Global Information Assurance Certification Paper

Securing ePayments: A Survey

Colleen Nakagawa
GIAC Security Essentials Certification (GSEC)
Practical, version 1.4b, option 1
September 20, 2004

I. Introduction

After nearly a decade, it is evident that the Internet has fulfilled early predictions of hosting 'the world's largest shopping mall.' Online shopping offers a strong value proposition to consumers: convenience, easy access, competitive pricing, and unique offerings (e.g. online auctions). Early on, it was assumed that lack of secure payment methods would severely hamper electronic commerce growth, but history has proved otherwise. Although estimates vary widely, the most recent data from the US Department of Commerce estimates that U.S. retail eCommerce sales reached $15.5 billion in the first quarter of 2004, an increase of 28.1 percent over the same period in 2003.[1]

Despite certain drawbacks, credit and charge cards (sent over a SSL-secured connection) remain the payment instruments of choice for "business to consumer" eCommerce transactions.[2] Payment cards are the most practical option for consumers and merchants for a number of reasons:

- Existing, standardized infrastructure - despite numerous payment card types, merchants can usually authorize and settle transactions via a single financial institution.
- Ubiquitous distribution – 1.2 billion credit cards in circulation in 2004.[3]
- Consumer familiarity, comfort, and brand recognition.
- Lack of any suitable, pervasive alternatives.

However, fraud represents a growing problem for eCommerce:

- According to the Gartner Group, U.S. e-tailers report "online fraud rates 19 times higher than for in store transactions at a total cost in 2001 of 700 million."[4]
- Visa USA has estimated that eCommerce fraud is approximately 10 per cent of their total fraud - despite the fact that eCommerce accounts for only 5 per cent of card sales. In 2002, Visa EU has reported that "card-not-present" fraud accounts for 23 per cent of total card fraud, up from 8 per cent in 1997.[5]
- In its *Fifth Annual Online Fraud Report*, CyberSource reported that online revenues lost to fraud were likely to exceed $1.6 billion in 2003.[6]

[1] "Quarterly retail e-commerce estimates." US Department of Commerce News. May 21, 2004. URL: http://www.census.gov/mrts/www/current.html.
[2] Sienkiewicz, Stanley. "The Future of eCommerce Payments." Federal Reserve Bank of Philadelphia, Payment Cards Center. April 2002. URL: http://www.phil.frb.org/pcc/conferences/futurepayments0902.pdf, p.16.
[3] "Card FAQs." Cardweb.com. March 19, 2004. URL: http://www.cardweb.com/cardlearn/faqs/2004/march/19d.xcml.
[4] Litan, Avivah. "Consumers Embrace Online Credit Card Security Systems." Gartner Group. February 15, 2002. URL: http://www4.gartner.com/DisplayDocument?doc_cd=104547, p.1.
[5] "A good Christmas for spending online with post Christmas Internet Sales Up 50 per cent but figures show attempted ecommerce fraud rose 25 per cent." Retail Decisions. January 9, 2004. URL: http://www.redplc.com/news/archive/default.msp?contentId=2092.
[6] CyberSource. 5th Annual Online Fraud Report: Credit Card Fraud Trends & Merchant Response; 2004 Edition, p. 4.

Public perception of the problem has also reached critical mass. Regular reports in the media of the latest hacker break-in, 'card number harvesting' Trojan, and phishing attack erode consumers' confidence and trust, so essential to continued sales growth.

This paper will review the risks involved in using payment cards on the Internet. I examine past efforts to reduce those risks, specifically focusing on the commercial failure of the Secure Electronic Transaction (SET) protocol. I will then examine some of the current efforts and determine whether there are any lessons for security practitioners in developing solutions that not only reduce risks, but that can succeed in the market.

It is assumed that the reader has knowledge of basic cryptography terms and concepts.

II. Payment cards – a brief overview

The term "payment card" encompasses several types of instruments, including credit and debit cards. For a list of definitions, see the website of paymentsystems.org: http://www.paymentsystems.org/content/cards.htm.

Figure 1 shows a typical Visa or MasterCard transaction to illustrate industry terms that will be used in this paper:

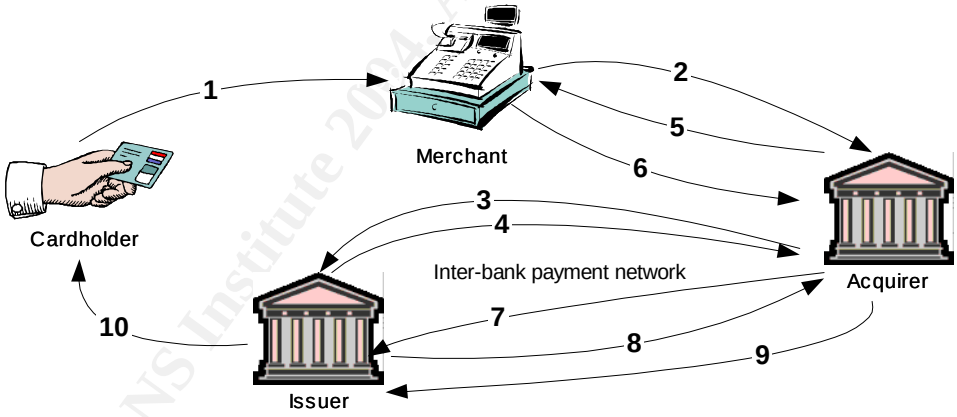

Figure 1: Typical credit card transaction

Purchase & payment (refer to Figure 1):

1. A consumer uses a payment card for goods or services.
2. The merchant sends transaction data to a "***payment gateway***" run by an "***acquirer***," (usually the merchant's bank but sometimes a third party processor), for "***authorization***."

3. The acquirer sends the transaction data to the "***inter-bank payment network***" (e.g. Visa or MasterCard), which sends the authorization request to the bank that issued the card (the "***issuer***.")
4. The issuer checks the consumer's line of credit and sends response to the inter-bank payment network authorizing or denying the transaction. The network conveys the message to the acquirer.
5. The acquirer sends the authorization result to the merchant's card terminal.

Settlement:

6. The merchant submits a batch of charges to the acquirer.
7. The acquirer conveys the request (via the inter-bank payment network) to the issuer.
8. The issuer debits the consumer's account and pays the acquirer.
9. The acquirer credits the merchant's account, retaining a percentage of the transaction amount, the "***merchant discount***" (typically 2%), as a fee for services. A portion of this fee, the "***interchange fee***" (typically 1.4%), is then shared with the card issuer.[7]
10. The issuer bills the cardholder.

A "***chargeback***" is a transaction that debits the merchant's account and credits the cardholder's account. The most common causes for chargebacks are that the cardholder denies engaging in the transaction (e.g. lost, stolen, or counterfeit card), failed to receive the goods or services ordered, or that the item received was not what was ordered.

III. Trust and security: establishing a foundation

A certain level of risk is present in any payment card transaction. Understanding the incremental risk introduced when cards are used for Internet purchases requires a look at the particular threats and vulnerabilities of that environment.

