Web Security

Dr. Arjan Durresi Louisiana State University Baton Rouge, LA 70810 Durresi@csc.lsu.Edu

These slides are available at:

http://www.csc.lsu.edu/~durresi/csc4601-04/

Louisiana State University

18- Web Security - 1

CSC4601 F04

How the Web Works: Other Elements

- ☐ Hyper-text markup language (html).
- Other application specific document.
 - E.G., MIME, graphics, video/audio, postscript, Java applets, etc.
- Browsers.
 - o Display html documents and embedded graphics.
 - O Run Java program.
 - Start helper applications.

o ...

Louisiana State University

18- Web Security - 4

CSC4601 F04



- How web works
- □ Threats
- SSL, Architecture, protocols
- □ TLS
- □ SET

Louisiana State University

18- Web Security - 2

CSC4601 F04

Web Security

- □ http://www.w3.org/Security/Faq
- □ Web now widely used by business, government, individuals
- ☐ But Internet & Web are vulnerable
- Have a variety of threats
 - integrity
 - o Confidentiality Revealing private information on server
 - o denial of service
 - o Authentication Execute unauthorized programs
- Need added security mechanisms

Louisiana State Universi

18- Web Security - 5

CSC4601 F04

How the Web Works - HTTP

- □ Hypertext transfer protocol (http).
- □ Clients request "documents" (or scripts) through URL.
- □ Server response with "documents".
- □ Documents are not interpreted by http.
- □ Stateless protocol, request are independent.

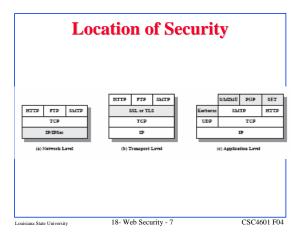
Threats

	Threats	Consequences	Countermeasures
Integrity	Modification of user data Trojan horse browser Modification of memory Modification of message traffic in teamit	Less of information Compromise of machine Vulnerability to all other threats	Cryptographic checksums
Confidentiality	Eavesdropping on the Net Theft of info from server Theft of data from client Info about network configuration Info about which client talks to server	*Loss of information *Loss of privacy	Encryption, web proxies
Denial of Service	Killing of user threads Flooding machine with bogus requests Filling up disk or memory Isolating machine by DNS attacks	Distraptive Annoying Prevent user from getting work done	Difficult to prevent
Authentication	Impersonation of legitimate users Data forgery	Misrepresentation of user Belief that false information is valid.	Cryptographic techniques

Louisiana State University 18- Web Security - 3 CSC4601 F04

na State University 18- Web Security - 6

CSC4601 F04



SSL Architecture

■ SSL session

- o an association between client & server
- o created by the Handshake Protocol
- o define a set of cryptographic parameters
- o may be shared by multiple SSL connections
- Once established operating state
- o During Handshake Protocol pending read, write states

□ SSL connection

- o a transient, peer-to-peer, communications link
- o associated with 1 SSL session

misiana State University

18- Web Security - 10

CSC4601 F04

SSL (Secure Socket Layer)

- □ Transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS (Transport Layer Security)
- uses TCP to provide a reliable end-to-end service
- □ SSL has two layers of protocols
 - SSL record protocol provides basic security services
 - o 3 higher-layer protocols:
 - □ Handshake, change cipher spec, alert

SSL Architecture

Louisiana State University

18- Web Security - 8

CSC4601 F04

CSC4601 F04

Session and Connection

- Session parameters:
 - ID, peer certificate, compression method, cipher spec, master secret, is resumable.
- Connection parameters:
 - Server and client random, server write MAC secret, client write MAC secret, server write key, client write key, IV, sequence number.

ouisiana State Universit

18- Web Security - 11

CSC4601 F04

SSL Handshake Cipher Spec Protocol Protocol SSL Record Protocol TCP

IP

Louisiana State University 18- Web Security - 9

Confidentiality

 using symmetric encryption with a shared secret key defined by Handshake Protocol

