime is something that cannot be escaped. The internet was once thought of as a free place, but is now being attacked by crime. These cyber criminals are called crackers (not Hackers). Hackers are individuals who alter their own computer, while crackers are individuals who cause malicious acts. These crackers invade people's privacy and steal

¹ Davis 2002

² <https://sisonline.unlv.edu/Share/Docs/Secured.html>

³ http://noie.gov.au/projects/consumer/shopping_online/index.htm

private information such as credit card numbers, social security numbers, and even identities. There are various ways crackers can steal this kind information. They can plant viruses into you computer, or they can directly attached a device to your internet.

Many of the viruses that crackers use are known as Trojans. Trojans are programs that run in the background of a user's computer without that person's knowledge. These viruses give crackers unauthorized access to individual's computers. The most common type of Trojan is a Remote Administration Trojans (RAT). This type of Trojan is popular because they let crackers have access to their victim's hard drive. Once the cracker has access to the hard drive, they can perform many functions on that computer such as open and close the CD-ROM drive or view the desktop and perform key logging. If the cracker has someone's IP address and has planted this virus on the victim's computer, the cracker can have full control over the victim's computer. Trojans can be bound to regular programs, so if a user runs that program the computer will become infected.⁴

One of the most valuable functions of a Trojan is the upload/download function, which can allow the cracker to view the keyboard presses of the computer user. For instance, if a user decides to buy a product on a website and enter their credit card number, the cracker can monitor the key presses and obtain the credit card number and any other vital information needed.

Apart from viruses, a cracker can attach a device to a person's computer so that they can directly access that computer without use of software on that computer. If a cracker wanted to get into someone's home system, they would have to know the type of

⁴ <http://princeigor.narod.ru/english/art8.html>

system being used as well as what firewall, if present. Then the cracker can find weak spots to attack and monitor the victim's every move. This type of attack is usually done more on a personal basis. The cracker must know a lot about the computer system he/she is trying to get into. For instance if someone was to crack into a bank, he may need the assistance of someone working in the bank, or someone else who may know the system and the components that they are using.

Crackers are individuals that looking into every little of software coding to find a flaw that they can exploit. They well spend hours, days, or even months trying to figure out how to break into a system. They generally don't have to have a computer science degree. Crackers can be anyone who is interested enough or determined enough to go above the law to get something done. Some of them even feel like they have a right to do what they do. Anyone can go on to the internet to find websites that give "hacking handbooks" or even programs that are written for the purpose of hacking into systems. However a true cracker writes his/her own code, as every system they break is different.

Antivirus Software

As the world becomes more reliant on computer systems, no matter how sophisticated the systems are, people are still vulnerable to various forms of attack. In March 1999, there was the "Melissa" virus. This virus was powerful enough to force large scale companies to turn of their email systems, until the virus was cleared. In 2000

the “I LOVE YOU” virus had similar devastating effects. Apart from these viruses, there are viruses such as trojans which hackers use to enter computer systems.

Types of Infection⁵

The most common types of infection are:

- **Viruses** - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail viruses** - e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.
- **Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
- **Trojan horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

There are various ways to protect a computer system against viruses, trojans and other vulnerabilities. The first way to protect against this type of threat is by having an antivirus software program. Two of the most popular antivirus program manufacturers are Symantec and McAfee Security.

⁵ <http://computer.howstuffworks.com/virus1.htm>

Symantec's Norton Antivirus 2003 is the latest update to this product. It can cost as little as approximately fifty US dollars for a home user, or more for business licenses. Below are some of the features the latest product by Symantec.

Key Features⁶

- Detects and blocks viruses in instant message attachments.
- Exclusive Worm Blocking technology detects worms such as Nimda in outgoing mail to prevent them from infecting other computers.
- Automatically removes viruses, worms, and Trojan horses.
- Scans and cleans both incoming and outgoing email messages.
- Downloads new virus definitions automatically to protect against new viruses.
- Script Blocking defends against fast-moving script-based viruses such as "ILoveYou" and "Anna Kournikova."
- Worm Blocking and Script Blocking can detect new threats even before virus definitions are created for them.
- Includes step-by-step instructions for installation, even on a computer that has already been infected.

⁶ http://www.symantec.com/nav/nav_9xnt/features.html

Below are some of the benefits of owning McAfee's VirusScan 7 antivirus software.

Benefits ⁷

- Detects viruses, Trojans, worms, malicious ActiveX controls and Java applets.
- Comes with an integrated personal firewall. This firewall puts up a barrier to protect the user and his/her PC, even when they are away from the computer. Automatically removes viruses, worms, and Trojan horses.
- Stops new malicious threats from infecting your system with Script Stopper. Script Stopper detects, alerts, and blocks malicious script actions to keep the computer safe from script-initiated threats. It adds an extra layer of protection from the most common type of infection method for consumer viruses.
- The Hostile Activity Watch Kernel (HAWK™) constantly monitors the computer for virus-like activity providing even more protection for Internet-based threats. It looks for events that may indicate new mass-mailers, or attachments with double file extensions. By monitoring for these typically malicious activities, HAWK notifies the user and lets him/her take action before damage occurs. HAWK saves time, and possibly data and money that could be lost by virus infiltration.
- VirusScan 7 lets the user quickly scan files and access other VirusScan features directly from Windows.
- VirusScan 7 scans Microsoft Office 2000+ documents to provide extra protection to users of Microsoft Word, Excel, and PowerPoint (2000+) in the event that VShield background scanning must be disabled.
- VirusScan 7 checks all entry points to the user's computer including the synchronization process with the user's Personal Digital Assistant (PDA.) By eliminating threats that could be transmitted during PDA synchronization, the integrity of the system cannot be threatened by the PDA entry point and the system is more secure.
- VirusScan's Quarantine feature lets the user clean files at a later date, submit a suspicious file to the AVERT research team, and isolate the file so it is completely inaccessible—the file is actually modified so it cannot be accessed in any way by the operating system. Quarantine provides a safeguard against any accidental access of an infected or suspicious file.

⁷http://mcafee.digitalriver.com/dr/sat3/ec_MAIN.Entry10?V1=429107&PN=1&SP=10023&xid=39692&D SP=&CUR=840&PGRP=0&CACHE_ID=0

Encryption

There have been various developments to protect internet users' vital information from being viewed. One of the most popular methods of protecting data is by encrypting the vital data. There are two main standards of encryption, 40 bit and 128 bit. 40 bit encryption was one of the first type encryptions used to protect users shopping, paying bills, banking, and other online tasks. Encryption works in binary, so that if you had a 2-bit encryption you would have four keys: 00,01,10,11. In a 3 bit, encryption you would have eight possible keys. To summarize n-bit could have a possible 2^n values. So using this theory the number of values of a 40 bit would be 2^{40} . While this may seem like a large number, with the existing computing power that is available to the generally public, an average computer could break the 40-bit code in a relatively short period of time. The latest encryption is the 128-bit encryption. Experts believe that this latest encryption should be able to last the next 10 years. The reason is compared to the 40 bit encryption 128 bit encryption has 2^{88} more possible values that a computer needs to take into consideration to crack the code. One of the most effective methods to crack encryption is called "brute force." Brute force works by making the computer run various simulations of the code, until it finds a match. While this can be an effective code-cracking method for 40 bit encryption, today's computers simply cannot break a 128 bit encrypted key in a reasonable amount of time.

