

Lecture 16 November 21, 2001

- Blind signatures + e-cash
- SSL

11/21/01

Gene Tsudik, ICS 268 Fall 2001

1

Electronic Cash

11/21/01

Gene Tsudik, ICS 268 Fall 2001

2

Outline

- What is electronic cash?
- Why electronic cash?
- Issues:
 - Off-line overspending
 - Anonymity
- How does e-cash work?
- Adding trustee trace-ability
- The anonymous change problem

11/21/01

Gene Tsudik, ICS 268 Fall 2001

3

Motivation

Conventional Cash is:



- Counterfeitable

- Slow

- Costly

- Vulnerable

- Bad for Remote Transactions

11/21/01

Gene Tsudik, ICS 268 Fall 2001

4

Credit Cards, Bank Cards, Checks, and Phone/subway cards:

Easy Fraud

Little Privacy

11/21/01 Gene Tsoulik, ICS 268 Fall 2001 5

Off-line Electronic Cash refers to two-party payment

Withdrawal

Payment

Deposit

- Low Communication Requirements

11/21/01 Gene Tsoulik, ICS 268 Fall 2001 6

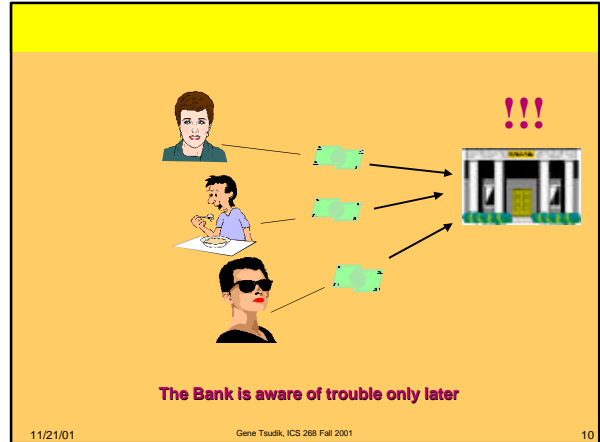
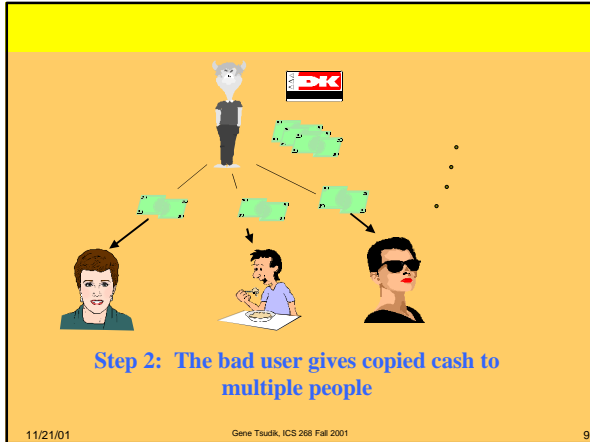
By Contrast, On-line Payments Look Like This

11/21/01 Gene Tsoulik, ICS 268 Fall 2001 7

Overspending: A problem with off-line e-cash

Step 1: The bad user copies his money

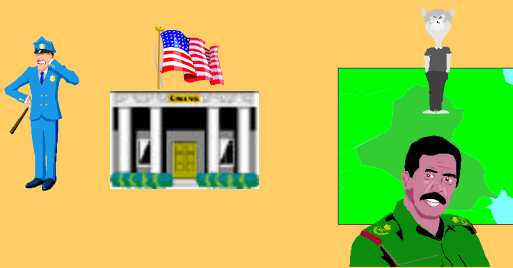
11/21/01 Gene Tsoulik, ICS 268 Fall 2001 8



- ### Techniques to Contain Over-Spending
- Use tamper-resistant hardware to prevent over-spending (e.g., MONDEX in Europe)
 - Trace over-spenders
 - Blacklist over-spenders
 - Put a bound on dollar-value of off-line transactions
- 11/21/01 Gene Tsudik, ICS 268 Fall 2001 11



