Global Information Assurance Certification Paper

Identity Theft and E-Commerce Web Security: A Primer for Small to Medium sized Businesses

Josh Sorbel
GIAC Security Essentials Certification (GSEC)
Practical, Version 1.4b, Option 1
24 November 2003

CONTENTS

Abstract

This paper is a survey in topics relating to e-commerce web site security, with special emphasis on prevention of identity theft. It is geared toward any small to medium sized business that is considering launching an e-commerce web site. This paper introduces topics that every e-commerce webmaster should be familiar with: drafting a privacy policy, Visa and MasterCard's SET protocol, identity theft insurance, and methods for purchase transactions with regard to security. It is generally assumed that standard security precautions are already being taken. This may include the use of a firewall, the existence of a security policy, and the presence of a competent security administrator.

I. Introduction

When in the course of human events, it becomes necessary for your business to sell its wares online, a decent respect to the rights of all of their customers requires such a business to protect them against identity theft[1].

This paper is intended for webmasters concerned about protecting their customers from identity theft. It is not meant to be a step by step process for securing e-commerce servers *per se*, but rather a survey in topics in e-commerce security with emphasis on the prevention of Identity Theft. General information about web security is not included here, as it is assumed that the server in question has been properly configured and hardened, patches applied, anti virus software installed, etc. (if you would like to research this prerequisite process, the article "Securing Network Servers" on cert.org is exhaustive [1]).

Identity theft is defined as "the illegal acquisition of personal information such as name, social security number, driver's license, or bank/credit account numbers in order to engage in unlawful acts" [2]. It is the fastest growing crime in America [4]. According to Gartner Research and Harris Interactive, approximately 7 million people became victims from August 2002-July 2003. This was a 79% increase from the previous year [4].

The rise of this white-collar crime demands attention from system security engineers and webmasters. In this day and age, it is not acceptable to offer credit card purchasing options on a site without having carefully considered the implications of a theft of customer information. E-commerce sites should also have a privacy policy, adequate site security, adequate encryption, and possibly, insurance against identity theft.

[1] This paragraph was inspired by the Declaration of Independence.

The role of greed in identity theft

Why is Identity Theft so pervasive? Identity Theft thrives, to some extent, because of the greed of certain credit issuing companies who too easily grant credit. In these cases, the account creation process is streamlined so that customers can quickly open a personal account without a full credit review. Companies overlook what should be obvious red flags: change of billing address, the usage of a hotel address for shipping, or bad credit. The company understands the potential risk but is willing to commit fraud for the sake of closing the transaction. If the transaction is illegitimate, they will quickly write off any losses [5].

As a community, it is important to realize that every business has a responsibility to carefully scrutinize each transaction. Besides the fact that the business community loses somewhere between $40,000 and $92,000 per case (albeit indirectly) [6], there is an adverse effect of such open policies: they encourage identity theft.

We start our topic selection with a discussion on encryption. What is the best way to encrypt communications between the customer and the web site? What is the best way for customers to access their stored information? The answer to both questions is SSL.

II. SSL, digital signatures, and authentication

According to the SANS Institute, "[SSL] is the de facto standard for secured communication and virtually all Web browsers and HTTP servers support SSL, at least as an option" [7]. If you are hosting an e-commerce web server, your best option will be to use SSL.

SSL stands for Secure Sockets Layer and is a secure method of communication between two SSL-enabled applications. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for any TCP/IP connection.

In general, SSL uses public key cryptography as its method of communication. Each communicating host has a public key (available to anyone interested) and a private key (a non-shared key owned by the host). An SSL connection involves generating a secret key at connection time for each host and a public key exchange. By using the Diffie-Hellman or RSA key exchange algorithms (the two most common), the hosts will not see each other's secret keys. For that matter, no passwords are exchanged and no passwords ever traverse the network.

Public key cryptography is effective because it is virtually impossible to determine someone's private key, even if you have the public key. This means that anyone can encrypt traffic using the host's public key, but only the host can decrypt and read the message.

Therefore, your customers will transmit their credit card numbers using your public key, and you will read the message using your secret, private key. When

you respond, you will encrypt the message with your user's public key and your user will decrypt using their private key.

Certificate authentication is generally accepted as the most secure method for web communication today. However, for some start up companies the cost may be prohibitive. In fact, the most common authentication methods on the web are actually form-based authentication, probably because they appear seamless to the end user. We will review form-based and basic authorization in addition to certificate authorization.