Computer encryption types belong in two categories. These two categories are Symmetric-key encryption and Public-key encryption. Symmetric-key encryption is when computers that are talking to each other have the same secret key (code). To satisfy this, each computer involved in the transaction must know which other computers are

talking to each other. The reason for this is so that a user could install the same key code in the computers. The two computers must have the same key codes is so it can decode the information when it is received. An example of how the symmetric-key encryption works, is if a user writes a coded message and changes certain letters, the person who is going to decode your message must know what letters you changed and how to change it back.

A public key encryption uses private key and public key. The private key is only known by one user's computer, while the public key is given out to other computers that wish to communicate with it securely. The way the other computer decodes any secure message sent by you, is by using both its own private key, as well as the public key that was sent to it.

A popular public key encryption is Secure Sockets Layer (SSL). SSL is an Internet security protocol developed by Netscape, which is used by internet browsers and web servers that transfer sensitive information. Just recently SSL became part of an overall security protocol called Transport Layer Security (TLS).

When one uses their internet browser they can tell if they are using a security protocol like TLS. If the web address in your browser window changes from an "http" to an "https," and a padlock appears in the bottom right-hand corner of the window, that website likely uses an SSL or TLS protocol. Because public key encryption uses many computer resources, systems use a combination of public-keys and symmetric-keys.

SSL Overview from the Customer's Browser viewpoint

- Browser checks the certificate to make sure that the site you are connecting to is the real site and not someone intercepting.
- Determine encryption types that the browser and web site server can both use to understand each other.
- Browser and Server send each other unique codes to use when scrambling (or encrypting) the information that will be sent.
- The browser and Server start talking using the encryption, the web browser shows the encrypting icon, and web pages are processed secured.⁸

Above is an overview of SSL, but a more in-depth view of SSL's functionality on the network level can be seen in Figure 1. In Figure 1, it can be seen that SSL is located between the application (Internet Explorer, Netscape, Telnet, etc.) and transport, where transport means TCP. TCP (Transmission Control Protocol) is responsible for verifying the correct delivery of data from client to server. TCP adds support to detect errors or lost data and to trigger retransmission until the data received is correct and complete.

SSL is located at this point is that because, as previously stated, SSL is a type of encryption, so in order for data to be encrypted before it is sent, it has to leave TCP, pass through SSL, then go to the application.

⁸ <http://www.ourshop.com/resources/ssl.html>

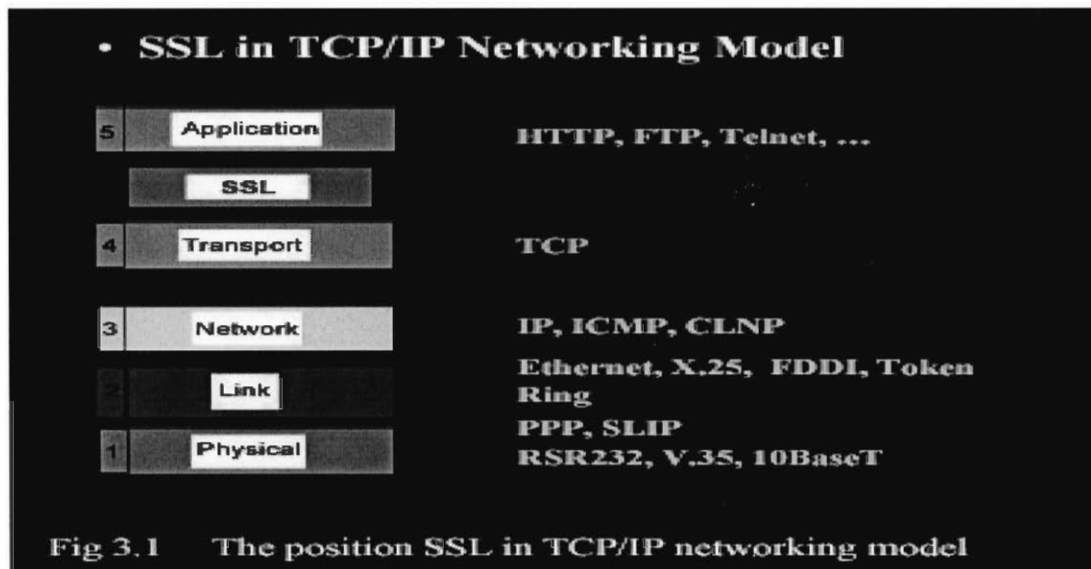


FIGURE 1⁹

Figure 1 is a top level design about how SSL functions. Figure 2 shows a deeper understanding of the working of SSL.

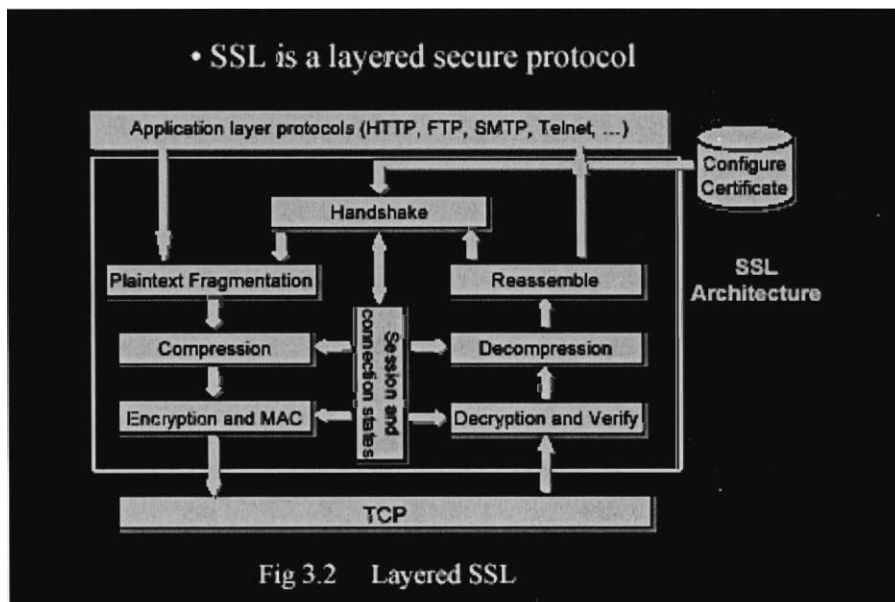


FIGURE 2²

As we can be seen with Figure 2, SSL has a certain architecture built into it. SSL protocol follows a certain procedure according to the flow of the diagram in Figure 2.

⁹ <http://www.site.uottawa.ca/~elsaddik/abedweb/teaching/elg5121/pres/26.pdf>

Data comes in through the application, gets compressed and encrypted, goes to the TCP, passes through the TCP, is decrypted, then gets displayed on the application (Internet Explore, Netscape, etc.).

Aside from SSL, there is a new product that is being developed by Microsoft called eXtensible Markup Language (XML). The reason XML was developed was to make communication and software more compatible as in this day information is constantly moving. Therefore it will be easier if software languages and applications had one base to work from rather than have incompatibilities.