Tracing over-spenders may be of little value



11/21/01

Gene Tausk, ICS 268 Fall 2001

13

Anonymity

Tracing of payments is a highly political issue

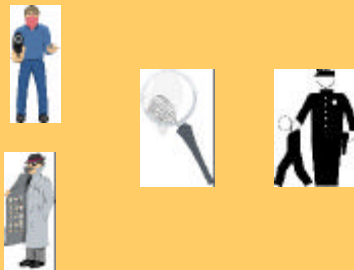


11/21/01

Gene Tausk, ICS 268 Fall 2001

14

Tracing is a crime-fighting tool



11/21/01

Gene Tausk, ICS 268 Fall 2001

15

Can be used to fight big-time international crime





11/21/01

Gene Tausk, ICS 268 Fall 2001



16

Tracing could be abused on many levels






11/21/01 Gene Tsudik, ICS 268 Fall 2001 17


Minting the Money

Secret Minting Key to Create Coins (Signatures)



Heart of Each Coin is a *Digital Signature*




Public Verification Key to Recognize Coins


11/21/01 Gene Tsudik, ICS 268 Fall 2001 18


Minting a conventional coin


ECash Withdrawer




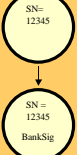
The Mint













11/21/01 Gene Tsudik, ICS 268 Fall 2001 19

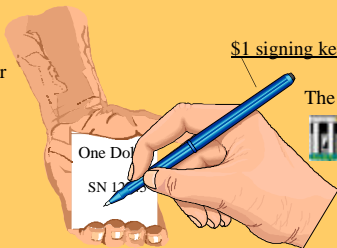
Without anonymity mint knows serial number

Ecash Withdrawer



The Mint

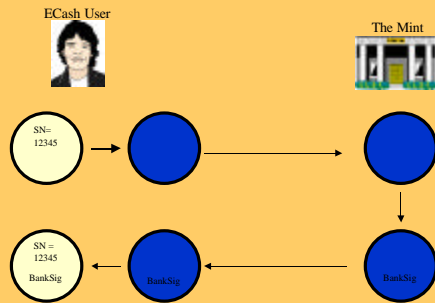




\$1 signing key

11/21/01 Gene Tsudik, ICS 268 Fall 2001 20

Minting an untraceable coin

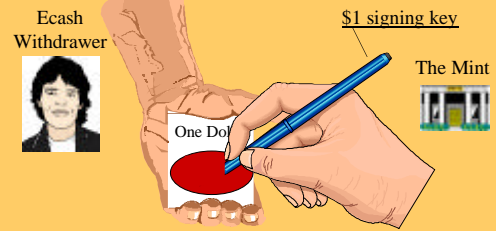


11/21/01

Gene Tsudik, ICS 268 Fall 2001

21

Blind signing is like signing through a veil

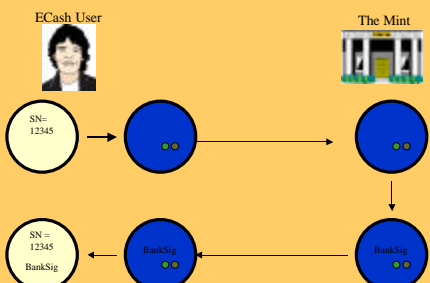


11/21/01

Gene Tsudik, ICS 268 Fall 2001

22

Minting a Trustee-traceable coin

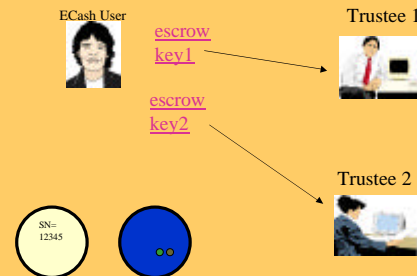


11/21/01

Gene Tsudik, ICS 268 Fall 2001

23

Escrowing trustee-traceable coins



11/21/01

Gene Tsudik, ICS 268 Fall 2001

24

Cryptographic Assumptions

Infeasible Tasks

1. *Factoring*. Given a number $N = pq$, find p and q
primes of at least 512 bits

1a. *RSA assumption*.
 Given exponent e and $m^e \pmod{N}$, find m

11/21/01 Gene Tsudik, ICS 268 Fall 2001 25

Cryptographic Assumptions

Infeasible Tasks


(continued)

of at least 512 bits


2. *Discrete log*. Given a prime p , a generator g ,
 and $g^x \pmod{p}$, find x

11/21/01 Gene Tsudik, ICS 268 Fall 2001 26

Example of Coin Minting

 *Public* Information:

- N A Large Composite Number
- H A one-way hash function

 *Private* Minting Information:


Key = p, q prime numbers such that $N=pq$

A coin has the form: $(x, H(x)^{1/3} \pmod{N})$, $1 < x < N$


11/21/01 Gene Tsudik, ICS 268 Fall 2001 27

Minting a conventional coin

ECash User



The Mint



$x, H(x)$

→

$x, H(x)^{1/3}$

→

↓

←

$x, H(x)$

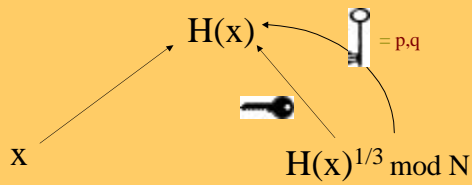
↓

$x, H(x)^{1/3}$

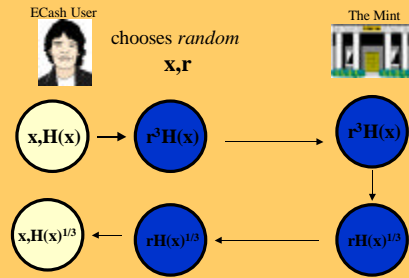
11/21/01 Gene Tsudik, ICS 268 Fall 2001 28

Anti-counterfeiting Assumption:

Without knowing the key, it is difficult to find pre-images that map to the same point



Blind Digital Signatures → Payer's Privacy [Chaum]



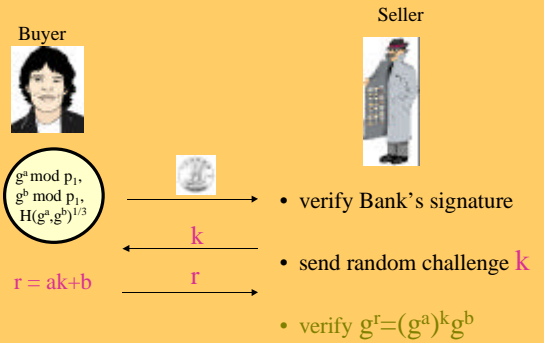
Tracing double-spenders (FY)

- p_1, p_2 : two large prime numbers such that $p_2 \mid p_1 - 1$
- G : subgroup of $Z_{p_1}^*$ such that $|G| = p_2$
- g : generator of G
- I : the user's identity, expressed as a number

= Coin = $(g^a \bmod p_1, g^b \bmod p_1, H(g^a, g^b)^{1/3} \bmod N)$

where $I = ab \bmod p_2$

Tracing double-spenders



Tracing double-spenders

Two Payments with the Same Coin
yield Buyer's Identity

$$\begin{aligned} r &= ak + b \\ r' &= ak' + b \end{aligned} \longrightarrow a, b \longrightarrow I \quad \text{Buyer}$$

11/21/01

Gene Tsudik, ICS 268 Fall 2001

33

Adding Trustee Traceability



User also gives bank: $E_1(a_1, b_1), E_2(a_2, b_2)$

where $a = a_1 + a_2, b = b_1 + b_2$

$$I = ab \text{ mod } p_2$$

Trustee 1



Trustee 2



11/21/01

Gene Tsudik, ICS 268 Fall 2001

34

The Perfect Crime? Kidnapping and other Extortion

Put \$1,000,000 into
account number XXX
or else!

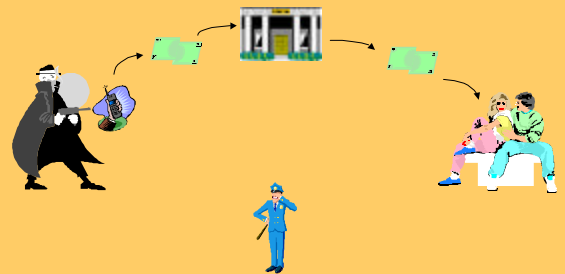


11/21/01

Gene Tsudik, ICS 268 Fall 2001

35

Once the money is withdrawn, it becomes untraceable



11/21/01

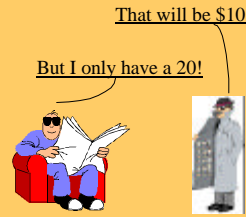
Gene Tsudik, ICS 268 Fall 2001

36

APPLICATION OF BLIND SIGNATURE TO A REAL CRIME
 B. von Solms and D. Naccache, *Computers and Security* 11, 6 (1992)