Form-based authentication

Form-based authentication is implemented with simple http commands. Form-based authentication can be implemented with a minimum of four lines of html code:

```
<form method=POST action="/login.cgi">
<input type=text name="userid">
<input type=password name="password">
<input type=submit value="Login">
```

The first line redirects the user to the login.cgi page; the next line provides the user with input box for his username; the third line provides the user with an input box for his password, and the fourth line is for naming the "login" submission button.

Form-based authentication, if used, should be used in conjunction with SSL.

Basic authentication

Basic auth is the simplest, cheapest, and least secure method of authentication. In basic auth, there is no encryption, so passwords are transmitted in the clear.

Basic authentication works by adding extra headers to http client requests. The first step is the client connecting to a protected page the same way he would connect to any other page. At that point the server notifies the client of its page's protected status and demands a password. Browsers will generally open up a dialog window with options for username and password, and the client will either login successfully or continue to get the HTTP 401 error, "unauthorized."

Basic auth is not recommended for any public site that would have a need for a user login process.

Keeping your customers' information confidential is paramount to your company's success. At the very least, a capable company will invest in form-based authentication over SSL. As the business starts to garner a reputation in it's industry, however, it will probably opt for an upgrade to certificate auth.

With SSL, we can be sure we are communicating privately with our customer, but what if our customer is using a phony credit card? There are several checks we can implement.

III. Methods for secure credit transactions

There are several methods by which secure transactions can take place.

A. Real Time Credit Card Authorization

Authorizing your customer's credit card in real time allows you to verify that the credit card is legitimate and has not been reported lost or stolen. The authorization can be done with third party software such as ICVerify (http://www.icverify.com) or Mail Order Manager (http://dydacomp.com). ICVerify is a client/server verification only system, while Mail Order Manager's verification is part of a larger suite of services, including contact management and order entry.

It is important to realize that the authorization, however, does not verify that said customer is who they claim to be.

B. Address Verification Systems

Address Verification Systems (AVS) provide an additional measure of security. An AVS will cross check the billing address (provided by the customer). Vendors may decide to decline a transaction based on a failed check.

Like real time authorization, AVS should be used as part of a defense-in-depth solution, as alone it does not provide complete assurance that the cardholder is legitimate. In addition, AVS suffers from a high failure rate: less than 60% of transactions will obtain a full match on AVS [8]. Of those, 98% are actually legitimate transactions [9]. This may translate into loss of revenue for the business.

One solution may be to flag orders that do not match up instead of declining them. A more thorough investigation can be made after the transaction has taken place.

C. Card Verification Codes

Card Verification Codes (CVV2 for Visa, CVVC for MasterCard, and CID for American Express) is a three or four digit number, independent of the sixteen-digit credit card number. The code does not get printed on receipts. For Visa and MasterCard, the code is a three-digit number that appears at the end of the account number on the back of the card. For American Express, the code is a four-digit number that appears on the front of the card above the account number.

Merchants can ask for this code on an order form. MasterCard actually requires it for all online purchases.

D. Predictive Statistical Models

A Predictive Statistical Model queries a database (external to your site) against millions of online sales to come up with a score for a given transaction. This score quantifies the risk of the transaction. Predictive statistical models can be used to accept or deny a transaction in real time or for analysis and review after the fact.

E. Rule-Based Detection

Rule-Based Detection integrates all of the above into a set of if-then statements, specific to your organization. The rule set is meant to get better over time as you become more aware of where the red flags should be. For example, a business might choose to deny any order greater than $1000. They might choose to deny orders coming from the Middle East. Any number of custom rules can be written.

There are several commercial products that have the ability to implement custom rules. Two such products are FraudShield (www.clearcommerce.com) and Equifax ElDverifier (www.equifaxsecure.com).

F. SET

SET (Secure Electronic Transaction) is fast becoming the de facto standard for secure online transactions [10]. SET was developed as a joint effort between Visa and MasterCard, and has the backing of IBM, Microsoft, Netscape, and VeriSign, among others. SET is significant because it allows for payment processing without the seller ever having to see the customer's credit card information. Without SET, a merchant must maintain a database of credit card numbers on site.

SET is popular because it addresses seven key business requirements [8]:

1. It provides confidentiality of payment and order information
2. It ensures the integrity of all transmitted data
3. It proves to the merchant that the cardholder is legitimate
4. It proves to the cardholder that the merchant is legitimate
5. It ensures the use of best security practices
6. It creates a protocol that does not depend on transport security mechanisms nor prevents their use
7. It facilitates and encourages interoperability among software and network providers.