The XML Security standards include XML Digital Signature for integrity and signing solutions, XML Encryption for confidentiality, XML Key Management (XKMS) for public key registration, location, and validation, Security Assertion Markup Language (SAML) for conveying authentication, authorization and attribute assertions, XML Access Control Markup Language (XACML) for defining access control rules, and Platform for Privacy Preferences (P3P) for defining privacy policies and preferences. Major use cases include securing Web Services (WS-Security) and Digital Rights Management (eXtensible Rights Markup Language 2.0 - XrML).¹⁰

¹⁰ <http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>

The following is an overview of the core XML Security standards:

- Integrity and signatures - XML Digital Signature
- Confidentiality - XML Encryption
- Key Management - XML Key Management Specification (XKMS)
- Authentication and Authorization Assertions - Security Assertion Markup Language (SAML)
- Authorization Rules - XML Access Control Markup Language (XACML)

as well as major XML Security applications:

- Web Services Security - Roadmap and WS-Security
- Privacy - Platform for Privacy Preferences (P3P)
- Digital Rights Management - eXtensible Rights Markup Language 2.0 (XrML)¹¹

For a more detailed explanation of the above terms, please refer to Appendix A.

The WS-Security specification outlines how XML Digital Signatures and XML Encryption may be used with XML Protocol (SOAP) messages as well as how security claims (such as identity credentials, for example) may be included with a message. This security mechanism goes beyond the SSL/TLS transport security mechanism, since it defines an end to end security mechanism and provides support for intermediary security processing.¹²

Digital signatures are useful for two purposes. The first is to provide persistent content integrity, and the second is to create and verify portable electronic signatures. Electronic signatures offer the digital equivalent of handwritten signatures and may be used for a variety of purposes, such as content approval, receipt confirmation, and

¹¹ <http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>

¹² <http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>

contract agreement. Digital signatures use cryptographic techniques to construct signatures that are stronger and more portable than other techniques for creating “electronic signatures”.¹³

With XML Encryption the owner of content may encrypt it to make it confidential. This will make the content unintelligible until it is decrypted. Encryption is generally performed using symmetric key encryption, since this is an efficient technique even for large documents. Symmetric key encryption uses the same key for both encryption and decryption. To send confidential information to a receiver, the sender must also share the symmetric key with the recipient but not anyone else. This can be difficult without person to person contact.¹⁴

Everything discussed thus far have been protocols that are setup in the browser system. Apart from using SSL and XKMS, credit card companies have come up with a Secure Electronic Transaction (SET). SET is a newer type of upcoming technology, which is introduced by banks as a type of encryption technology that helps protect the transfer of payment information over open networks, such as the Internet, which allows credit card users to make payments to merchants. All major credit card companies, such as MasterCard and Visa, are slowly developing his type of payment method to help customers with secure transactions

¹³ <http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>

¹⁴ <http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>

What are "SET components"? ¹⁵

- A Cardholder Application, sometimes called a Wallet, is a product run by an online consumer that enables secure payment card transactions over a network. SET protocol messages are accepted by SET Merchant, Payment Gateway, and Certificate Authority components.
- A Merchant Server component is a product run by an on-line merchant to process payment card transactions and authorizations. It communicates with the Cardholder Application, payment gateway, and certificate authority components.
- A Payment Gateway component is a product run by an acquirer or a designated third party that processes merchant authorization and payment messages (including payment instructions from cardholders) and interfaces with private financial networks.
- A Certificate Authority component is a product run by a financial institution or approved third party that is authorized to issue and verify digital certificates as requested by Cardholder Application components, Merchant Server components, and/or Payment Gateway components over public and private networks. The term Certificate Authority may also apply to the designated issuer of certificates

One major advantage SET has over other forms of secure payment is that SET has the addition of a "digital certificate." A digital certificate is an electronic credential. In other words, it is like a digital ID. These certificates are digital documents that bind a public key to an individual. Using this binding process, it allows verification of that individual. A Certificate Authority (CA) is a trusted third party organization or company that issues digital certificates. The CA is responsible for guaranteeing that the individuals or organizations granted these unique certificates are, in fact, who they claim to be.

¹⁵ http://www.setco.org/faq_usr.html

SET uses an encryption type that is a combination of DES and RSA cryptography. The way it works is the public and private keys are passed from cardholder applications to merchants and merchants to gateways. The certificates are all issued by SETCo supported Brands, including Visa and MasterCard.¹⁶

What are the key benefits to merchants for implementing SET?¹⁷

Some of the initial key benefits are:

- Increased sales from existing online shoppers who can now more confidently expand the number of merchant sites they shop at,
- Additional sales from consumers who have traditionally been constrained from electronic shopping due to their concerns about security on the Internet,
- Increased savings through a reduction of exception handling,
- Reduced costs associated with fraud.

Credit Card Technology

In the world today there are three major credit cards names, Visa, MasterCard and American Express. They all taken steps to help consumers with credit card safely. Visa has come up with a system called “Verified by Visa.” The way that this system works can be seen in Figure 3. When a consumer visits a site that is a participating Verified by Visa site, the consumer would proceed to purchase an item as they normally would.

¹⁶ http://www.setco.org/faq_usr.html

¹⁷ http://www.setco.org/faq_usr.html

However, when the final purchase is being made the consumer has to enter a password to verify that they are the owner of the card. Since this new system has just been recently implemented, few merchant websites have this technology.

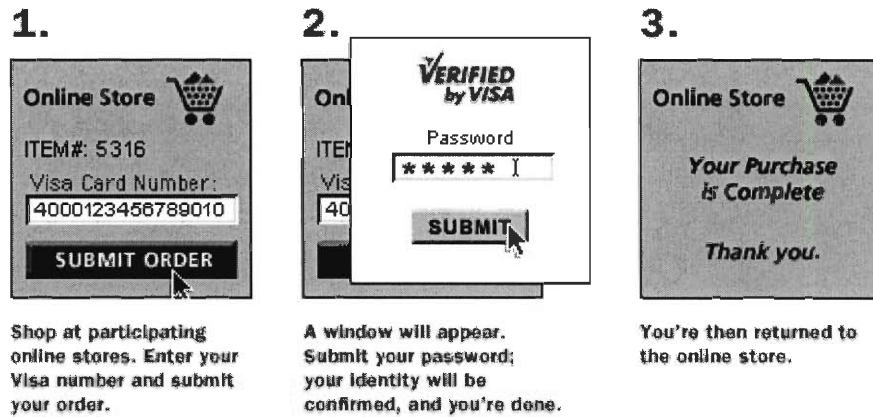


Figure 3: Verified by Visa¹⁸

Similar to Verified by Visa, MasterCard has a system called electronic wallet (E-wallet). An E-wallet is basically an online version of the consumer's physical wallet. Payment and personal information is stored safely in one place for consumers to access when they need to pay for something online. The electronic wallet helps fill online order forms quickly and easily.

¹⁸ http://www.usa.visa.com/personal/secure_with_visa/verified/how_it_works.html

Electronic wallets are ready to serve as full-fledged shopping assistants.¹⁹ In addition to filling out online forms, electronic wallets can do even more. For example, some other features include:

- Password storage for multiple web sites
- Wallet transaction history
- Storage of multiple shipping addresses
- Store directories
- Automatic notification of special offers and discounts

All of the major credit card companies have come out with smart cards. There is a Smart Chip on these cards that is a computer microchip and holds a certificate of authenticity. It provides additional security when shopping on the Internet.

