Session # 50
Enable Secure Web Commerce Applications
Michael T. Raggo, CISSP, CCSA, CCSE, CCSI, MCP

Michael T. Raggo is a Senior Security Consultant for VeriSign, Inc. He is an instructor for VeriSign’s security classes including Strategic E-Commerce Architecture and Security, Check Point Firewall-1, Applied Hacking & Countermeasures, and Open Source Security Tools. Mr. Raggo is also a consultant with an extensive background in Firewalls, Security Assessments, Web Server security, SSL, PKI, and Intrusion Detection Systems.

Prior to joining VeriSign, Mr. Raggo was Supervisor of System Administration for www.nasdaq.com at the NASDAQ Stock Market. Mr. Raggo also has 15 years experience as a UNIX System Administrator.
Enabling Secure Web Commerce Applications

Session Number 50
Michael T. Raggo
Wednesday, August 8, 2001
8:30-10:00AM
Key Points

Types of E-Commerce Sites
Secure Web Transport Protocols
Secure Transaction Protocols
Types Of E-Commerce

Where is E-Commerce today?
Current State of E-commerce

2000 / 2001
Is E-Commerce growing? You bet!

- In the US, 36 million people went online and spent on average $304.00
  - 54% increase from the year before.
- A total of $10 billion dollars was spent online in 2000 (Jupiter Media Metrix)
  - Of these consumers 90% were very satisfied with their online shopping experience.
- Internationally, $132B was generated by E-Commerce in 2000 (Active Media Research)
Prediction?

In 1998, International Data Corporation (IDC) predicted that online spending would reach $100B by the end of 2000.

- They were wrong. We hit $100B in 1999.
- Why were they wrong?

They didn’t account for B2B E-Commerce.
How big is the B2B market?


Source: the Yankee Group, 2000
E-Commerce and PKI

Public Key Infrastructure
Welcome to Cyberspace...
The House of E-Commerce

Reliable E-Commerce

Technology
- Authentication
- Privacy
- Authorization
- Integrity of Data
- Non-repudiation

Management

Security Infrastructure

Security Policies
Elements of Secure E-Commerce

Privacy
Integrity
Non-Repudiation
Authorization
Authentication

Digital Signature
Private Key

John Hancock

Elements include:
- Encryption
- Privacy
- Integrity
- Non-Repudiation
- Authorization
- Authentication
Security Principles for E-Commerce

A PAIN ....

**A**uthentication
Know who you’re communicating with

**P**rivacy (Confidentiality)
Protect sensitive information

**A**uthorization
Ensure users do not exceed their authority

**I**ntegrity (of the Data)
Prevent tampering or alteration to information

**N**on-Repudiation
Produce legally binding evidence of transactions
The Challenge: Alleviate A PAIN

How do we apply these principles to e-commerce?

- Authentication and Authorization
  - The element of anonymity is an invitation to commit fraud
  - Who’s on the other end of the line?

- Privacy
  - Most Internet data is written and transmitted in clear text. (SMTP, HTTP, POP3, etc.)
  - How do we make it unreadable?
The Challenge: Alleviate A PAIN

– Integrity of Data
  • Data can be intercepted and changed
  • How can we ensure integrity?

– Non-Repudiation
  • How to “tie” a message to the sender
  • How can we sign a message?
Digital Authentication

- Authentication and Authorization
  - The element of anonymity is an invitation to commit fraud
  - Who’s on the other end of the line?
Digital Authentication

Criteria

- It must uniquely identify that individual or entity
- It must be verifiable by the other party or third parties
- It must allow a party to “sign” an electronic document as easily as a paper document
- It must provide a high level of protection against impersonation or tampering
- It must be viewable by anyone, yet not forgeable
Digital Authorization

Authorization is the process of determining the actual capabilities of an authenticated user

- Can the user view salaries in the HR system? Or change salaries?

Once a user is authenticated, authorization is normally an application-level decision
Privacy = Encryption

Privacy
- Most Internet data is written and transmitted in clear text. (SMTP, HTTP, POP3, etc.)
- How do we make the data unintelligible, except to the intended recipient(s)?