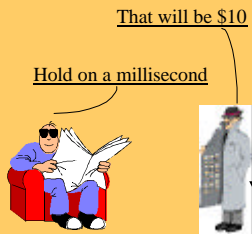
1. Open bank account, receive smartcard, and kidnap baby
2. Present the threat and collect the money:
 - Choose $\{x_1, x_2, \dots, x_p\}$ and $\{r_1, r_2, \dots, r_p\}$
 - Compute $\{B_j\}$, where $B_j = r_j^{x_j} \text{ mod } n$, mail $\{B_j\}$ to authorities with threat to kill baby unless they:
 - For all j , compute $D_j = \sqrt[p]{B_j} \text{ mod } n$**
 - and publish $\{D_j\}$ in a newspaper**
 - Buy newspaper and compute $\{C_j = D_j/r_j \text{ mod } n\}$.
 - $\{(x_j, C_j)\}$ now represents legal, untraceable and authorized e-money
3. Free baby, and spend electronic money without fear of capture

Anonymous Change Problem

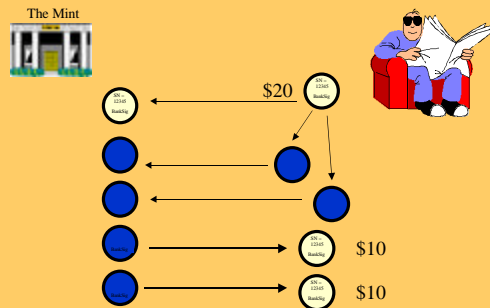


- Seller may not have change
- Change could be traced
- Store may not have a line to the bank
- Don't want to identify self to bank while "at the store"

On-Line Anonymous Change



On-Line Anonymous Change



11/21/01 Gene Tsudik, ICS 268 Fall 2001 41

Further Electronic Cash Issues

- How important is anonymity?
- Are there better anonymity-preserving solutions?
- Are there better off-line anonymous change protocols?
- How significant are off-line payments?

Note: Anonymity can be achieved in both off-line and on-line payments

11/21/01 Gene Tsudik, ICS 268 Fall 2001 42

SSL

Secure Sockets Layer

11/21/01 Gene Tsudik, ICS 268 Fall 2001 43

Secure Sockets Layer (SSL)

- An industry standard protocol
- Used to establish secure communications between server and client browsers
- Includes a public key certification system (but not a PKI!)
- Establishes identity of server, and, optionally, client
- Allows server and client to agree on level of encryption for subsequent communication

11/21/01 Gene Tsudik, ICS 268 Fall 2001 44

Secure Sockets Layer (SSL)

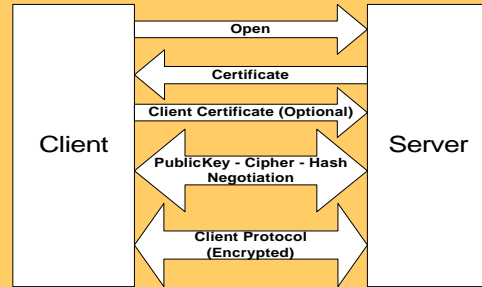
- SSL allows two parties who have never met to securely communicate.
- Asymmetric ciphers → secure key exchange
- Symmetric ciphers → secure data exchange
- Certificates signed by CA-s → prevent man-in-the-middle attacks

11/21/01

Gene Tsudik, ICS 268 Fall 2001

45

SSL theory of operation

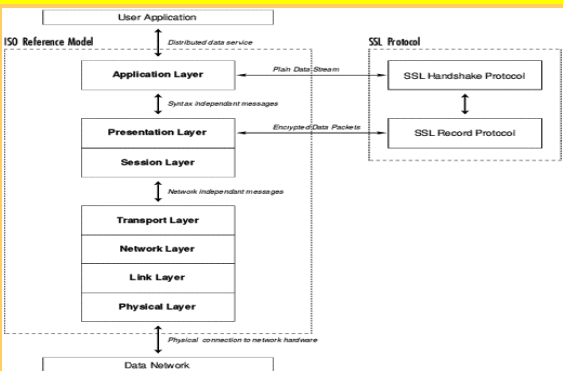


11/21/01

Gene Tsudik, ICS 268 Fall 2001

46

SSL and the ISO model



11/21/01

Gene Tsudik, ICS 268 Fall 2001

47

Secure Sockets Layer (SSL) v3

• Version 3 (old!)