SSL Record Protocol

- o IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
- o message is compressed before encryption
- Message integrity
 - o using a MAC with shared secret key
 - o similar to HMAC but with different padding

Louisiana State University 18- Web Security - 12 CSC4601 F04

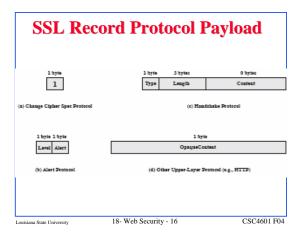
SSL Record Protocol

- Layered protocol:
 - Fragment application data into blocks
 - Compress data
 - Apply message authentication code (MAC) = h(m|s) for message m and secret s
 - Encrypt with client (cw) or server (sw) write key
 - o Transmit over TCP
- □ Specify content type for higher protocols

Louisiana State University

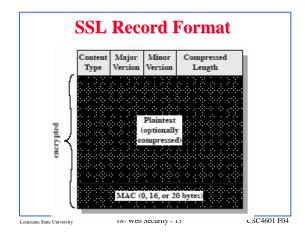
18- Web Security - 13

CSC4601 F04



SSL Record Protocol Operation Application Data Fragment Compress Add MAC Encrypt Append SSL Record Header Louisians State University 18- Web Security - 14 CSC4601 F04

SSL Change Cipher Spec Protocol One of 3 SSL specific protocols which use the SSL Record protocol A single message Causes pending state to become current Hence updating the cipher suite in use



SSL Alert Protocol Conveys SSL-related alerts to peer entity Severity warning or fatal Specific alert unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown Compressed & encrypted like all SSL data

SSL Handshake Protocol

- □ Allows server & client to:
 - o authenticate each other
 - o to negotiate encryption & MAC algorithms
 - o to negotiate cryptographic keys to be used
- ☐ It is used before any application data is transmitted
- Comprises a series of messages in phases
 - Establish Security Capabilities
 - o Server Authentication and Key Exchange
 - o Client Authentication and Key Exchange
 - Finish

Louisiana State University

18- Web Security - 19

CSC4601 F04

SSL Handshake Protocol Message Types

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

ana State University 18- Web Security - 22

CSC4601 F04

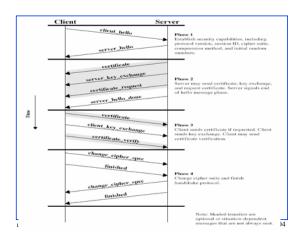
Establish Security Capabilities

- Used to initiate a logical connection and to establish the security capabilities associated with it
- ☐ Initiated by client **client_hello_message**, parameters:
 - Version the highest SSL version understood by the client
 - Random 32-bit timestamp and 28 bytes random, serve as nonce
 - Session ID a variable length Session ID. A nonzero value indicates the client wants to update existing connection.
 Zero – new one
 - CipherSuite list of combinations of cryptographic algorithms supporte by client in decreasing order of preference
 - o Compression method list supported methods

Louisiana State University

18- Web Security - 20

CSC4601 F04



Establish Security Capabilities

- ☐ The server responds with **server_hello** message with the same parameters as the client_hello
 - Version
 - o Random independent of client
 - Session ID
 - CipherSuite the single cipher selected
 - Compression the method selected

Server Authentication and Key Exchange

- □ Server begins this phase by sending its certificates
- Next sender server sends a server_key_exchange message (not sent if a certificate with fixed DH was sent or when RSA will be used)
- □ Next a nonanonymous server (server not using DH) can request a certificate from the client
- ☐ Final message **server_done** message

Louisiana State University 18- Web Security - 21 CSC4601 F04 Louisiana State University 18- Web Security - 24 CSC4601 F04

Client Authentication and Key Exchange

- Client verifies the certificate of server and the parameters are acceptable
- ☐ If server has requested a certificate, the client sends it with a **certificate** message.
- □ Next client_key_exchange_message
- ☐ Finally the client sends a **certificate_verify** message
- To provide explicit verification of a client certificate (following any client certificate with signing capability)