*A. Risk = threats * vulnerabilities*

1. The Internet

When a payment card is used in a "bricks and mortar" transaction, trust and security are relatively straightforward. Buyer, seller, goods, and card are physically present and can be inspected for value and authenticity. The card-issuing bank is liable for fraudulent in-store transactions involving their cards.

In "card-not-present" scenarios, trust and security are more difficult to achieve. In a mail order/telephone order ("MOTO") transaction, the buyer should have some confidence that he has reached a legitimate merchant. For example, the seller may have invested

[7] United States. U.S. District Court. "Decision. UNITED STATES OF AMERICA, Plaintiff, vs. VISA U.S.A. INC., VISA INTERNATIONAL CORP., AND MASTERCARD INTERNATIONAL INCORPORATED, Defendants." October 9, 2001. URL: http://www.usdoj.gov/atr/cases/f9800/9857.htm.

in an “800” number and produced a glossy, printed catalog. The seller, however, has much less confidence in the legitimacy of the buyer. If the buyer is using a payment card, the cardholder name, number, and expiration date are easily available to anyone who, for example:

- Has had possession of the card (e.g. unauthorized family member, waiter, store clerk).
- Accessed it in a database (authorized or unauthorized access; internal or external user).
- Obtained the information from an Internet-based card-swapping ring.

In the “virtual” world of the Internet, it is feasible for either buyer or seller to be impersonated. Buying and selling parties, the payment, and all communications are “virtualized” and represented by data. Furthermore, that data is transmitted via an open, public network making the data susceptible to eavesdropping, manipulation, and forgery. Merchants bear most of the incremental risks in this scenario as reflected in:

- Higher “card-not-present” merchant discount fees.
- Liability for chargebacks.
- Chargeback penalties (typically in the $15-$30 range).[8]
- Higher costs due to fraud management overhead.
- Lost business when orders are rejected due to suspicion of fraud.

2. The consumer and the consumer’s PC

Most consumer Internet purchases originate on a home PC, and the vulnerability of the typical home PC (and its operator) is well established. There is much to consider: buggy software, improperly configured software, insecure default installations (e.g. software, wireless LANs, etc.) as well as a seemingly endless onslaught of worms, viruses, keystroke loggers, and other malware. Because of these vulnerabilities, the adequacy of traditional password or PIN-based authentication techniques is particularly questionable when used in the context of the typical PC environment.

Additionally, people can be tricked. In an environment where users have become numb to regular messages requesting installation of applets, plug-ins, ActiveX controls, etc., it is not surprising that machines can become infested with Trojans, keystroke loggers, and spyware. “Phishing” attacks, which use spoofed emails and/or websites and social engineering to trick people into revealing sensitive information such as credit card numbers, are also on the rise. According to the Anti-Phishing Working Group, statistically phishers enjoy a 5% response rate.[9]

3. The merchant and the merchant’s system

Despite professional care taking, merchant servers (or, that of the hosting company) are not immune to problems of buggy software, improper configuration, or criminal hacking efforts. Additionally, in order make purchasing more convenient, many online

[8] “OnGuard Fraud Management Solutions.” Paymentech. URL: http://www.paymentech.com/pdf/OnGuard.pdf.
[9] “Home Page.” Anti-Phishing Working Group. URL: http://www.antiphishing.org/.

merchants save customer information, including credit card numbers, for use in "one click", express checkout systems. Compilations of purchase-enabling customer data (by online or offline merchants), are extremely attractive targets for thieves. For example:

- In March 2004, BJ's Wholesale Club Inc. revealed the theft of thousands of customer records – including credit card numbers.[10]
- In August 2004, two men pleaded guilty to charges that they conspired to hack into the systems of Lowe's home improvement in order to steal credit card data.[11]
- In February 2003, Omaha-based Data Processors International acknowledged that 8 million credit card numbers were stolen during a hacker break-in.[12]

In addition to financial losses, merchants can suffer blows to reputation, and more recently, legal repercussions. On July 1, 2003, legislation known as California SB 1386 went into effect. The law affects companies that maintain data on California residents and requires organizations to:

> "disclose any breach of the security of the system … to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The law further states, "Any customer injured by a violation of this act may institute a civil action to recover damages."[13]

B. Mitigating risk

To mitigate the risk associated with using payment cards for eCommerce, we must satisfy four key security principles:

- Authentication - Are the parties who they say they are?
- Integrity - Are messages secure against tampering or alteration?
- Confidentiality - Are information secured against access by unauthorized parties?
- Non-repudiation - Is the transaction documented in such a way that the parties cannot deny that it occurred?

These goals are often intertwined and in the electronic world, cryptography plays a fundamental role in achieving each.

[10] Sullivan, Bob. "BJ's Wholesale suspects credit card leak." MSNBC.com. March 12, 2004. URL: http://www.msnbc.msn.com/id/4516301/.
[11] The Associated Press. "3 admit hacking into Lowe's computer." August 4, 2004. URL: http://seattlepi.nwsource.com/business/apbiz_story.asp?category=1310&slug=Hacking%20Charges%20L6&searchpagefrom=1.
[12] Mearian, Lucas. "System break-in nets hackers 8 million credit card numbers." Computerworld. February 24, 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,78747,00.html.
[13] California. Senate. "SB 1386 Senate Bill (full text)." February 12, 2002. URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

1. Authentication – the core issue

Authentication[14] is an implicit part of any trusted eCommerce relationship: both buyer and seller want to know whom they are dealing with. Authentication is key to reducing fraudulent, "cardholder non-authorized" Internet transactions.

In an in-store transaction, a merchant can be reasonably assured of the legitimacy of the buyer and his card by examining the card (e.g. checking for costly and difficult to forge holograms and inspecting the card for tampering) and comparing the receipt signature with that on the card.

With "card-not-present" transactions, merchants must rely on other methods to infer legitimacy of the buyer and card. Some of the prevalent techniques include:[15]

- Address verification service - Checks the card billing address provided by the customer with the address on file with the issuer. Additionally, the merchant may refuse to ship to an address other than the billing address.
- Manual review – Usually involves contacting the customer to verify or collect information for transactions flagged as potentially fraudulent.
- Card verification number – Knowledge of the 3 or 4-digit number printed on the signature stripe (which is not included on the magnetic stripe and is never printed on receipts) implies that the purchaser has (or has had) physical possession of the card.
- Commercial fraud screening/risk scoring services - Typically uses statistics and heuristic scoring techniques to detect potentially fraudulent activity.

Historically, buyers have not been overly concerned with authenticating Internet merchants. This is likely to change, as SPAM, Phishing attacks, and news of spoofed web sites increases consumer awareness of the potential for fraud.

Traditionally, digital authentication is based on:

- Something you know (e.g. a password, mother's maiden name)
- Something you have (e.g. a token, photo ID, ATM card, digital certificate)
- Something you are (e.g. a fingerprint, a retina pattern)

There are pros and cons associated with each of the methods. In order for the authentication to be considered "strong", it must be based on at least 2 out of the 3. Many modern computing systems employ digital signature or certificate schemes based on public-key cryptography for authenticating people and systems.