There are four entities involved with a SET transaction:

1. The cardholder. The cardholder opens a credit card account (MasterCard or Visa only) with a bank. The bank then issues an electronic wallet to the customer. The electronic wallet will be used to make purchases over the Internet.
2. The Electronic Wallet Provider is usually the same entity that granted the cardholder a credit line.
3. The Merchant.

4. The Acquirer. The acquirer is the financial institution that processes payment authorizations from a merchant. It uses a payment gateway to accomplish this. Also, the Acquirer provides the SET software to the merchant.

The steps involved in a SET transaction are as follows:

1. The cardholder places an order over a web site.
2. After choosing his payment method, the cardholder checks the merchant's identity by asking for the merchant's public key.
3. After verifying the merchant's public key, the cardholder utilizes his electronic wallet to retrieve his credit card number and SET certificate for payment. The cardholder then sends this information to the merchant.
4. The merchant combines his own SET certificate with the cardholder's information and sends it out to the acquirer.
5. To authorize payment, the acquirer will examine the merchant and cardholder's information. The acquirer will then digitally sign an authorization message and send it to the merchant.
6. The merchant sends a confirmation letter to the customer, generates a receipt, and ships the goods.

The authorization process can also take place if the cardholder does not have an electronic wallet. In this case, however, the merchant will have access to the cardholder's credit card information. [11]

IV. Insurance for Identity Theft

Do you need insurance?

The Computer Security Institute conducts an annual "Computer Crime and Security Survey" for a state-of-the-industry picture of fraud and security incidents in the United States. The results of the 2002 survey were alarming:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months [12].
- Eighty percent acknowledged financial losses due to computer breaches [12].
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported a combined $455,848,000 in financial losses [12].

With almost a half billion in losses for 2002, e-commerce insurance is worth considering. AIG (www.aig.com) is the biggest, offering claims arising from acts, errors, and omissions in the insured's computer and Internet services.

To be fair, e-commerce insurance is generally for the big boys, like CCBN (www.ccbn.com), which hosts investor relations web pages for over 2500 publicly traded companies and carries web casts for quarterly earnings calls [13]. CCBN carries a number of tech policies through CHUBB (www.chubb.com), including errors and omissions insurance and business interruption insurance.

The vast majority of businesses looking to get their first e-commerce site up running would probably opt out of an expensive insurance policy. It would be a good idea, however, to at least consider the financial implications of your site going down or an information (read: credit card) compromise.

V. The Privacy Policy

Any site that collects customer information should have a privacy policy. Customer information is divided into three categories: *personally identifiable* (any information that ties a user to your site), *sensitive* (any information that is generally protected by the individual), or *legally protected* (any information whose collection is regulated by law). Sensitive information could be transaction history, home address, email address, or phone numbers. Examples of legally protected information would be financial, medical, education and credit information. The type of information that your site collects is the determining factor in how extensive your privacy policy needs to be.

Drafting an effective privacy policy will take a certain amount of effort. At a minimum, representatives from marketing, legal, public relations, finance, and information systems will need to be consulted. Considerations include the type of data collected, how it is collected, where it is stored, how long it is kept, and whether it is shared with other companies. Enforcement of the policy includes continuing internal or third party audits.

The first steps in implementing a privacy policy involve analyzing your organization's needs and collecting information about current practices.

- Do you need to know who is visiting your web site? Do you need the specific IP addresses or more general data, such as hits per page?
- Would information regarding browser type, machine type or other client-side information be useful?
- Do you need your customer's names, addresses, or phone numbers?
- Do you need demographic information, such as gender, income or industry affiliation information?
- Do you need to store data about what goods a customer has purchased in the past?
- Do you need your customer's credit card, cardholder name and expiration date?
- How long does all of this information need to be kept?

The next step in implementing a privacy policy is to collect information about current practices. You may want to track data from the point of collection to the

time that it is discarded. It will be necessary to work with all departments involved in processing, tracking and fulfilling orders, identifying where all data is stored, and if the data is commingled with other data. Walk through the process of filling an order to figure out how data is used and stored. It is also a good idea to conduct a general security audit at this time.

Step three is to organize and analyze the findings. Customer data should be organized into personally identifiable, sensitive, or legally protected data. You may also be able to find better ways to use data so that less has to be collected in the first place.