Louisiana State University

18- Web Security - 25

CSC4601 F04

Cryptographic Computations: Details (1)

- \square Client generates a 48-byte pre-master-secret s_n
- Master secret:
 - o s_m =MD5(s_p |SHA('A'| $s_p | r_c | r_s$)) | MD5(s_p |SHA('BB'| $s_p | r_c | r_s$)) | MD5(s_p |SHA('CCC'| $s_p | r_c | r_s$))
 - Where r_c : client, server random

Louisiana State University

18- Web Security - 28

CSC4601 F04

Finish

- Client send change_cipher_spec
- ☐ Then **finished message** using the new key

Louisiana State University

18- Web Security - 26

CSC4601 F04

Cryptographic Computations: Details (2)

- □ Session key: same as above, but use the master secret in place of s_p to generate byte stream to cut out:
 - o Client, server MAC secret
 - o Client, server write key
 - o Client, server IV

Louisiana State Universi

18- Web Security - 29

CSC4601 F04

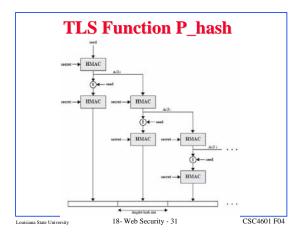
Cryptographic Computations

- Master secret creation
 - A pre-master-secret is exchanged first.
 - RSA, or Diffie-Hellman.
 - Both sides compute master secret based on premaster-secret.
- ☐ Generation of cryptographic parameters.
 - Client/server write MAC secrets, client/server write keys, client/server write IV are generated from master secret.

TLS (Transport Layer Security)

- □ IETF standard RFC 2246 similar to SSLv3
- with minor differences
 - o in record format version number
 - o uses HMAC for MAC
 - o a pseudo-random function expands secrets
 - o has additional alert codes
 - o some changes in supported ciphers
 - o changes in certificate negotiations
 - o changes in use of padding

Louisiana State University 18- Web Security - 27 CSC4601 F04 Louisiana State University 18- Web Security - 30 CSC4601 F04



Key Features of SET

- Confidentiality of information using DES:
 - Cardholder account and payment information is secured over the network
 - Prevents merchant from learning the cardholder's credit card number, which is only provided to the issuing hank
- Integrity of data using RSA digital signatures, SHA-1 hash:
 - Payment information: order information, personal data and payment instructions
- Cardholder account authentication using X.509v3 digital certificates with RSA signatures – merchant verify that a cardholder is a legitimate user of a valid credit card
- Merchant authentication cardholder verify that a merchant has a relationship with a financial institution allowing it to accept payment cards

Louisiana State University

18- Web Security - 34

CSC4601 F04

Secure Electronic Transactions (SET)

- Open encryption & security specification
- To protect Internet credit card transactions
- □ Developed in 1996 by Mastercard, Visa etc
- □ Not a payment system
- □ Rather a set of security protocols & formats
- SET provides:
 - Secure communications amongst parties
 - Trust from use of X.509v3 certificates
 - o Privacy by restricted info to those who need it

Louisiana State University

18- Web Security - 32

CSC4601 F04

SET Components Merchant Internet Cardholder Certificate Authority Payment Gateway 18- Web Security - 35 CSC4601 F04

Business Requirements for SET

- Confidentiality of payment and ordering information use encryption
- □ Integrity of all transmitted data use digital signatures
- Authentication of cardholder use digital signatures and certificates
- Authentication that a merchant can accept credit card transactions - use digital signatures and certificates
- Ensure the use of the best security practices and system design techniques
- Neither depends on transport security nor prevent their use (IPSec, SSL/TLS)
- ☐ Facilitate interoperability among software and network protocols independent of hardware, software platforms