American Express has come out with the American Express BLUE credit card, which contains the smart chip technology. American Express also has a smart card reader, which can be installed on to your computers USB slot to make the smart card chip accessible.

This Smart chip can be used in combination with a PIN code to use with Smart Chip Private Payments. With Private PaymentsSM, consumers can protect their card information when shopping online by using a secure, temporary transaction number. Once the consumer has a Smart Card reader installed on his/her PC, they can lock access to Private Payments on your PC so only they can use it to shop online from that PC. Blue's smart chip holds a unique certificate of authenticity that is read by your Smart

¹⁹ <http://www.mastercard.com/sg/personal/ewallet.html>

Card reader. This certificate identifies the user to Private Payments and helps ensure that the owner of the card is the only person to have access on that PC.²⁰

Private Payments is a safe and secure method of shopping online for several reasons:

- Generation of Private Payments numbers occurs only upon your request and verification of your User ID and Password.
- All Private Payment numbers are communicated from the American Express servers to your computer's desktop using the industry standard Secure Socket Layer (SSL) technology, which encrypts the Private Payments number while it is in transit from our servers to your computer.
- Because the user's actual Card account number is never revealed to a merchant in a Private Payments transaction, using Private Payments reduces the possibility of your actual Card account number being stolen or misused as a result of purchasing online.
- Any association between your actual Card account number and your Private Payments number (for billing purposes only) occurs exclusively within American Express' databases and billing systems. For further information on how American Express protects the privacy of your personal information, please refer to the American Express Internet Privacy Statement.²¹

Visa's Smart Card system works in conjunction with their Verified by Visa system. As merchants increasingly adopt chip and authentication technology, the smart Visa card brings added levels of security. For online shopping, the password-protected smart Visa card and Reader work with "Verified by Visa" to authenticate the transactions. The benefits of the reader and this technology are much like those of American express.

According to a November 6, 2002 article, "MasterCard Builds Smart Card Partnerships," in BankTech, an online news source on banking technologies, "Fraud was

²⁰ http://home4.americanexpress.com/blue/faq_chip.asp?Entry=80&from=smartchip

²¹ <http://www26.americanexpress.com/privatepayments/faq.jsp>

growing at a pace that local banking associations in France could not contain MasterCard helped them fight back with smart card technology.”²²

All of the three major credit card companies are taking steps to provide their consumers with added protection as the world turns to e-commerce more and more to do business. Security is a big concern, however, and credit card companies are taking steps to control this issue.

²² <http://www.banktech.com/story/BNK20021106S0017>

Chapter III: Procedure

The project group began the project by researching different aspects of internet security. The purpose of this was to establish an understanding of the state of multiple aspects of web security. This included researching the risks involved with general internet use, as well as more specific threats coming from credit card use online, broadband internet connections, and corporate attacks. The group also briefly studied public perceptions and how they related to the actual state of internet security. This preliminary research was largely done using the online database, ABI Inform.

The project team also conducted weekly meetings with project advisor and assistant professor of management at Worcester Polytechnic Institute, Huong Higgins. During these meetings, the group and Prof. Higgins would discuss the current state of the project, and relay ideas about the project between each other. After approximately six weeks of investigating general topics in internet security, the team decided to direct the project to a more specific goal. With the help of Prof. Higgins, the group focused the project towards researching the use of credit cards online, as well as the risks involved and the technologies and policies used to prevent theft.

Once the team had determined a more specific topic, they met to decide on the best way to approach the problem. The first task was to clearly state what exactly the goals of the project were. After some discussion, the group agreed that the purpose of the project was to research the current state of security technologies available to prevent credit card theft while the data is in transit, and make recommendations to both consumers and retailers about the risks associated with online credit card theft. The next step was to determine the best way for the team to solve the problem at hand. The

decision made was to break the problem into smaller, easier to answer questions that when combined, would lead to the project goals. The team created a Gantt chart, which can be seen in Appendix B.

The question the team decided to answer first was “What is the risk of a credit card number being stolen online?” The team soon realized that this would be a difficult question to answer, so the project group split that question up into two separate parts. The first would be to answer “How many credit card numbers are stolen yearly,” while the second would be to answer “How many credit card transactions occur online yearly?” With these two figures, the group would be able to find an approximate percentage of internet transactions are fraudulent, which would give a representation of the risk of online credit card theft. To uncover this data, the group began by researching credit card companies to see if they disclosed data about how many online transactions they process. The team visited the websites of Visa, American Express, MasterCard, and Discover Financial Services. While at these websites, the project team scoured for data relating to credit card transactions and thefts, as well as overall fraud rates. The team also located contact information and when appropriate sent questions to the customer service departments of the companies in hopes of a reply.

Next, the project group began researching government agencies to determine if they may have data regarding risks of online fraud. The team began by making a list of known government agencies that may deal with online credit card theft. This list included the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), the Department of Homeland Security (DHS), the Securities and Exchange Commission (SEC), the General Accounting Office (GAO), and the Federal Trade Commission (FTC).

The team reviewed articles posted on each of the sites, searching for data showing the number of cases of credit card theft reported to each agency. While searching the FBI website, the group also discovered two more government agencies, the National White Collar Crime Center (NW3C), the National Infrastructure Protection Center (NIPC), and the Internet Fraud Complaint Center (IFCC). The IFCC is a partnership between the NW3C and the FBI that deals with complaints of internet fraud within the United States²³. They release an annual report that details the center's data for internet fraud and breaks it down by type of fraud, location, and other aspects. The team examined CyberNotes, an online magazine published by the NIPC that reports on internet security vulnerabilities. The project group also utilized resources from the Australian National Office for the Information Economy (NOIE). The project group also noted potential people to contact at certain agencies, if any specific questions arose.

The project team also looked to companies specializing in internet security to determine the risks of online credit card theft while the data is in transit. The group investigated websites of internet security firms such as Verisign, RSA Security, Systrust, Webtrust, and Sanctum Inc. At these websites, the group noted different technologies available as well as packages available to different types of clients. The group also studied specific technologies, like Secure Sockets Layer. This involved researching websites such as Netscape, Apache SSL, and Verisign. The team took a small sample of various websites to examine what companies they used for providing SSL, which can be seen in Appendix C.

By this time the team had also begun to search for answers to the next question, "How are credit card numbers stolen while in transit?" This involved researching

²³ IFCC 2001 Internet Fraud Report

different types of software and hardware used by criminals. To find this, the team once again turned to the internet, and began by using search engines such as Google, Ask Jeeves, and CNet. With these searched the group found and useful websites, many for companies who develop technology to defend computers against cracker attack. Using these results combined with articles found in the ABI Inform database, the project group found answers to the question at hand.

For the final questions, the group was to research current and future technologies developed to prevent credit card theft while the data is in transit. This included research using the ABI Inform database, as well as other online investigation. The team scoured websites of technology developers such as Netscape, Microsoft, and Secure Electronic Transfers LLC for pertinent information. The team also searched websites of companies that utilize this technology, such as Verisign, RSA Security, and Thawte. The team contacted representatives of some of these companies via email, and received a reply from Christine Nolan from RSA Security, who provided the group with some detailed information about what features RSA can offer to its clients.