Drafting your policy

After auditing your organization, you should determine what your privacy policy should contain. A good policy should address the following principles:

A. Notice
Customers should be given notice as to what kinds of data are being collected, how the data is used, whether it is made available to third parties, how it is secured, and the amount of customization of the web site their data provides.

B. Consent
Consent implies that customers should have a choice to opt out of having their data collected and stored. It would be prudent for an e-commerce site to allow customers who wish to opt out continued access to the site's services, rather than offering an all-or-nothing policy.

C. Access and Accuracy of data
All customers should be able to access their data and change it easily.

D. Security
The security of data refers to the way your company stores, processes, maintains and protects customer information.

E. Redress
This section would include what steps a consumer who feels that their privacy has been violated should take.

F. Enforcement
Enforcement can be done through third party oversight with companies such as Trust-e (www.truste.org) and BBOnline (www.bbonline.org), or it can be done internally. The choice between self and third party enforcement is largely dependent on the type and sensitivity of information being collected.

Finally, as the policy is being drafted, be sure it is clear and concise, not vague and legalistic. It should be a document that the layperson can understand, make conscious decisions about his or her data being collected, and ultimately become

loyal to an e-commerce website that is forthcoming with their information security practices.

As a final word, it may be helpful to use a wizard to draft your policy. The Direct Marketing Association has offers a free wizard online [14].

VI. Conclusion

The security of your e-commerce web site is tantamount to its success. A high profile theft of customer credit information can do more than kill your web traffic - It can entangle your business in a myriad of fines, lawsuits, and paperwork. It is a business's practical and ethical responsibility to protect its customers' data to the fullest extent possible by drafting a privacy policy, enforcing strong encryption, and carefully checking each transaction.

As a business community, it is our collective responsibility to stop the rising incidences of identity theft. It is only through the efforts of our webmasters and security administrators that this statistic can eventually be turned around. In the digital future, ideally, there will be no such thing as Identity Theft.

Bibliography

[1] CERT Coordination Center. “Securing network servers.” 2000. URL: http://www.cert.org/security-improvement/modules/m10.html - cert.org (4 Nov. 2003).

[2] Seminole County Sheriff’s Office. “Identity theft.” URL: http://www.seminolesheriff.org/advisories/identity_theft_fdle_intro.php (4 Nov. 2003).

[3] Identity Theft Resource Center. “Facts and statistics.” May 2002. URL: http://www.idtheftcenter.org/html/facts_and_statistics.htm (4 Nov. 2003).

[4] Gartner Group. “Gartner says identity theft is up nearly 80 percent.” 2003 Press releases. 2003. URL: http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp (2 June 2003).

[5] Identity Theft Resource Center. “Identity theft – the aftermath.” May 2002. URL: www.idtheftcenter.org/idaftermath.pdf (2 June 2003).

[6] Software Information Industry Association. “Internet identity theft, a tragedy for victims.” June 2000. URL: http://www.siia.net/sharedcontent/divisions/ebus/id_theft.pdf (2 June 2003).

[7] The SANS Institute. Security essentials I textbook. 551.

[8] Fergerson, Julie. “Five tools you can use to prevent fraud.” 2002. URL: http://retailindustry.about.com/library/uc/02/uc_fraud1.htm (3 June 2003).

[9] Clear Commerce Corporation. “Fraud prevention guide.” 2003. URL: http://www.clearcommerce.com/pdf/whitepapers/ClearCommerce_Fraud_Prevention_White_Paper.pdf (2 June 2003).

[10] Moussy, Lance. “Online Payments.” 10 September 2000. URL: http://www.lancexport.com/online.htm (11 Oct. 2003).

[11] SetCo. “Frequently asked questions.” 2003. URL: http://www.setco.org/faq_usr.html (5 Nov. 2003).

[12] Richard Power. “Computer Crime and Security Survey.” 7 April 2002. URL: http://www.rrtidd.com/WebQuests/598Forensics/03CrimeSurvey/2002ComputerCrimeSurvey.pdf (5 Nov. 2003).

[13] Corporate Communications Broadcast Network. “Company overview.” 2003. URL: http://www.ccbn.com/about/company_overview.asp (11 Oct. 2003)

[14] Direct Marketing Association. “How to construct your privacy policy.” URL: http://www.the-dma.org/privacy/creating.shtml (4 Nov. 2003).

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event