SET Transaction

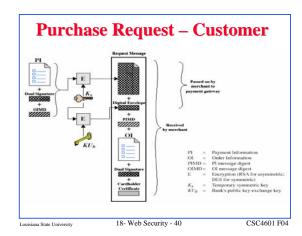
- . Customer opens account
- Customer receives a certificate X.509v3 digital certificate signed by the bank. The certificate verifies the customer's RSA public key and its expiration date.
- Merchants have their own certificates one for the public key to sign messages and the other for key exchange
- 4. Customer places an order
- Merchant is verified
- 6. Order and payment are sent the payment information cannot be read by the merchant
- Merchant requests payment authorization from payment gateway
- 8. Merchant confirms order
- 9. Merchant provides goods or service
- 10. Merchant requests payment

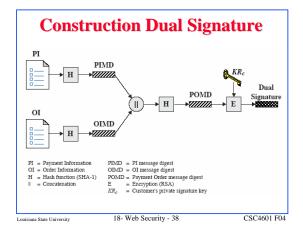
Louisiana State University 18- Web Security - 33 CSC4601 F04 Louisiana State University 18- Web Security - 36 CSC4601 F04

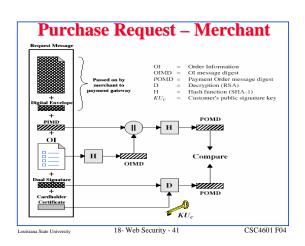
Dual Signature

- Customer creates dual messages o order information (OI) for merchant

o payment information (PI) for bank ■ Neither party needs details of other □ But **must** know they are linked □ Use a dual signature for this o signed concatenated hashes of OI & PI 18- Web Security - 37 CSC4601 F04







mencaps to menchants. Merchant require with a CA hadron they can exchange a Marchant require with a CA hadron they can exchange a Marchant require with a CA hadron they can exchange a Marchant require with a Canada and Approximate pole very to the Canada and Approximate pole very to the Canada and Approximate pole very to the Approx	Cardholder registration	Cardholders must register with a CA before they can send SET
Proclaime respects Menage from construent to menchane containing of the matchester Perpanent andirectations Rhough from continuent to menchane condition of the matchester Perpanent andirectations Rhough feweres menchane and prynomest generally is understore as given amount of an expendent on a given conflict cash account. Perpanent copiere Allows the menchanet to require proprient from the prynomest general and proprient and proprient and proprient and proprient from the prynomest general and proprient and proprient from the prynomest general and proprient from the proprient and proprient from the control of the conflictation approprient from the proprient from t		
By meant and receivation. Exchange between searchant and poyment games you subscribe a between the property of the control of the property of the control of the property of	Merchant registration	
given miscount for a preclaime on a given coulds can decrease. Allows the measurement to reposite prepared from the purposent of the control	Purchase request	Message from customer to merchant containing OI for merchant and PI for bonk.
Certificate inquiry and status If the CA to unable to complete the processing of a certificate uniform of the complete to the complete the processing of a certificate uniform of the certificate of the complete to the conference of the certificate curricular and the certificate of the superior to character flowers for certificate certificates of the superior to character flowers for certificate processing to the superior to character flowers for certificate of the superior flowers for certificate of the superior flowers for the certificate of the conference of the conf	Phymeut authorization	Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.
expense quickly, in vital sands apoly in the cambolisher or assertant carbolisher aroundate student face critical polysis sessing to carbolisher aroundate student face critical polysis sessing to determine the union of the everlican engine and so review the control of the everlican engine and to review the determine the control of the everlican engine and to review the control of the everlican engine and the everlican engine and everlicant control of the everlicant engine and everlicant engine and color for the precisions engines to the processing of an other face for the precisions engines to the processing of an other face for the everlicant engine and everlicant engine to be control of the conference and everlicant engines. If the color will not be completed, the event of extended could, as a face of the vital or the conference and event and event and control of the event event of the event of the color of the event of the event of the event of the control of the event event of the event of the conference and the control of the event of the event of the event of the event of the control of the event of the event of the event of the event of the control of the event of the event of the event of the event of the control of the event of the event of the event of the event of the control of the event of the event of the event of the event of the control of the event of the event of the event of the event of the control of the event of the even of the event of the event of the event of the event of the even of the event of the event of the event of the event of the even of the event of the event of the event of the event of the even of the event of the event of the event of the event of the even of the event of the event of the event of the event of the even	Phymeut capture	
other fart the proclase response to the best received. Note that the best control proclase of the proclase response to the best control proclase. And the proclase of the proc	Certificate inquiry and state	request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the Certificate Inquiry message to determine the status of the certificate request and to receive the
the other will an the completed, the amendment reversors the enter admixtration. But period for the first will not be completed (text) and interesting the control of the admixtration of the completed (text) and control of the admixtration. Control of the admixtration. Allows a summature content control control of the control of the admixtration of the proposed preserve produced progress an annual produced progress an annual processor of the admixtration of the	Purchase inquiry	order after the purchase response has been received. Note that this message does not include information such as the stams of back ordered goods, but does indicate the status of authorization.
Transaction amounts that were entered increasely by a clerk. Allows a merchant to insear a certifit or entrolledar's account and a contract of the contract o	Authorization reversal	the order will not be completed, the merchant reverses the entire authorization. If part of the order will not be completed (such as when poods are back ordered), the merchant reverses out of the
such as whose goods are personned or were changed designed to the property of the sensible, and the carbifolder. All commissations between the conflicted are found that present in a certain breage. Credit reversal. Allows a number to control preserving repeat conficient property and sensitive and conficient property conficient property and sensitive and property property conficient property confic	Capture reversal	Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
Proposate gamery certificate and prices a membrane to query the growther gamery and involve a copy of the gamery, a source for growther gamery and singularities copy of the gamery a source for gamery and singularities and gamery and singularities and gamery and singularities and gamery ga	Credit	such as when goods are returned or were damaged during shipping. Note that the SET Credit message is always initiated by the merchant, not the cardholder. All communications between the cardholder and merchant that result in a credit being
teriport copy of the parently is criter to be pre-taking and signature extensions. Block administration Advers a sarchine to communicate information to the portneral figure message. Error message Solution of content verification in a message become it fight female or content verification ten.	Credit reversal	Allows a merchant to correct a previously request credit.
geneway reperfulge merchant bundles. Extre message backease that a required rejects a message because it fails foreast or content vertification texts.	Payment gateway certificat request	copy of the gateway's current key-exchange and signature
format or content verification tests.	Batch administration	Allows a merchant to communicate information to the payment gateway regarding merchant batches.
	Error message	Indicates that a responder rejects a message because it fails format or content verification tests.
as State University 18- Web Security - 39	40	- Web Security - 39