Below is a brief list of sources used by the project team. For a complete, detailed list, please check the bibliography.

| |
|---|
| <p>ABI Inform</p> <ul style="list-style-type: none">- ABA Bank Compliance- Asian Business- Bank Systems & Technology- Catalog Age- Chemical Week- Communications News- Credit Card Management- Industrial Management + Data Systems- INFOR- Information Management & Computer Security- Journal of Public Policy & Marketing- Management Services- Power Engineering- Strategic Finance- TMA Journal <p>Government Sources</p> <ul style="list-style-type: none">- Federal Bureau of Investigation- National White Collar Crime Center- Internet Fraud Complaint Center- Critical Infrastructure Assurance Office- Australian National Office for the Information Economy <p>Security Companies</p> <ul style="list-style-type: none">- Netscape- Microsoft- Verisign- RSA Security- Sanctum Inc.- Systrust- Webstrust- Apache SSL <p>Credit Card Companies</p> <ul style="list-style-type: none">- Visa- MasterCard- American Express <p>Other Sources</p> <ul style="list-style-type: none">- CyberSource Corporation- Silk City Recording Company, Inc.- Responservice- Internet Commerce Services Corporation- Information Security Magazine- XWSS.org- Granite Web Design |
|---|

Chapter IV: Results

The term “hacker” is readily used for people who break into other people’s computers and cause destruction. However this is a common misconception, hackers are people that are technological savvy and the fidget with there own gadgets and don’t invade people’s privacy. Cracker is the appropriate terminology for one who breaks in to someone’s computer to terrorize him or her.

Crackers can load various viruses on to their victim’s computers to instigate the damage. The most common virus that is used is called the trojan horse (trojan). The trojan virus runs in the background of the victim’s computer, therefore making its presence oblivious to the victim. Crackers can use this virus to view what’s on the victim’s computer, see what buttons the victim types, therefore making everything the victim does viewable by a third party. Worms are another form of virus, worms just keep replicating slowing the computer network down, while seeking weaknesses in the system and exploiting them.

Due to the awareness that private data has to be protected, there was an initial 40 bit encryption created, however it was soon realized that with advancing technology that a 40 bit encryption could be easily cracked by the method “brute force”. Therefore in its place a 128 bit encryption was created. Having a 128 bit, encryptions mean that there is a 2^{128} possible combination.

Computer encryption types belong in two categories. These two categories are Symmetric-key encryption and Public-key encryption. Symmetric-key encryption is when computers that are talking to each other have the same secret key (code). A public key encryption uses private key and public key. The private key is only known by one

user's computer, while the public key is given out to other computers that wish to communicate with it securely.

Secure Sockets Layer (SSL) is a popular type of public key, which is encrypted to 128 bits. This internet security protocol was developed by Netscape, and is used now in all the internet browsers. SSL works in between the application (i.e. browser), and the transport (i.e. TCP). SSL is one of the most widely used protocols as it is integrated into the browsers.

Apart from SSL, there is a new product that is being developed by Microsoft called eXtensible Markup Language (XML). The reason that Microsoft is doing is because it, in this day it would be good if there was a stable basis were all software could be developed. The XML Security standards include XML Digital Signature XML Encryption, XML Key Management (XKMS), Security Assertion Markup Language (SAML), XML Access Control Markup Language (XACML) and Platform for Privacy Preferences (P3P) for defining privacy policies and preferences.

Credit card companies are also trying to provide consumer with protection against fraudulent action. Three of the worlds biggest credit card companies Master Card, Visa Card and American Express, have come up with ways to help their costumer base. Visa has come out with a system called "Verified by Visa". In this system the customer can mask his/her credit card number by using a false number which is given by Visa for online use, and an access pin well verify if the card holder is the one entering the card number. In the same way Master Card has an "E-wallet" system where it stores all your private information in an encrypted space, where you could access it by using your pin.

American Express has a credit card which incorporates a "smart chip" this chip

can be used along with a smart card reader, which keeps your card number secure through the use of digital certificates, and it can only be used by an authorized person

Secure Electronic Transaction (SET) is a newer type of upcoming technology, which was introduced by banks as a type of encryption technology that helps protect the transfer of payment information over open networks, such as the Internet, which allows credit card users to make payments to merchants.

Chapter V: Analysis of Results

Crackers use a wide variety of methods to intercept and steal credit card numbers online, by taking advantage of poorly configured or secured systems. One of the most popular methods is to use viruses. All consumers and retailers using the internet to conduct business should have antivirus software installed on all of their systems. Not only that, they must update their software at least monthly to make sure they can keep as current as possible. While these programs cannot completely protect against all viruses, they will help keep the computer systems safer.

Since SSL is nearly impossible to crack, it has become the most widely used security protocol. Recently Swiss researchers may have cracked a form of SSL known as Open SSL, but this is not a major threat to credit card transfers online.²⁴ It is also one of easiest protocols to implement, as there are many different versions offered by multiple companies. Its encryption is secure enough that nearly all consumers and retailers can be confident that SSL can protect their credit card information.

eXtensible Markup Language is a relatively new security standard that may one day replace SSL as the most widely used system. XML offers a wider range of features than SSL, including XKMS, XML Encryption, XML Digital Signature, and others. Unfortunately, XML's integration into computer networks will take years, as it is expensive and difficult to implement properly. Once implemented, however, XML can provide consumers and retailers with unprecedented security.

There are many useful technologies that can be used to verify that the person making a purchase online is in fact the owner of that credit card. Verified by Visa is one

²⁴ McLindon 2003

such technology. It requires the purchaser to know both the card number as well as a password to go with that card. This means that if a cracker intercepts and obtains a card number, it is essentially useless without the password. Another technology is American Express' smart card. Since this requires a card reader in order to make purchases, an intercepted card number is completely useless without the physical card as well. SET is the most widely used technology for verifying the purchaser, and uses an "e-wallet" to do this. All of these technologies not only help protect the consumer's card, it also protects the retailer by verifying that the transaction is not fraudulent. Many retailers lack insurance to cover for fraudulent transactions, so these systems can save retailers money.

Chapter VI: Conclusions and Recommendations

The project's objectives are to identify the threats of theft to internet users making online purchases using credit cards and to recommend steps consumers and retailers can follow to prevent it. By conducting a thorough investigation of the technologies currently in use and being developed, the project group's motivation is to help consumers make knowledgeable choices when making online purchases with a credit card. Through a comprehensive analysis of various sources, the project team gathered information to make decisive conclusions on the current state of internet security technologies aimed at preventing credit card theft online.

A consumer's risk of online credit card theft during transit can be reduced by following some simple steps. These steps include utilizing technologies such as SSL, SET, and advanced credit card technologies. Both the retailer and consumer can implement these technologies and policies in order to reduce risk. However, if either the retailer or consumer fails to follow the recommend procedure, the risk of theft increases.

If a consumer or retailer who uses or may in the future use the internet for purchases would like to learn more about completely securing their information from criminals, the project team recommends that they investigate other security issues. These include the threat of credit card numbers being stored and stolen from a database and protecting the user's physical card from theft.