Encryption
- It must be built in to standard client applications
- It must provide a high-level of protection against forgery and misuse
Data Integrity Across the Internet

- It is necessary to ensure that data cannot be altered in transit

- Unauthorized changes must be immediately detectable

- Tie a checksum to the sender’s signature
Non Repudiation Criteria

We must securely bind the user’s digital identity to their physical identity

- The Digital ID is bound to the digital signature
Digital Certificate = Digital ID

An electronic document whose validity is guaranteed by a trusted third party.
The House of E-Commerce

Reliable E-Commerce

Technology
- Authentication
- Privacy
- Authorization
- Integrity of Data
- Non-Repudiation

Security Infrastructure

Management

Security Policies

© 2001 Verisign Inc.
Secure Transport Protocols

SSL
What is SSL?

SSL is Secure Sockets Layer.

- It is the most commonly used protocol for encrypting communications between browsers and servers and is freely available in most browsers.
Defense:
Secure Sockets Layer (SSL)

- Originally designed by Netscape
- SSL 2.0 introduced Dec 1994;
- SSL 3.0 in Nov 1995
- Now standardized under the IETF as TLS 1.0 (transport layer security)
SSL Characteristics

- A web server running in SSL mode typically uses port 443 for encrypted communications.
- When used with HTTP, requires a dedicated TCP/IP socket.
SSL Characteristics

- Application and platform independent
- Program layer between application protocols (http, telnet, FTP, NNTP) and TCP/IP
- Can be modified to be used by any TCP program
- Open, non-proprietary

Web Applications

<table>
<thead>
<tr>
<th>HTTP</th>
<th>FTP</th>
<th>SMTP</th>
<th>NNTP</th>
<th>New Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SSL

TCP/IP
What is encrypted?

Once the SSL connection has been established, the following communications are encrypted:

- URL of requested document
- Contents of requested document
- Contents of any forms the client has filled-out
- Cookies
- HTTP header contents
A Secure Server

We are confident of our system’s ability to protect all transactions; however, this is not an invitation for people to attempt unauthorized access to the system. This is a private computing system which is restricted to authorized individuals. Actual or attempted unauthorized use of this computer system will result in criminal and/or civil prosecution. We reserve the right to view, monitor, and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing, or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system if you...

The Server’s Certificate, 1

This page was encrypted. This means it was difficult for other people to view this page when it was loaded.

This Certificate belongs to: vault.snic.com
Financial Services
ALLTEL Information Services
Atlanta, Georgia, US
This Certificate is valid from Tue Nov 04, 1997 to Thu Nov 05, 1998
Certificate Fingerprint:
Welcome to SFNB has the following structure:

- **https://vault.sfnb.com/cgi-bin/accentSum**
  - Background Image: **https://vault.sfnb.com/vfnb/images/bkground.gif**
  - Form 1:
    - Action URL: **https://vault.sfnb.com/cgi-bin/accentSum**
    - Encoding: `application/x-www-form-urlencoded` (default)
    - Method: POST

### Netsite: https://vault.sfnb.com/cgi-bin/accentSum

**File MIME Type:** text/html

**Source:** Currently in memory cache

**Local cache file:** none

**Last Modified:** Unknown

**Content Length:** 2991

**Expires:** No date given

**Charset:** Unknown

**Security:** This is a secure document that uses a medium-grade encryption key suited for U.S. export (RC4-40, 128 bit with 40 secret).

<table>
<thead>
<tr>
<th>Certificate</th>
<th>This Certificate belongs to: vault.sfnb.com, Financial Services, MIS Information Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This Certificate was issued by: Secure Server Certification Authority, RSA Data Security, Inc.</td>
</tr>
</tbody>
</table>
SSL 3.0

- Bidirectional; client can optionally also have a certificate
- Server has the option to require a client cert.
- Allows key exchange methods other than RSA
Transport Layer Security, TLS

- IETF’s standard protocol for http security
- Will definitely be based on SSL 3.0
- May include Kerberos authentication from MIT
- Currently at TLS 1.0
SSL Handshake Protocol

Client initiates connection

Server responds by sending its certificate.

Client verifies the server’s cert and may send its own cert if requested

Client sends the server a random session key encrypted with the server’s public key

Client and server use the shared key to encrypt/decrypt data over the secure channel

Client

Server
Cipher Suite

- A Cipher Suite is the combination of the symmetric encryption algorithm, message digest method, and authentication.