2. Integrity

It is evident that parties to an eCommerce transaction need to be able to trust in the integrity or veracity of the communications between them. Integrity measures aim to

[14] Authentication should not be confused with card *authorization*, which is the process that verifies available credit and that the card has not been reported lost or stolen.
[15] CyberSource, p. 5.

protect against changes by unauthorized persons or unauthorized/unintentional changes by authorized users. Systems employing hashing algorithms and message digests can be utilized to detect changes to files or messages.

3. Confidentiality

Confidentiality ensures that order and payment information is not disclosed to unauthorized parties. Confidentiality should not be confused with "data privacy" – which usually refers to protection of stored data (e.g. in a merchant data base), nor should it be confused with anonynimity. Credit card-based purchases are never anonymous.

In electronic systems, confidentiality is typically achieved by obscuring data via symmetric key encryption systems.

4. Non-repudiation

Non-repudiation ensures that the parties to a transaction cannot deny that it occurred. Authentication is a prerequisite for non-repudiation.

In the physical or mail order world, the merchant captures the buyer's signature (via paper receipt, order form, or electronic terminal). This can be compared with the signature on file to help prove that the cardholder made the purchase.

If a cardholder repudiates an eCommerce transaction, and there is no evidence that merchandise was delivered (e.g. package receipt signature), it is difficult for the merchant to dispute a chargeback. According to MasterCard's website, 70% of eCommerce chargebacks are "cardholder unauthorized" due to cardholders simply saying, "I didn't do it." Some of this is due to fraudulent use of a cardholder's information; however, the Internet has provided fertile ground for a repudiation problem known in the industry as "friendly fraud." Friendly fraud typically occurs when legitimate cardholders purchase "frowned-upon" goods (e.g. pornography, gambling) and then deny engaging in the transaction. In the December 2001 issue of *U.S. Banker*, Steve Orfei, senior vice president of MasterCard International, estimated that half of all "card-not-present fraud" could be attributed to porn-related "friendly fraud."[16]

Electronic systems use cryptographic receipts to ensure that communicating parties cannot deny sending a message.

C. Tradeoffs

Developing any security solution requires that architects take into account the factors influencing how relevant parties will make their risk tradeoffs. Solutions for securing card payments on the Internet are no exception. Consumers, merchants, and financial institutions will evaluate an offered solution and decide:

- To avoid the risk altogether (e.g. the consumer may avoid shopping on the Internet).

[16] Bennett, Robert. "I didn't do it." US Banker. December 2001. URL: http://www.us-banker.com/article.html?id=2004041579NTHYMH.

- To accept the risk & and associated costs (e.g. the merchant may choose to budget funds for fraud loss rather than adopt the solution).
- To transfer the risk (e.g. the merchant may pass on increased costs to the consumer).
- To accept the risk, but take action to reduce it (e.g. the merchant may use other methods, like address verification or manual review).

A key factor shaping the tradeoffs made by parties to a credit card transaction is the distribution of **liability**, as set by law and by card association rules. Liability (or, who pays for the cost of fraud) is central to the question of whether the parties have a market incentive to adopt a solution. Notably:

- Federal law limits consumer liability to the first $50 USD of fraudulent credit card transactions. Typically, the issuer waives even this amount making consumer liability zero.[17]
- Card association (Visa, MasterCard) rules have allowed issuers to charge back fraudulent "card-not-present" transactions to merchants. Thus, merchants bear most of the cost of "card-not-present" fraud.[18]

  Note: Internet merchants also bear indirect costs related to "card-not-present" fraud. For example, merchants are typically charged higher interchange fees for transactions originating online. Additionally, revenue is lost when legitimate orders are rejected due to suspicion of fraud.

Other factors that must be considered when evaluating the market viability of a solution:

- Usability and convenience. Maintaining the quality of the consumer's shopping experience is of paramount importance to merchants. In a study[19] conducted in 2001, Visa surveyed consumers who shop online and found:
  - 81% agreed that entering a PIN or password before completing a transaction is secure.
  - Only 18% found swiping cards through readers attractive.
  - Only 15% would download special software.
- Technical considerations. For example,
  - Size of the implementation effort and ease of integration with legacy environments.
  - On-going operational costs.
  - System performance: impact on transaction time and ability to scale during periods of heavy load.

The bottom line is that any successful solution to the challenge of securing card-based payments on the Internet will need to satisfy a number of requirements. Security is just one aspect amongst many.

[17] Sullivan, Bob.
[18] Bennett, Robert.
[19] Sienkiewicz, Stanley, p. 19.

IV. Past solutions

A. SSL, the de facto standard

Secure Sockets Layer (SSL) secures the TCP/IP transport layer on behalf of higher-level application protocols (such as HTTP) by adding the following capabilities:

- Authentication of the server, via digital signatures.
- Authentication of the client, via digital signatures.[20]
- Privacy of the communication stream via encryption.
- Data integrity via message authentication codes.

SSL was developed by Netscape in 1994 and has become a de facto standard. The Internet Engineering Task Force (IETF) used SSL 3.0 as the basis for the non-proprietary Transaction Layer Security (TLS) protocol.

SSL was designed with two protocol layers:

- The first layer is the Record Protocol, which facilitates data transfer between client and server. It performs encryption/decryption, digital signing, and compression for the protocol's second layer.
- The second layer is composed of three protocols.
    - The Handshake Protocol initiates the SSL session. The server authenticates itself to the client via public key encryption. Optionally, the server may require the client to authenticate itself. Client and server then negotiate the symmetric keys used to ensure privacy and integrity of the subsequent communications.
    - The Alert Protocol handles errors and problems with the SSL session.
    - The Change Cipher Spec Protocol is used by either the client or server to notify the receiver that subsequent messages will be encrypted using a just negotiated algorithm and key.

Despite its near ubiquity as the foundation for "secure Internet payments", it is important to note that SSL is a generic, secure communications protocol – not, a payment protocol. SSL merely protects information in transit between the consumer's web browser and the merchant's web server. Notably:

- It provides for the authentication of computers, not people or entities. Furthermore, even fraudulent websites have been able to obtain legitimate certificates.
- It does not protect data on the consumer PC or on the merchant servers – arguably, the places where it is most vulnerable.
- It does not address non-repudiation.

[20] Almost never implemented for business-to-consumer eCommerce.

Although it didn't materially reduce merchant risk, in light of no workable alternative offered by banks and the card associations, eCommerce merchants adopted SSL. SSL provided a *sufficient* level of security for them to start and grow their businesses: it was widely available (already implemented in all major web browsers), non-disruptive to the consumer shopping experience, and easy to use for all involved. URLs protected by SSL, distinguished by the "https://" prefix, and pages displayed with secure icons (e.g. locks) gave consumers a (perhaps unjustified) level of comfort.

B. SET, build it and they will come?

The promise of electronic commerce was a major driver in the evolution of the World Wide Web, and by the mid-90s, Visa and MasterCard were engaged in a race to develop a standard for secure eCommerce payments. In 1995, Visa and its partner Microsoft published the Secure Transaction Technology ("STT") specification. Within weeks of STT's unveiling, MasterCard, whose partners included IBM and Netscape, published the Secure Electronic Payment Protocol ("SEPP.")