The following are recommendations the project group feels are appropriate to safeguard credit card numbers from being stolen while in transit online.

Recommendations for Consumers

1. Do not type your credit card number unless you are sure that both the computer you are using and the site you are connected to is secure.
2. Never send credit card information over unsecured mediums such as instant messaging, email, or chat programs.
3. Always have an antivirus software program installed on your computer and update it at least monthly.
4. Make sure you are using a current version of SSL with 128 bit encryption. Do this by updating your internet browser to the latest specifications.
5. Check the website you are ordering from to make sure it uses SSL or similar technologies. To do this, check the lower right hand corner of your browser and look for a padlock icon. This does not guarantee the site is completely secure, but can give some assurance.
6. Use a credit card with advanced technology, such as Verified by Visa or smart card.
7. Try to confirm the validity of the site you are purchasing from by checking to see if it is approved by an online security firm such as Verisign, Webtrust, or RSA Security.
8. Maintain control of your computer by not allowing others to access it. This can be accomplished by using passwords for login.
9. Set up a firewall between your computer and the internet. When configured properly, a firewall can deter crackers from pursuing your information further.
10. Use a credit card that offers insurance if your information is stolen. While this will not prevent your card number from being stolen, it is a last resort if anything were to happen; your losses can be minimized.

Recommendations for Retailers

1. Maintain your computer systems by making sure no unauthorized personnel are allowed to use them.
2. Routinely check your system to make sure no devices have been placed that might collect the data being transferred.
3. Use a form of SSL encryption to insure safe transfer of credit card information. This will also instill trust among your consumers.
4. Allow for the use of technologies such as SET, Verified by Visa, and smart cards, so that the consumer's identity is known to be correct.
5. Always have an antivirus software program installed on your computer and update it at least monthly.
6. Only accept credit card transactions that have gone through your secure system. Do not accept purchases made over email or other insecure mediums.
7. Have appropriate routers and firewalls installed between your computer systems and the internet to deter crackers from pursuing your information.
8. Once you have implemented your security features, request an audit by a company such as Webtrust or Verisign to confirm your site's security.

Bibliography

- Amato-McCoy, Deena "MasterCard Builds Smart Card Partnerships." Bank Systems & Technology. 39 (Nov 2002): 42-44. Online. ProQuest. Internet. 13 February 2003.
- Bhimani, Anish, "Web Services, Not So Fast", 2002, Information Security Magazine, October 2002, <<http://www.infosecuritymag.com/2002/oct/webservices.shtml/>>
- Black, Tricia E. "Taking Account of the World as it will be: The Shifting Course of U.S. Encryption Policy." Federal Communications Law Journal. 53 (Mar 2001): 289-314. Online. Proquest. Internet. 5 November 2002.
- Bobbit, Mike. "Bullet Proof." Information Security Magazine, May 2002, <<http://www.infosecuritymag.com/2002/may/bulletproof.shtml>>
- Boyd, Josh "Safety on the Auction Block", 2000 Information Security Magazine, January 2000 <http://www.infosecuritymag.com/articles/january00/columns_security_market.shtml>
- Brain, Marshall "How Computer Viruses Work", 2003 how stuff works, <<http://computer.howstuffworks.com/virus1.htm>>
- "Building an E-Commerce Trust Infrastructure." 2002. Verisign, Inc. 12 November 2002 <<http://www.verisign.com/resources/gd/buildEcommerce/>>.
- "Building an E-Commerce Trust Infrastructure: SSL Server Certificates and Online Payment Services." Verisign, Inc. Mountain View, CA, 2000.
- Burroughs, Richard. E., and Rajiv Sabherwal. "Determinants of Retail Electronic Purchasing: A Multi-period Investigation." INFOR. 40 (Feb 2002): 35-56. Online. ProQuest. Internet. 4 November 2002.
- Chiger, Sherry. "6th Annual Electronic Marketing Survey." Catalog Age. 19 (Jun 2002): 71-76. Online. ProQuest. Internet. 13 February 2003.
- Chou, David C., David C. Yen, Binshan Lin, and Philip Hong-Lam Cheng. "Cyberspace Security Management." Industrial Management + Data Systems. 99 (1999): 353-361. Online. ProQuest. Internet. 5 November 2002.
- Critical Infrastructure Assurance Office. Practices for Securing Critical Information Assets. Washington D.C., 2000.
- D'Amico, Esther. "Cybersecurity Gains Momentum." Chemical Week. 164 (Aug 21, 2002): 42-43. Online. ProQuest. Internet. 5 November 2002.

- D'Amico, Esther. "Locking Up Cyber Security." Chemical Week. 164 (Jan 2, 2002): 37-38. Online. ProQuest. Internet. 4 November 2002.
- Davis, Donald. "Once again, with feeling." Credit Card Management. 15 (Nov 2002): 48-50. Online. ProQuest. Internet. 13 February 2003.
- "Electronic Security Technology Roadmap." Power Engineering. 104 (Nov 2000): 37. Online. ProQuest. Internet. 5 November 2002.
- "Electronic Wallet", 2003, MasterCard
<<http://www.mastercard.com/sg/personal/ewallet.html>>
- "FAQ - About Private Payments". 2001, American Express
<<http://www26.americanexpress.com/privatepayments/faq.jsp>>
- "FAQ - About Smart Chips", 1999, American Express
http://home4.americanexpress.com/blue/faq_chip.asp?Entry=80&from=smartchip
- "Frequently Asked Question", 2003, SETco, <http://www.setco.org/faq_usr.html>
- "Getting Started With XML Security", 2002,
EarthLink, <<http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>>
- Giesen, Lauri. "Good tidings for 'Net commerce." Credit Card Management. 15 (Oct 2002): 18-24. Online. ProQuest. Internet. 13 February 2003.
- Grayson, Margaret. "What's in Store for 2002?: Internet Security and the Evolutions of Apps." Communication News. 48 (Dec 2001): 13. Online. ProQuest. Internet. 5 November 2002.
- Guard, Mary Beth and L. Michael Guard. "Card smart." ABA Bank Compliance. 23 (May/Jun 2002): 38-45. Online. ProQuest. Internet. 13 February 2003.
- "Guide to Securing Your Web Site For Business." Verisign, Inc. Mountain View, CA, November 2002. <<http://www.verisign.com/resources/gd/secureBusiness/>>.
- Hawkins, Steve, David C. Yen, and David C. Chou. "Awareness and Challenges of Internet Security." Information Management & Computer Security. 8 (2000): 131-143. Online. ProQuest. Internet. 4 November 2002.
- "How it works", 2003, Visa
<http://www.usa.visa.com/personal/secure_with_visa/verified/how_it_works.html
>