- When an SSL enabled client initiates a connection with a web server, they negotiate a cipher suite. The mutually agree on the strongest encryption method that they both support.
Cipher Suite

Symmetric Encryption
- DES (40 & 56 bit),
- 3DES (168),
- RC4 (40 & 128)

Message Digest
- MD5 or SHA-1

Authentication
- RSA public keys and certificates OR Diffie-Hellman for anonymous mode
But can you export 128-bit encryption???

In January 2000, the United States dramatically relaxed its export regulations, most importantly 128-Bit Encryption.
Regulatory

“Today, any cryptographic product is exportable under a license exception (that is, without a license) unless the end-users are foreign governments or embargoed destinations (Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Talisman-controlled areas of Afghanistan as of January 2000). Export to government end-users may also be approved, but under a license.”

Source RSA Security http://www.rsasecurity.com/rsalabs/faq/6-4.html

More info. can be found at the Bureau for Export Administration at www.bxa.doc.gov
Strength of Encryption Key Lengths

40-Bit Key
   About 3.5 hours to break code

56-Bit Key
   About 22 hours to break code

64-Bit Key
   About 33 days to break code

128-Bit Key
   About 2000 years to break code
How Server Authentication Is Being Used

VeriSign has issued more than 575,000 server certificates

Using sites:

- Web publishers, retailers
- Anyone requiring presentation of passwords, credit cards, etc.
- On-line banking
- Information vendors
SSL 3.0 Server Certificates

Server has a key pair and certificate
Server is authenticated to clients
  - Prevents server spoofing
The server’s key pair is used to establish symmetric keys to encrypt and integrity-check session
Implemented in 2.0 browsers
Server Authentication Method

Client

- Generate random secret
- Encrypt with server’s public key

Certificate

Server

- Decrypt with server’s private key
- Shared random secret

Encrypted secret
SSL With Client Certificates

- Client has a key pair and certificate
- Client is authenticated to the server (and vice-versa)
- More secure and manageable than passwords, cookies
- Implemented in version 3.0 (and higher) browsers
Client Authentication Method

Client

Certificate

Server

Digitally sign handshake history

Signature over handshake history

Verify digital signature

Server still handles the encryption – this is for authentication only
CA Certificates - Netscape Navigator

Go To:
Security Signers
CA Certificates - Internet

Go to:
View Internet Options Content Certificates
SSL Configuration Tip

Select Require 128-bit and eliminate 40-bit encryption support.
SSL 2.0

SSL 2.0 can be attacked: (rollback attack)
- SSL 2.0 can be forced to use a weaker encryption algorithm than you specify, which can then be brute force attacked

SSL 2.0 is also vulnerable to various spoofing attacks

Note: DISABLE SSL 2.0 Support on your web server!!!
Netscape/iPlanet SSL Configuration Tip

Turn off SSL 2.0
Prevents SSL spoofing

- Allow:
  - SSL version 2
  - SSL version 3

SSL 2.0 ciphers:
- RC4 with 128 bit encryption and MD5 message authentication
- RC4 with 40 bit encryption and MD5 message authentication
- RC2 with 128 bit encryption and MD5 message authentication
- RC2 with 40 bit encryption and MD5 message authentication
- DES with 56 bit encryption and MD5 message authentication
- Triple DES with 168 bit encryption and MD5 message authentication

SSL 3.0 ciphers:
- RC4 with 128 bit encryption and MD5 message authentication
- RC4 with 40 bit encryption and MD5 message authentication
- Triple DES with 168 bit encryption and SHA message authentication
- DES with 56 bit encryption and SHA message authentication
- RC2 with 40 bit encryption and MD5 message authentication
- No encryption, only MD5 message authentication
SSL 3.0 Protection

SSL V3.0 protection services:
- authentication of server to client
- (optionally) authentication of client to server
- confidentiality via symmetric encryption
- integrity check value on all data transferred

Based on public key technology and certificates
Different encryption algorithms can be negotiated
Makes certificates easy to use
- Virtually “invisible” to the user
- Certificates are simply added to the browser
SSL: Meeting The Five Pillars

Privacy
- Client generates a master key and sends it to the server using the server’s public key
- Master key used to generate 2 session keys (1 for each direction)
- All traffic is encrypted with the symmetric keys
- Transparent to all higher level protocols

Authentication and Integrity
- Server’s certificate authenticates the server
- Optional client certificate
- Record sequence number to ensure no illegal replays

NOTE: SSL does not provide for digital signature
The House of E-Commerce

Reliable E-Commerce

Technology
- Application
- A

Security Infrastructure
- Authorization
- Security
- Non-Repudiation

Management
- Security Policies

© 2001 Verisign Inc.
Secure Transactions

SET
What about Authorization and Non-Repudiation?