Two competing "standards" would clearly have resulted in an onerous burden of redundant costs and efforts for all concerned (banks, merchants, consumers, technology vendors). Industry pressure eventually forced Visa and MasterCard to work together. Drawing upon the best technologies from both STT and SEPP, the companies introduced the Secure Electronic Transaction ("SET") protocol in 1996.[21]

1. Description

SET augments the security provided by SSL by authenticating the parties to a transaction (versus SSL-based eCommerce, which usually authenticates only the web server). Cardholders, merchants, and acquirers must go through a registration process and obtain digital certificates. Additionally, they are required to obtain and install SET-specific software. The following table outlines cryptographic methods utilized by SET to achieve its security objectives:

Security Objective	**Methods employed**
• Authentication ➢ Is the cardholder the legitimate user of the card? ➢ Is the merchant legitimate – does it have a bona fide relationship with a financial institution enabling it to accept credit card payments?	• Parties must obtain digital certificates from a certificate authority. The certificates establish authenticity of the public keys, forming a basis for authenticating the parties via digital signatures.
• Integrity ➢ Is the order and payment data received the same data that was sent?	• 'One way' cryptographic hashing algorithms calculate message digests. Senders digitally sign message digests.

[21] United States. U.S. District Court.

• Confidentiality ➢ Messages cannot be read by unauthorized parties	• Symmetric key encryption protects data during transmission

Note: Although non-repudiation is not a part of the official specification, SET's use of digital signatures could form a basis for banks and card associations to establish policies for non-repudiation.

A SET purchase splits the transaction data into two parts: the order information and the payment information. By encrypting order information with the merchant's public key, and payment information with the bank's public key, the protocol ensures that *merchants cannot access payment details and banks cannot access order details*.

Although the merchant and the bank can only decrypt half of the transaction data, a cryptographic structure called a *dual signature* allows them to verify that the two parts are related. Dual signature works by including hashes of both the order and the payment information with the purchase request. The 2 hashes are concatenated and the result is hashed again. The customer then digitally signs the resulting hash. So, for example, when the bank receives the purchase request, it can:

- Decrypt the payment information using the bank's private key.
- Re-compute the hash of the payment information; concatenate this value with the order information hash included in the message.
- Hash the concatenated values and verify that this is the same data that was signed by the purchaser, thus confirming the relationship between order and payment. See figure 2, below:

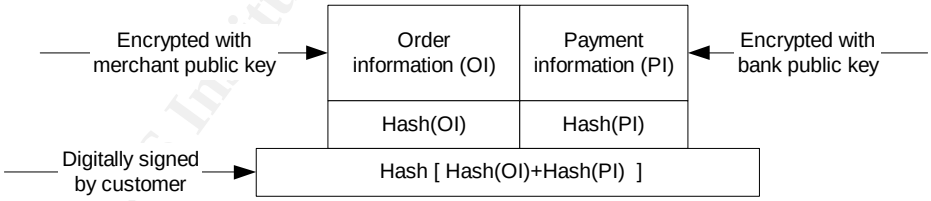

Figure 2. SET dual signature

A SET purchase is illustrated below. Note that the parties involved in the SET-specific portions of the transaction have been issued digital certificates.

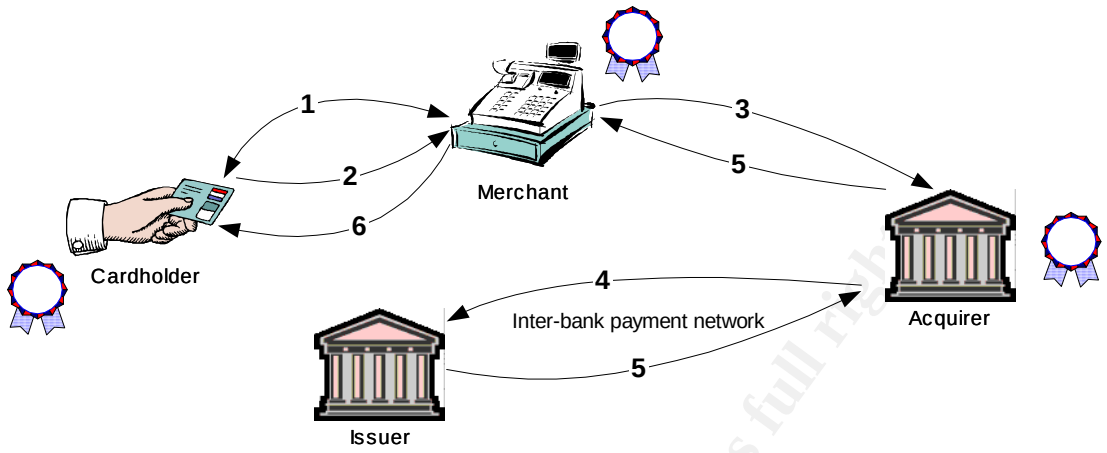

Figure 3. A SET purchase

1. The cardholder initiates a SET purchase. The merchant's SET software returns a file describing the purchase along with the merchant's certificate and that of the acquiring bank.
2. The cardholder's SET wallet software computes the "dual signature" data structure and returns it to the merchant.
3. The merchant decrypts the order information and forwards the payment information to the acquirer.
4. The acquirer decrypts the payment information and requests authorization from the issuing bank.
5. The acquirer receives the response and forwards it to the merchant.
6. If the purchase was authorized, the merchant returns a response to the cardholder's wallet software confirming the transaction.

2. 3D-SET

3D-SET sought to reduce the complexities and deployment issues of the original SET protocol by moving cardholder certificates to a central server maintained by the issuing bank. The aim was to simplify the enrollment process for the cardholder and eliminate the requirement for a "fat" digital wallet on the cardholder's PC.

3. The market verdict

Despite promotion by the card associations, lots of publicity in the trade press, and significant investments by vendors to develop compliant software, neither SET nor 3D-SET were widely adopted. Trial deployments in Europe and Asia met with limited success and activity in the critical U.S. market was practically non-existent.

Numerous reasons are cited for SET's commercial failure. During early pilots, banks discovered implementation and deployment issues:[22]

- SET-compliant products (cardholder wallets, merchant gateways, acquirer gateways, and digital certificates) from different vendors were not always compatible.
- It was harder than expected to develop policies governing cardholder authentication. Also, banks had to either assume (or outsource) the role of 'certificate authority', managing, in effect, a Public Key Infrastructure (PKI).
- Customer support would have been a challenge. If a SET transaction failed, where would the cardholder turn? The problem could've been with the cardholder wallet, merchant software, or acquirer software. Or, it might have had nothing to do with SET software. For example, there could have been a problem with the cardholder's PC or Internet connection. All of this pointed to a costly and non-trivial end user support problem; one likely to have been borne by issuing banks (or, worse, merchants.)