Purchase Request – Merchant

- 1. Verifies cardholder certificates using CA sigs
- 2. Verifies dual signature using customer's public signature key to ensure order has not been tampered with in transit & that it was signed using cardholder's private signature key
 - $H(PIMD\|H(OI))$ and $D_{KUC}[DS]$ if they are equal
- Processes order and forwards the payment information to the payment gateway for authorization (described later)
- Sends a purchase response to cardholder

CSC4601 F04 18- Web Security - 42 Louisiana State University

Payment Gateway Authorization

- 1. Verifies all certificates
- Decrypts digital envelope of authorization block to obtain symmetric key & then decrypts authorization block
- 3. Verifies merchant's signature on authorization block $H(H(PI)||OIMD \text{ and } D_{KUC}[DS]$ if they are equal
- Decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
- 5. Verifies dual signature on payment block
- 6. Verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
- 7. Requests & receives an authorization from issuer
- 8. Sends authorization response back to merchant

Louisiana State University

18- Web Security - 43

CSC4601 F04

Payment Capture

- Merchant sends payment gateway a payment capture request
- ☐ Gateway checks request
- Then causes funds to be transferred to merchants account
- □ Notifies merchant using capture response

Louisiana State University

18- Web Security - 44

CSC4601 F04

Summary



- Have considered:
 - o need for web security
 - ${\color{orange} \circ}$ SSL/TLS transport layer security protocols
 - SET secure credit card payment protocols

Louisiana State University

18- Web Security - 45

CSC4601 F04