Authorization is usually provided at the application level
Non-repudiation – digitally sign a transaction
Secure Transactions

- SSL provides secure communications between Web server and client.
- However, it does not provide the ability to securely transfer payments between the merchant and the bank.
SET – Secure Electronic Transactions

- Originally developed January 1996 by MasterCard, Visa, Netscape, Microsoft, GTE, IBM, VeriSign, and other companies.
- It was originally designed to secure card payments over the Internet between merchant sites and processing banks.
- SET is managed and promoted by the SETCo consortium (www.setco.org).
SET (Secure Electronic Transaction) was also designed to address some of the problems with SSL
- Checking the credit card number for validity
- Validating the user is authorized to use the credit card
- Authorizing the transaction with the user’s bank
- Processing the transaction
SET

Protocol Stack

Payment Protocols
(SET, CyberCash, First Virtual, ...)

S-HTTP, HTTP, S/MIME, telnet, mail, news, ftp, ntp, dns, and others

Secure Sockets Layer

Transport Control Protocol

Internet Protocol

Data Link Layer
SET – Secure Electronic Transactions

Primary Participants
- Issuer
- Cardholder
- Merchant
- Acquirer (supports merchants with a service that provides processing of bank card transactions)

Secondary Participants
- Payment Gateway (authorization and capture of transactions, operated by acquirer or 3rd party)
- Certification Authorities
Payments

- Consumer
- Payment Gateway
- Financial Networks
- Issuer
- Aquirer
- Merchant

1. The consumer initiates a payment transaction on the internet.
2. The transaction is routed through the payment gateway.
3. The payment gateway communicates with the financial networks.
4. The financial networks connect with the issuer and the acquiring bank.

This diagram illustrates the process of online payments.
SET Services

Authentication (user and merchant)
- Digital signatures

Confidentiality
- Encryption

Integrity – for all transmitted data
- MessageDigests

Non-repudiation – for the consumer

Authorization
The House of E-Commerce

Reliable E-Commerce

Security Infrastructure

Security Policies

Management

Technology

Authentication
Authorization
Confidentiality
Integrity
Non-repudiation

© 2001 Verisign Inc.
Deployment of SET has been limited. So far, it has not attracted a large number of merchants. Currently, 80% of SET deployments are in Asian and European countries. Reasons for lack of deployment include costs and difficulty of installation.
Currently, most vendors still have proprietary solutions for providing secure payments:

- VeriSign PayFlow
- CyberCash
- Netegrity
XKMS

- XKMS (XML Key Management Specification) is an open standard that VeriSign co-authored with Microsoft and WebMethods.
- XKMS defines XML-based transactions for managing public keys in support of digital signature and encryption functions
- Ideal for mobile devices

http://www.verisign.com/developer/xml/xkms.html
S2ML (Security Services Markup Language) is a specification developed by VeriSign, Netegrity and others to solve the problem of how B2C and B2B transactions

S2ML defines XML-based transactions for conveying information regarding the privileges or entitlements of people or organizations between different sites

http://www.verisign.com/rsc/wp/xml/s2ml/s2ml_wp.pdf
http://www.s2ml.org/
XKMS & S2ML

XKMS and S2ML are totally complementary. For example, a business might use XKMS in verifying a digitally signed transaction, then use S2ML to learn more about the business credentials, e.g., credit rating, of the signer.
Summary

Building a successful E-Commerce site is by no means a single person job. It requires knowledge, research and a game plan. Hopefully this presentation will guide you in the correct direction toward building that secure E-Commerce site.
Reference Guides

Administrating Web Servers, Security and Maintenance
by Eric Larson, Brian Stephens (December 15, 1999)

E-Commerce Security
By Anup K. Ghosh (1998)

Electronic Commerce
By Gary Schneider, James Perry (2000)

Electronic Commerce – Security, Risk Management and Control
By Marilyn Greenstein, Todd Feinman (2000)

Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption
by Warwick Ford, Michael S. Baum (April 1997)

SSL and TLS Essentials
By Stephen Thomas (2000)