The requirement that all parties install additional software was also a hindrance. For merchants, there was the licensing cost, not to mention additional maintenance and technical support expenses. For the cardholder, the process of obtaining and installing both wallet software and a digital certificate (one certificate for each card they wished to use) was particularly burdensome. Additionally, the wallet was not portable – the consumer was limited to using it from a single PC.

Because SET made extensive use of cryptographic computations, there were also concerns about performance. Hardware accelerators and more powerful (and expensive) servers could have alleviated the problem, but without sufficiently large pilot tests, scalability remained a question mark. For example, what would happen to an acquirer's gateway during the Christmas rush?[23]

Lastly, the card associations did not do enough to motivate banks and merchants by shifting liabilities. Although the card associations planned to treat SET transactions as "card present," making SET eligible for the lowest merchant discount rate, merchants were still held liable for chargebacks. Without a reduction in their chargeback exposure, merchants had scant reason for incurring the expense of implementing SET. Furthermore:

- Because few banks were participating and promoting SET to their cardholders, SET wallets were not widely distributed, making the potential customer base miniscule.
- Merchants were not eager to support multiple payment methods (SET and SSL).

[22] Roberts, Bill. "On you mark, get SET, wait!" Datamation. April 1, 1998. URL: http://itmanagement.earthweb.com/secu/article.php/602391.
[23] Ibid.

As the SET effort stalled, SSL-based eCommerce took off[24]. As described in the previous section, SSL required minimal effort on the part of the merchant and no effort on the part of the consumer, banks, or card associations. Justified or not, SSL gave many consumers a sufficient level of comfort to use their payment cards on the Internet.

Some have described SET as "close to technologically perfect."[25] However, the bottom line is that high barriers to entry and availability of an "adequate" alternative (SSL) left SET with a weak business case.

V. Current efforts

As SET languished, Visa and MasterCard began separate efforts to revisit the cardholder authentication problem. In May 2001, MasterCard announced Secure Payment Application/Universal Cardholder Authentication Field (SPA/UCAF). Technical specifications for Visa's 3-D Secure were first released in June 2001.

A. 3-D Secure and Verified by Visa

Visa's 3-D Secure protocol authenticates cardholders, but without the complexities and implementation issues of SET. Most notably, there is no requirement for the cardholder to install software.

1. How it works

The cardholder enrolls in the program via his issuing bank. He provides relevant personal information then picks a password and a "Personal Assurance Message." The protocol does not dictate how cardholders will be authenticated; it is up to each issuer to decide on a method (e.g. password, smart card, PIN). The flow of a 3-D Secure purchase is illustrated in Figure 4.

[24] Tebbutt, Dan. "Ready, SET, stop." Australian Personal Computer Magazine. March 3, 1999. http://www.apcmag.com/apc/v3.nsf/0/568A421986B443CBCA256D44001AD58D.
[25] Bennett, Robert.

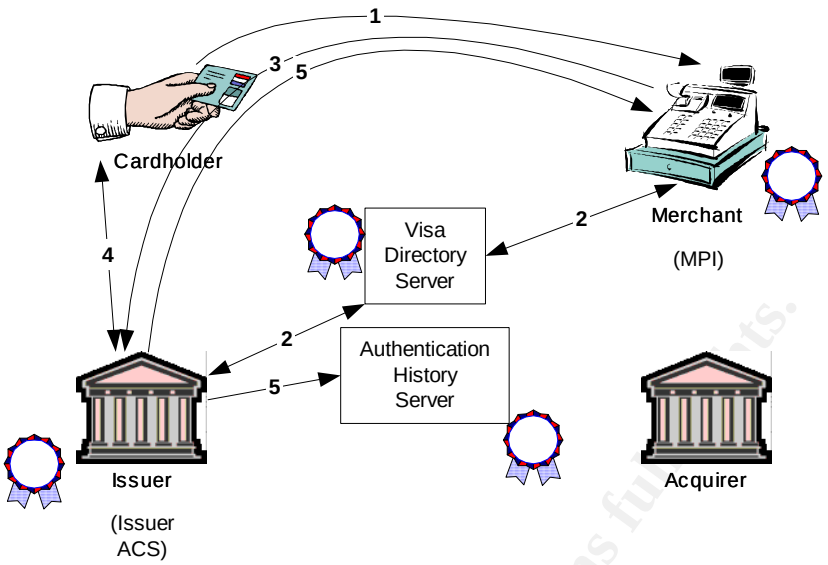

Figure 4. 3-D Secure Purchase Flow

Authorization step	Notes
1. A participating cardholder shops at the web site of a participating merchant and clicks the "buy" button.	• The cardholder provides billing and payment card information (as usual) over a SSL connection.
2. Merchant Server Plug-in (MPI) software is activated and issues a query to Visa determine whether the card (cardholder) is enrolled in the program. If yes, Visa returns a response containing the URL for the appropriate "Issuer Access Control Server (ACS)."	• MPI software may be located on the merchant site, at the acquirer or at a 3rd-party processor site. • If the card number is in a participating range, the Visa directory queries the appropriate Issuer ACS to validate cardholder participation.
3. The MPI sends an authentication request to the issuer via the cardholder browser.	
4. The issuer's ACS authenticates the cardholder and generates a response message, which includes a unique cryptographic value based upon transaction data.	• An authentication dialog is displayed to the cardholder requesting a password (or, another method such as a smart card, PIN, etc.) • The cardholder's "Personal Assurance Message" can be displayed so that the cardholder can be confident that he is, in fact, communicating with his bank.

5. The ACS returns the authentication result to the MPI via the cardholder browser and logs the result to an Authentication History Server.	• The ACS digitally signs the authentication response. • The Authentication History Server provides an audit trail.
6. The MPI checks the response; if the cardholder was authenticated, the transaction proceeds as usual with authorization.	• The MPI validates the message via the ACS' digital signature.

3-D Secure communications are carried via mutually authenticated SSL connections (note the certificates in the diagram). The exception to this is communications involving the cardholder, thus avoiding the need for the cardholder to obtain a certificate.

3-D Secure is the technology foundation for the *Verified by Visa* program. Significantly, merchants who participate become protected from fraud-related chargebacks, with liability transferred to the issuer:[26]

- April 1, 2002
  - Liability for repudiated transactions at participating European merchants shifted to the issuer.
- April 1, 2003
  - Acquirers worldwide were required to support 3-D Secure for their online merchants.
  - If a participating merchant attempts 3-D authentication, liability for a repudiated transaction shifted to the issuer *whether or not the issuer or cardholder is participating.*

This shift of liability from merchants to card issuers should provide a catalyst for merchant adoption. As more merchants participate, issuers will be strongly motivated to promote uptake amongst their cardholders. Increased cardholder participation will promote more merchant participation, and so on. Online merchants who implement 3-D Secure may also be eligible for reduced merchant discount rates.

B. MasterCard SPA/UCAF and SecureCode

The Secure Payment Application/Universal Cardholder Authentication Field (SPA/UCAF) specification defines:

- A data structure, the UCAF, a 32-byte field that serves as a "carrier" for passing authentication information between the relevant parties.
- A mechanism for transporting the UCAF.