- “How SSL Works.” Netscape Communications Corporation. 1999
<<http://developer.netscape.com/tech/security/ssl/howitworks.html>>
- Hulme, George V. “Visa voices biometrics support.” InformationWeek. 912 (Oct 28, 2002): 55. Online. ProQuest. Internet. 13 February 2003.
- “Increase Web Security and Performance.” Communication News. 39 (Sep 2002): 44-45. Online. ProQuest. Internet. 5 November 2002.
- Internet Fraud Complaint Center. “Internet Fraud Preventive Measures.” February 4, 2003.
- “Introduction to SSL.” Netscape Communications Corporation. October 9, 1998.
<<http://developer.netscape.com/docs/manuals/security/sslin/contents.htm#1041640>>
- Klemow, Jason. “Credit card transactions via the Internet.” TMA Journal. 19 (Jan/Feb 1999): 10-14. Online. ProQuest. Internet. 13 February 2003.
- Lee, James and Claudine Kolle. “Securing cyberspace.” Asian Business. 38 (Apr 2002): 23-28. Online. ProQuest. Internet. 13 February 2003.
- “McAfee Virus Scan: Benefits”, 2003 McAfee,
<http://mcafee.digitalriver.com/dr/sat3/ec_MAIN.Entry10?V1=429107&PN=1&SP=10023&xid=39692&DSP=&CUR=840&PGRP=0&CACHE_ID=0>
- McCarthy. Mary Pat and Stuart Campbell. “Taking E-Security to a Higher Level.” Financial Executive. 17 (Dec 2001): 50-51. Online. ProQuest. Internet. 5 November 2002.
- McGuire, Brian L. and Sherry N. Roser. “What Your Business Should Know About Internet Security.” Strategic Finance. 82 (Nov 2000): 50-54. Online. ProQuest. Internet. 5 November 2002.
- McLindon, Andrew. “Swiss researchers crack SSL.” Electricnews.net, February 21, 2003. <<http://electricnews.net/news.html?code=9350591>>
- Mearian, Lucas. “Visa eyes voice recognition for online purchases.” Computerworld. 36 (Nov 4, 2002): 22. Online. ProQuest. Internet. 13 February 2003.
- Miyazaki, Anthony D. and Ana Fernandez. “Consumer Perceptions of Privacy and Security Risks for Online Shopping.” The Journal of Consumer Affairs. 35 (Summer 2001): 27-44. Online. ProQuest. Internet. 4 November 2002.

- Miyazaki, Anthony D. and Ana Fernandez. "Internet Privacy and Security: An Examination of Online Retailer Disclosures." Journal of Public Policy and Marketing. 19 (Spring 2000): 54-61. Online. ProQuest. Internet. 4 November 2002.
- National Office for the Information Economy. "Setting the record straight about online credit card fraud for consumers." 2002.
- National White Collar Crime Center, Federal Bureau of Investigation. IFCC 2001 Internet Fraud Report. 2002.
- "Norton Antivirus: Key Benefits" 2003, Symantec,
<http://www.symantec.com/nav/nav_9xnt/features.html>
- "Online sales: A rare bright spot." Credit Card Management. 14 (Feb 2002): 6. Online. ProQuest. Internet. 13 February 2003.
- "Personal Certificates." Netscape Communications Corporation. 2002.
<<http://wp.netscape.com/security/techbriefs/personalcerts/index.html>>
- Punch, Linsa. "Authentication's tentative gains." Credit Card Management. 15 (May 2002): 26. Online. ProQuest. Internet. 13 February 2003.
- "Reining in risky Web merchants." Credit Card Management. 15 (Nov 2002): 6. Online. ProQuest. Internet. 13 February 2003.
- "Security Report" Education Jobs <<http://www.educationjobs.com/security.htm>>
- "Server Certificates." Netscape Communications Corporation. 2002.
<<http://wp.netscape.com/security/techbriefs/servercerts/index.html>>
- "Simplified SSL - About Secure Sockets Layer and HTTPS", 2002, Ourshop,
<<http://www.ourshop.com/resources/ssl.html>>
- Simpson, Burney. "An OK year at best." Credit Card Management. 15 (May 2002): 34. Online. ProQuest. Internet. 13 February 2003.
- Sorrentino, Raf. "The delicate balance in fraud control." Credit Card Management. 15 (Jan 2003): 50-51. Online. ProQuest. Internet. 13 February 2003.
- "Stolen credit cards are big business online." 2002. The Times of India, May 15, 2002
<http://www.responservice.com/archives/may2002_issue2/media/cybertlk.htm/>.
- Tyler, Geoff. "Let's Go Internet Shopping." Management Services. 43 (Jan 1999): 26-29. Online. ProQuest. Internet. 4 November 2002.

Vijayarathy, Leo R. and Joseph M. Jones. "Print and Internet Catalog Shopping: Assessing Attitudes and Intentions." Internet Research. 10 (2000): 191-202. Online. ProQuest. Internet. 5 November 2002.

"Why Buying Online is Safe",_1998, Internet Commerce Services Corporation.
<<https://sisonline.unlv.edu/Share/Docs/Secured.html>>

Appendix A: XML Details²⁵

WS Alphabet Soup

Open standards are the foundation of Web services. All proposed Web services standards go through either the Organization for Advancement of Structured Information Standards (OASIS) or the World Wide Web Consortium (W3C). XKMS, for example, is under consideration by W3C, while SAML and WS-Security are before OASIS.

Four standards are the main focus of all Web services efforts. These standards are often referred to as "the Four Horsemen of Web services:"

- **XML (Extensible Markup Language):** The format for describing content within a given application, and the basis for all Web services protocols. XML is a superset of HTML and provides for a great deal of flexibility in identifying components of a given set of data. XML allows for the definition of schemas particular to a given industry, application type or other community of interest.
- **SOAP (Simple Object Access Protocol):** An XML-based transport protocol for communications between Web services applications. SOAP rides on top of HTTP (or, for that matter, SMTP and other protocols).
- **WSDL (Web Services Description Language):** The XML template through which Web services are described and, ultimately, published into a directory of Web services.
- **UDDI (Universal Description, Discovery and Integration):** The syntax for indexing WSDL descriptions of Web services into a directory. Think of UDDI as the Yellow Pages for Web services. However, instead of people looking up companies, it's applications looking up other applications.

The security standards landscape is less clear. A number of proposals are under consideration:

- **SAML (Security Assertion Markup Language):** An XML specification for delivering trusted authentication/authorization assertions.
- **XML Signature:** Defines formats and procedures for digitally signing XML documents.
- **XML Encryption:** Standard for encrypting XML documents.

²⁵ <http://www.infosecuritymag.com/2002/oct/webservices.shtml>

- **XKMS (XML Key Management Specification):** Defines Web services for managing cryptographic keys in support of XML Signature and XML Encryption.
- **WS-Security:** Defines SOAP headers used to implement Web services security, such as how to add encryption and digital signatures, leveraging XML Signature and XML Encryption.

In addition, there are a number of other proposed Web services standards. Among the more prominent:

- **EbXML:** An international standard for an e-business XML schema.
- **WSCM (Web Services Component Model):** An initiative for the composition and presentation of Web services.
- **WSIF (Web Services Invocation Framework):** An IBM proposal to reduce the dependence of applications on a given API or messaging standard.
- **BPEL4WS (Business Process Execution Language for Web Services):** Joint Microsoft/IBM specification for a Web services workflow standard, allowing for complex interactions of a peer-to-peer nature. This proposal combines WSFL (Web Services Flow Language) and XLANG (XML Language), which were submitted previously by IBM and Microsoft respectively.