1. How it works

[26] Steeley, Oliver. "Guaranteed Transactions, the Quest for the 'Holy Grail'." ePSO - ePayments System Observatory Newsletter, number 10. November 2001. URL: http://epso.jrc.es/newsletter/vol10/docs/ePSO-N10.pdf.

- The UCAF is incorporated as a hidden field on the merchant's web site.
- During the checkout process, a "blank" UCAF is passed back to the cardholder's browser.
- A wallet applet on the cardholder's PC detects the hidden UCAF field, triggering an authentication dialog with the cardholder's issuer.
- Upon successful cardholder authentication the issuer generates a token unique to the transaction. The token is logged and also returned in the UCAF to the merchant (via the cardholder's browser).
- When the merchant submits the standard authorization (verify that the transaction is within credit limits) request to his acquirer, the UCAF data is included in the request.
- The acquirer routes the authorization request to the issuer, where the issuer confirms transaction authenticity by comparing the UCAF received with the one logged.

SecureCode is MasterCard's eCommerce authentication program based upon SPA/UCAF. In September 2002, MasterCard announced that it had licensed 3-D Secure from Visa and made the technique one of three supported cardholder authentication methods:

- PC Authentication Program – an implementation of SPA/UCAF; requires the cardholder to download an applet.
- Chip Authentication Program – smart card-based authentication; requires the cardholder to have a smart card reader.
- MasterCard 3-D Secure Implementation – MasterCard's implementation of 3-D secure; no cardholder software is required.

Regardless of the method selected, cardholder authentication data is carried via the UCAF infrastructure.

Mirroring the Visa move, MasterCard has announced that merchant participating in *SecureCode* will be able to shift the cost of chargebacks due to cardholder non-authorization to issuers.[27]

C. Verified by Visa and SecureCode - rollout

Visa and MasterCard's latest programs are not without their implementation challenges. Some considerations:

- Until Visa and MasterCard announce a single, unified approach, merchants and consumers face having to implement two solutions for the same problem - certainly, an unattractive prospect. Many merchants accept payment cards such as American

[27] "MasterCard Launches Mastercard SecureCode --New Global E-Commerce Security Solution For Consumers." MasterCard International. September 23, 2002. URL: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=653&category=keyword&keyword=securecode.

Express and Discover, in addition to Visa and MasterCard. So far, these other industry players have not announced support for either the Visa or MasterCard scheme. The market is unlikely to tolerate multiple cardholder authentication approaches.

- The lack of a single approach will particularly test the tolerance of the cardholding public. The average consumer has 2.7 general-purpose bank credit cards.[28] Authentication and/or purchase procedures that differ between card brands will be met with resistance. The matter will be exacerbated if procedures for a single card brand vary between issuing banks.
- The systems are complex, having multiple parts and communications boundaries; complexity can lead to fragility.
- Cardholder technical support, which surfaced as a major issue with SET, is likely to be a significant challenge. For example, what if the user has popup blocking software that interferes with the authentication dialogue?

Despite the challenges, the Visa and MasterCard programs seem to be gaining traction with merchants. In its *Fifth Annual Online Fraud Report*, CyberSource reported that in 2004, 26% of merchant respondents plan to implement *Verified by Visa*, and 22% will implement MasterCard *SecureCode*.

It is still too early to ascertain how successful these programs might be. In addition to merchant adoption, there will need to be widespread uptake among issuers and cardholders. Merchants may be able to boost cardholder uptake by providing rewards when consumers use the authentications systems (effectively, passing back savings resulting from lowered merchant fees and fraud/chargeback costs). If program participation reaches critical mass, the market and the test of time will reveal the effectiveness of the programs and the soundness of the underlying technology. Cyber criminals will aggressively search for exploits, and the password passing paradigm – with all of it's inherent weaknesses- is still at the core of the Visa and MasterCard programs. Consider:

- Unless a smart card is used, the security of both systems relies upon a shared secret (e.g. passwords or PINs). Thus, the schemes are subject to the weaknesses common to all password-based systems: people choose weak passwords, reuse passwords, share passwords, etc. As the number of accounts held by a typical user proliferates, the issue of password reuse will become even more problematic.
- Any system is only as secure as the software (and hardware) that it is built upon. If the programs are adopted widely, cyber criminals will utilize well-worn methods in trying to "break the system." For example: password-stealing Trojans, spoofed merchant sites with spurious authentication dialogs, and social engineering techniques.

[28] "Card FAQs." Cardweb.com. November 7, 2003. URL: http://www.cardweb.com/cardlearn/faqs/2003/november/10.xcml.

Visa has estimated that up to 80% of eCommerce chargebacks and fraud could be eliminated with the use of Authenticated Payment.[29] Challenges notwithstanding, the quest to reduce eCommerce fraud, along with strategic liability shifts, will help drive the latest programs to greater success than that experienced by SET.

D. What about smart cards?

Any discussion of secure Internet payments would be incomplete without at least a mention of smart cards. An adequate treatment of smart cards would certainly constitute another paper; however, the following discussion touches upon some of the more salient points.

A "smart card" is a card containing an embedded microchip. The addition of computing power and data storage is the latest in the evolution of payment card features. Smart card "security" is based upon the premise that "hardware" is less subject to tampering than software.

Because a smart card is, effectively, a general-purpose computer, there are many possible applications. For eCommerce, chip-enabled payment cards can help to secure payments by providing a robust means of authenticating users via a digital signature system. The security of any public key cryptography system is compromised if the private keys are not kept secret. By storing its owner's private key, a smart card can help maintain control over the key. By protecting the smart card with a password, authorized use of the card is dependent upon two factors: possession of the card and knowledge of the password.

Smart card solutions are not without challenges, however. For example:

- Use of a smart card requires a reader. Until smart card readers become standard equipment for mass market PCs, it is difficult to see widespread adoption on the part of average consumers.
- If a smart card's strength lies in the fact that it contains a secret key, the key should never leave the card. Transferring a secret key from the card to a PC would negate the added security provided by the card. Thus, the transaction data to be "signed" should be imported onto the card and all computations performed there (which may require a more powerful, expensive microprocessor).
- A smart card must be protected against fraudulent use by securing it with a PIN, password, or biometric. Thus, for example, it is desirable for the card reader to have a keypad for entry of the PIN (a vulnerability would be introduced if the PIN was entered via the PC). This points to a more costly card reader.
- Smart cards can't protect against all attacks. For example, a spoofed web site or Trojan on the PC can trick the cardholder into authorizing a fraudulent transaction with his smart card.

[29] "3-D Secure Introduction, Version 1.0.2." Visa International. September 26, 2002. URL: http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf, p. 6.

- Widespread adoption of smart cards will probably be contingent upon extensive utility in the physical world as well as for eCommerce. This will require upgrading of the current merchant terminal infrastructure – a sizable and expensive undertaking.

So, although smart cards may offer a compelling security story, the *business* case hasn't been as clear. Visa and MasterCard first evaluated smart cards in the 1980s as a means to reduce payment card fraud. However, the idea drew little support from merchants and issuers, who were not convinced of the business case. In a late 90s antitrust case involving Visa and MasterCard, the court wrote regarding smart cards:

> "Moreover, the costs of replacing the existing magnetic stripe infrastructure would have been substantial. Merchants -- whose cooperation and financial support for a migration to chip technology were crucial to its success -- did not believe that the extra effort and costs of processing chip cards would be justified by any real benefit over the recently installed magnetic stripe terminals. Card issuers also resisted the new technology, unconvinced that a business case existed. As a result, in the 1980s Visa and MasterCard concluded, after independent and joint analyses, that the significant costs of chip technology outweighed its limited benefits in the United States."[30]

Three of the major payment card companies (Visa, MasterCard, American Express) have introduced smart card products, none of which have (yet) enjoyed widespread adoption. Still, smart cards could address the weakest points of current password-based systems and pervasive PC technologies. We are likely to see a migration to more robust solutions incorporating smart cards and digital certificates. It is unclear, however, how long this migration will take.

E. Defense-in-depth

There are no single, bulletproof answers to reducing eCommerce fraud. Risk mitigation must be approached with a defense-in-depth strategy, employing a variety of best practices.

In addition to adopting cardholder authentication programs offered by the card associations, merchants should continue to use a multi-pronged approach to reducing eCommerce fraud. For example:

- Use address verification.
- Manually review transactions flagged as potentially fraudulent.
- Use card verification number checks.
- Employ rules-based systems to screen transactions for high-risk profiles.
- Review a transaction's geographic origin. Transactions originating overseas pose a greater risk, accounting for almost half of the chargebacks for U.S.-based web

[30] United States. U.S. District Court.

merchants. Geolocation technology allows a merchant to compare the transaction's geographic origin with the billing and shipping address.[31]

Merchants must also follow well-established information security practices for Internet-connected servers and customer data. For example, Visa's Cardholder Information Security Program (CISP) mandates that all entities "… storing, processing, or transmitting Visa cardholder data" comply with program requirements[32]:

1. Install and maintain a working firewall to protect data
2. Keep security patches up-to-date
3. Protect stored data
4. Encrypt data sent across public networks
5. Use and regularly update anti-virus software
6. Restrict access by "need to know"
7. Assign unique ID to each person with computer access
8. Don't use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly test security systems and processes
11. Implement and maintain an information security policy
12. Restrict physical access to data

Initially, the CISP applied only to the largest Internet merchants. However, beginning in September 2004, any entity that accepts Visa (including bricks & mortar merchants) must comply.[33]

As has been mentioned, merchant databases containing cardholder information have become particularly attractive targets for thieves. In May 2004, in response to the rising incidence of stolen cardholder account data, the various card brands released a joint letter to merchants detailing specific requirements for securing cardholder information, highlights of which include:[34]

- Specific requirements on data that must **never** be stored (e.g. card validation code).
- Store only data that is essential to the business.
- Proper disposal of obsolete transaction data with cardholder information.
- Ensure that 3rd parties (e.g. vendors, service providers) adhere to rules.
- Report security incidents immediately.

Cardholders can also take simple, common sense steps to help minimize exposure to card fraud. For example:

---

[31] "Geolocation for Internet Security." The Nilson Report, Issue #814. July 2004, p. 1.
[32] "Cardholder Information Security Program." Visa USA. URL: http://usa.visa.com/business/merchants/cisp_index.html?ep=v_sym_cisp - b.
[33] "Credit Card Firms Trying to Retain Customer Trust." Epaynews.com. May 27, 2004. URL: http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=10856747076222152l2&block=.
[34] "Joint Industry Letter Re: Merchant Requirements for Securing Cardholder Information." May 25, 2004. URL: http://www.mastercardmerchant.com/docs/Industry_Letter_FINAL.pdf.

- Only do business with reputable merchants.
- Get a card with a very low limit for use in Internet transactions.
- Consider single use card numbers (available from some issuers).

VI. Concluding remarks

If trends continue, Jupiter Research is forecasting that online sales will reach $65 billion in 2004.[35] With no significant alternative in sight, payment cards will remain the de facto payment vehicle enabling eCommerce growth. As online sales grow, so will corresponding losses due to fraud, making the need for strong authentication of cardholders greater than ever.

The card industry has made some missteps in its efforts to secure online payments. SET was arguably a technically elegant and complete solution, but by failing to approach security as a whole program (not just a technology), its market failure was inevitable. Security solutions operate in the context of tradeoffs made by all players (consumers, merchants, financial institutions, and card associations). Any solution to the cardholder authentication problem will need to consider:

- The suitability of the solution for mass-market adoption, including the public's level of tolerance for technical complexity.
- The costs to all players in terms of real dollars and convenience along with ease of use.
- The distribution of costs, incentives, and liabilities amongst all players.
- The legal framework surrounding the solution. The law rarely keeps up with the market and never keeps up with technology. For example, laws concerning the validity of 'digital signing', and distribution of financial liability (particularly where it impacts the consumer) are likely to continue to evolve.
- The fact that security is as much an education issue as a technology or process issue. This is especially true when rolling out a solution to the mass-market.

Trust and security are essential to any system of commerce. In developing solutions to improve trust and security in eCommerce payments, a technically sound solution is necessary, but far from sufficient. To be successful, an ePayments risk management program must be approached as an economic exercise that factors in relevant business processes, distribution of liability, costs, and other tradeoffs that influence program adoption.

[35] "Online Sales Sizzle in 2Q." CNNMoney. August 20, 2004. URL: http://money.cnn.com/2004/08/20/news/economy/ecommerce_sales/

VII. References

1 "After the Hype: eCommerce Payments Grow Up." Federal Reserve Bank of Philadelphia, Payment Cards Center. June 18, 2003. URL: http://www.phil.frb.org/pcc/conferences/eCPC_summary.pdf (July 19, 2004).

2 Anti-Phishing Working Group. "Phishing Attacks Trend Report." May 2004. URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf (August 4, 2004).

3 Arikan, Onur. "'SET' to Pull Down the Insecurity Barrier in Front of eCommerce." July 25, 2001. URL: http://www.sans.org/rr/papers/index.php?id=569 (July 9, 2004).

4 The Associated Press. "3 admit hacking into Lowe's computer." August 4, 2004. URL: http://seattlepi.nwsource.com/business/apbiz_story.asp?category=1310&slug=Hacking%20Charges%20L6&searchpagefrom=1 (August 4, 2004).

5 Bennett, Robert. "I didn't do it." US Banker. December 2001. URL: http://www.us-banker.com/article.html?id=2004041579NTHYMH (August 1, 2004).

6 Burns, Peter. "Fraud Management in the Credit Card Industry." Federal Reserve Bank of Philadelphia, Payment Cards Center. April 2002. URL: http://www.phil.frb.org/pcc/workshops/workshop7.pdf (July 19, 2004).

7 California. Senate. "SB 1386 Senate Bill (full text)." February 12, 2002. URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (August 5, 2004).

8 "Card FAQs." Cardweb.com. March 19, 2004. URL: http://www.cardweb.com/cardlearn/faqs/2004/march/19d.xcml (July 19, 2004).