Appendix B: Project Gantt Chart

| | | | | |
|--|------------|--------------------|--------------------|---------|
| Identify risks of credit card theft online and how to prevent it | 37d | Wed 1/22/03 | Thu 2/27/03 | |
| How many Credit Card Numbers are Stolen Yearly? | 14d | Wed 1/22/03 | Tue 2/4/03 | |
| Identify Credit Card Companies & Contacts | 2d | Wed 1/22/03 | Thu 1/23/03 | |
| Research Online Data | 3d | Fri 1/24/03 | Sun 1/26/03 | 4 |
| Contact Companies | 2d | Mon 1/27/03 | Tue 1/28/03 | 4 |
| Receive Replies | 7d | Wed 1/29/03 | Tue 2/4/03 | 6 |
| Identify Government Agencies & Contacts | 2d | Wed 1/22/03 | Thu 1/23/03 | |
| Research Online Data | 3d | Fri 1/24/03 | Sun 1/26/03 | 9 |
| Contact Agencies | 2d | Mon 1/27/03 | Tue 1/28/03 | 9 |
| Receive Replies | 7d | Wed 1/29/03 | Tue 2/4/03 | 11 |
| Identify Online Security Companies & Contact | 2d | Wed 1/22/03 | Thu 1/23/03 | |
| Research Online Data | 3d | Fri 1/24/0 3 | Sun 1/26/03 | 14 |
| Contact Companies | 2d | Mon 1/27/03 | Tue 1/28/03 | 14 |
| Receive Replies | 7d | Wed 1/29/03 | Tue 2/4/03 | 16 |
| Research Journals, Periodicals | 7d | Wed 1/29/03 | Tue 2/4/03 | |
| How many credit card transactions occur online? | 20d | Wed 1/22/03 | Mon 2/10/03 | |
| Identify Credit Card Companies & Contacts | 2d | Wed 1/22/03 | Thu 1/23/03 | |
| Research Online Data | 3d | Fri 1/24/03 | Sun 1/26/03 | 22 |
| Contact Companies | 2d | Mon 1/27/03 | Tue 1/28/03 | 22 |
| Receive Replies | 7d | Wed 1/29/03 | Tue 2/4/03 | 24 |
| Identify Banks & Contacts | 2d | Fri 1/31/03 | Sat 2/1/03 | |
| Contact Banks | 2d | Sun 2/2/03 | Mon 2/3/03 | 27 |
| Receive Replies | 7d | Tue 2/4/03 | Mon 2/10/03 | 28 |
| Research Journals, Periodicals | 7d | Sun 2/2/0 3 | Sat 2/8/03 | |
| How are Credit Card Numbers Stolen | 15d | Tue 2/4/03 | Tue 2/18/03 | |
| Identify Companies in credit card theft prevention | 6d | Tue 2/4/03 | Sun 2/9/03 | |
| Contact Companies | 2d | Mon 2/10/03 | Tue 2/11/03 | 34 |
| Receive Replies | 7d | Wed 2/12/03 | Tue 2/18/03 | 35 |
| Identify different types of software used | 6d | Tue 2/4/03 | Sun 2/9/03 | |
| Detailed research of how software works | 7d | Mon 2/10/03 | Sun 2/16/03 | 38 |
| Identify different types of software used | 6d | Tue 2/4/03 | Sun 2/9/03 | |
| Detailed research of how hardware works | 7d | Mon 2/10/03 | Sun 2/16/03 | 41 |
| What Technologies and policies are currently available to prevent theft and how do they work? | 20d | Sat 2/8/03 | Thu 2/27/03 | |
| Research journals and periodicals to identify technologies | 2d | Sat 2/8/03 | Sun 2/9/03 | |
| Identify technology companies and contacts | 3d | Mon 2/10/03 | Wed 2/12/03 | 45 |
| Contact Companies | 2d | Thu 2/13/03 | Fri 2/14/03 | 46 |
| Receive Replies | 5d | Mon 2/17/03 | Fri 2/21/03 | 47 |
| Establish criteria for interview candidates | 3d | Mon 2/10/03 | Wed 2/12/03 | |
| Identify Individuals to interview | 4d | Thu 2/13/03 | Sun 2/16/03 | 50 |
| Develop questionnaire (If necessary) | 4d | Thu 2/13/03 | Sun 2/16/03 | 50 |
| Contact individuals | 2d | Mon 2/17/03 | Tue 2/18/03 | "52,51" |
| Conduct Interviews (if necessary) | 9d | Wed 2/19/03 | Thu 2/27/03 | 53 |

| | | | | |
|--|------------|-------------------|--------------------|---------|
| What technologies and policies are being developed? | 20d | Sat 2/8/03 | Thu 2/27/03 | |
| Research journals and periodicals to identify technologies | 2d | Sat 2/8/03 | Sun 2/9/03 | |
| Identify technology companies and contacts | 3d | Mon 2/10/03 | Wed 2/12/03 | 57 |
| Contact Companies | 2d | Thu 2/13/03 | Fri 2/14/03 | 58 |
| Receive Replies | 5d | Mon 2/17/03 | Fri 2/21/03 | 59 |
| Establish criteria for interview candidates | 3d | Mon 2/10/03 | Wed 2/12/03 | |
| Identify Individuals to interview | 4d | Thu 2/13/03 | Sun 2/16/03 | 62 |
| Develop questionnaire (If necessary) | 4d | Thu 2/13/03 | Sun 2/16/03 | 62 |
| Contact individuals | 2d | Mon 2/17/03 | Tue 2/18/03 | "63,64" |
| Conduct Interviews (if necessary) | 9d | Wed 2/19/03 | Thu 2/27/03 | 65 |

Appendix C: Sample of Website SSL Providers

The following are the results of a small sample of websites the project group researched to gauge the use of SSL security. Each of the websites below offered secure transactions using SSL, and listed in the right column is the company that supplied the SSL technology to the website. This sample includes retailers of various sizes, educational institutions, and financial institutions.

| Website | SSL Provider |
|-------------------------|---------------------|
| www.amazon.com | Verisign / RSA |
| www.barnesandnoble.com | Verisign / RSA |
| www.bestbuy.com | Verisign / RSA |
| www.boomkat.com | Verisign Class 3 |
| www.coloradocyclist.com | Verisign / RSA |
| www.dell.com | Verisign / RSA |
| www.ebay.com | Verisign / RSA |
| www.fleet.com | Verisign Class 3 |
| www.forcedexposure.com | Thawte |
| www.hiway.org | Verisign Class 3 |
| www.holycross.edu | Entrust.net |
| www.kohls.com | Verisign / RSA |
| www.monarchcomputer.com | Thawte |
| www.nashbar.com | Verisign / RSA |
| www.nwafcu.org | Verisign / RSA |
| www.rightstuf.com | Verisign / RSA |
| www.target.com | Verisign Class 3 |
| www.tigerdirect.com | Verisign / RSA |
| www.trekbikes.com | Verisign / RSA |
| www.uconn.edu | UConn |
| www.umass.edu | Thawte |
| www.umn.edu | Thawte |
| www.underarmor.com | Verisign / RSA |
| www.unh.edu | Verisign / RSA |
| www.usbank.com | Verisign Class 3 |
| www.verizon.com | Verisign Class 3 |
| www.walmart.com | Verisign / RSA |
| www.warprecords.com | BT Trustwise |
| www.wpi.edu | Thawte |
| www.yahoo.com | Verisign / RSA |