9 "Card FAQs." Cardweb.com. November 7, 2003. URL: http://www.cardweb.com/cardlearn/faqs/2003/november/10.xcml (July 19, 2004).

10 "Cardholder Information Security Program." Visa USA. URL: http://usa.visa.com/business/merchants/cisp_index.html?ep=v_sym_cisp - b (July 21, 2004).

11 Cheney, Julia. "Identity Theft: a Pernicious and Costly Fraud." December 2003. http://www.phil.frb.org/pcc/papers/Identity_Theft.pdf (July 19, 2004).

12 Cheney, Julia. "Identity Theft: Where do we go from Here?" April 2004. URL: http://www.phil.frb.org/pcc/papers/identitytheft_0404.pdf (July 19, 2004).

13 Clark, Tim. "Visa, Mastercard try to revive SET." CNET News.com. May 12, 1999. URL: http://news.com.com/2100-1017-225723.html?legacy=cnet (July 6, 2004).

14 "Credit Card Firms Trying to Retain Customer Trust." Epaynews.com. May 27, 2004. URL: http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=1085674707622215212&block= (July 21, 2004).

15 CyberSource. "5th Annual Online Fraud Report: Credit Card Fraud Trends & Merchant Response; 2004 Edition."

16 Garfinkle, Simson. "Is the Web Set for SET?" Wired.com. June 16, 1997. URL: http://webmonkey.wired.com/packet/garfinkel/97/24/index2a.html (July 20, 2004).

17 Garfinkel, Simson and Spafford, G. "Web Security & Commerce." O'Reilly & Associates. 1997. 210-219, 313-332

18 "Geolocation for Internet Security." The Nilson Report, Issue #814. July 2004.
19 "A good Christmas for spending online with post Christmas Internet Sales Up 50 per cent but figures show attempted ecommerce fraud rose 25 per cent." Retail Decisions. January 9, 2004. URL: http://www.redplc.com/news/archive/default.msp?contentId=2092 (July 20, 2004).
20 Jewell, Mark. "ID Theft Symptom of Database Culture." August 10, 2004. URL: http://seattlepi.nwsource.com/business/apbiz_story.asp?category=1310&slug=Wholesale%20Credit%20T (August 10, 2004).
21 "Joint Industry Letter Re: Merchant Requirements for Securing Cardholder Information." May 25, 2004. URL: http://www.mastercardmerchant.com/docs/Industry_Letter_FINAL.pdf (8/11/04).
22 Litan, Avivah. "Consumers Embrace Online Credit Card Security Systems." Gartner Group. February 15, 2002. URL: http://www4.gartner.com/DisplayDocument?doc_cd=104547 (July 20, 2004).
23 "MasterCard Launches Mastercard SecureCode --New Global E-Commerce Security Solution For Consumers." MasterCard International. September 23, 2002. URL: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=653&category=keyword&keyword=securecode (August 9, 2004).
24 Mearian, Lucas. "System break-in nets hackers 8 million credit card numbers." Computerworld. February 24, 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,78747,00.html (July 20, 2004).
25 Mearian, Lucas. "Visa sets technical specifications for online authentication." Computerworld. June 29, 2001. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,61789,00.html (August 9, 2004).
26 Merkow, Mark. "Mastercard's Response to the Online Payments Quandary." internet.com. January 10, 2002. URL: http://ecommerce.internet.com/news/insights/outlook/article/0,3371,10535_952181,00.html (August 9, 2004).
27 Netscape DevEdge, "Introduction to SSL." October 9, 1998. URL: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm (July 21, 2004).
28 Netscape. "The SSL Protocol Version 3.0." March 1996, URL: http://wp.netscape.com/eng/ssl3/ssl-toc.html (July 21, 2004).
29 "OnGuard Fraud Management Solutions." Paymentech. URL: http://www.paymentech.com/pdf/OnGuard.pdf (August 22, 2004).
30 "Online Sales Sizzle in 2Q." CNNMoney. August 20, 2004. URL: http://money.cnn.com/2004/08/20/news/economy/ecommerce_sales/ (August 25, 2004).
31 "Quarterly retail e-commerce estimates." US Department of Commerce News. May 21, 2004. URL: http://www.census.gov/mrts/www/current.html (July 28, 2004).
32 Roberts, Bill. "On you mark, get SET, wait!" Datamation. April 1, 1998. URL: http://itmanagement.earthweb.com/secu/article.php/602391 (July 6, 2004).
33 "Secure Card Payments on the Internet, Addendum." European Committee for

Banking Standards. 3/03. URL: http://www.ecbs.org/Download/TR410_ADD_V1.PDF (August 9, 2004).
34 "Security Essentials Book 1.2 Defense-in-depth." The SANS Institute. Ch 8, p.123-125; Ch 12, p.357-370.
35 "SET Secure Electronic Transaction Specification, Book 2 Programmers Guide, Version 1.0." (May 31, 1997).
36 Sienkiewicz, Stanley. "The Future of eCommerce Payments." Federal Reserve Bank of Philadelphia, Payment Cards Center. April 2002. URL: http://www.phil.frb.org/pcc/conferences/futurepayments0902.pdf (July 19, 2004).
37 Sorbel, Josh. "Identity Theft and E-commerce Web Security: A Primer for Small to Medium Sized Businesses." November 24, 2003. URL: http://www.giac.org/practical/GSEC/Josh_Sorbel_GSEC.pdf (July 9. 2004).
38 Steeley, Oliver. "Guaranteed Transactions, the Quest for the 'Holy Grail'." ePSO - ePayments System Observatory Newsletter, number 10. November 2001. URL: http://epso.jrc.es/newsletter/vol10/docs/ePSO-N10.pdf (July 20, 2004).
39 Sullivan, Bob. "BJ's Wholesale suspects credit card leak." MSNBC.com. March 12, 2004. URL: http://www.msnbc.msn.com/id/4516301/ (July 20, 2004).
40 Tebbutt, Dan. "Ready, SET, stop." Australian Personal Computer Magazine. March 3, 1999. http://www.apcmag.com/apc/v3.nsf/0/568A421986B443CBCA256D44001AD58D (July 19, 2004).
41 "3-D Secure Introduction, Version 1.0.2." Visa International. September 26, 2002. URL: http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf (August 9, 2004).
42 "3-D Secure System Overview, Version 1.0.2." Visa International. May 1, 2003. URL: http://international.visa.com/fb/paytech/secure/pdfs/3DS_70015-01_System_Overview_external_v1.0.2_May_2003.pdf (August 9, 2004).
43 The Tower Group. "An Introduction to Secure Electronic Transactions." April 1998.
44 United States. U.S. District Court. "Decision. UNITED STATES OF AMERICA, Plaintiff, vs. VISA U.S.A. INC., VISA INTERNATIONAL CORP., AND MASTERCARD INTERNATIONAL INCORPORATED, Defendants." October 9, 2001. URL: http://www.usdoj.gov/atr/cases/f9800/9857.htm (July 21, 2004).

Last Updated: May 30th, 2017

Upcoming Training

Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 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 Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
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	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event