> Asymmetric Ciphers

- ▶ RSA
- ▶ Diffie-Hellman (KE only)

> Digital Signatures

- ▶ RSA
- ▶ DSS

> Message Digests

- ▶ MD5
- ▶ SHA1

> Symmetric Ciphers

- ▶ RC4 - 128 bit
- ▶ RC2 - 128 bit
- ▶ IDEA - 128 bit
- ▶ 3DES - 168 bit
- ▶ DES - 56 bit
- ▶ RC4 - 40 bit (98 clear)
- ▶ RC2 - 40 bit (98 clear)

11/21/01

Gene Tsudik, ICS 268 Fall 2001

48

Certificates

- contain information about the server
 - Public Key (RSA, DH)
 - Company
 - Division/Group (Organizational Division)
 - Location - City/State/Country
 - Site name → must match DNS reverse lookup

11/21/01

Gene Tsudik, ICS 268 Fall 2001

49

Certificate Authority

- Certificates signed by a recognized CA
- CA-s are trusted “neutra” third parties, e.g.:
 - Verisign (RSA Certificate Authority)
 - Thawte Consulting (South Africa)
 - CertiSign Certificadora Digital

11/21/01

Gene Tsudik, ICS 268 Fall 2001

50

Legal Issues - Patents/Trade Secrets

- Patent
 - RSA - Patent 4405829
 - ▶ Covers use of RSA
 - ▶ RSAREF toolkit is only legal noncommercial use of RSA in the US
 - ▶ Patent expired September 20, 2000
 - DH - Patent 4200770
 - ▶ Covers use of all asymmetric ciphers
 - ▶ Patent expired April 29, 1997
 - IDEA - Patent 5214703
 - ▶ Noncommercial use ok
 - ▶ Patent expires May 25, 2010
 - DSS - Patent 4995082
 - ▶ Patent contention with NSA
 - ▶ Patent expires February 19, 2009
- Trade Secrets
 - RC2, RC4
 - ▶ Check with RSA for licensing

11/21/01

Gene Tsudik, ICS 268 Fall 2001

51

Products

- Web Servers
 - Apache-SSL
 - ▶ Publicly available
 - ▶ Noncommercial use only due to patents
 - Stronghold / Raven
 - ▶ Commercial version of Apache
 - ▶ Patent licenses included
 - Netscape Fasttrack / Enterprise
 - ▶ Fasttrack only supports export encryption (40 bits)
- Toolkits
 - SSLeay
 - ▶ Written by Eric Young
 - ▶ Available from <http://www.ssleay.org>
 - ▶ Used in Apache-SSL, Stronghold, Raven
 - ▶ Publicly available
 - ▶ Commercial use requires printed notice only
 - ▶ Does not include licenses to use patented ciphers

11/21/01


Gene Tsudik, ICS 268 Fall 2001

52


SSL Mechanics

- URLs start with HTTPS, not HTTP
 - > https://www.bs.com
- The default port is 443, not 80
- Everything else is the same

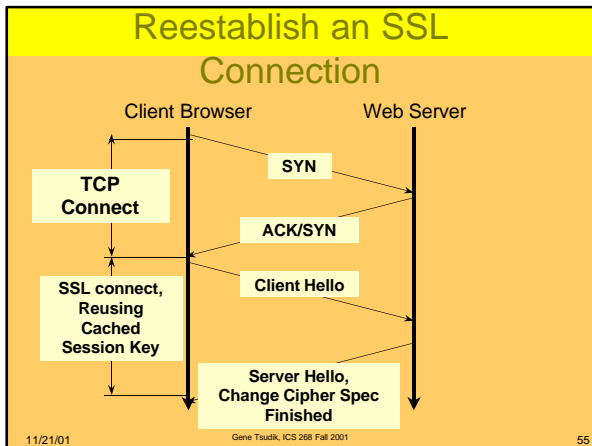
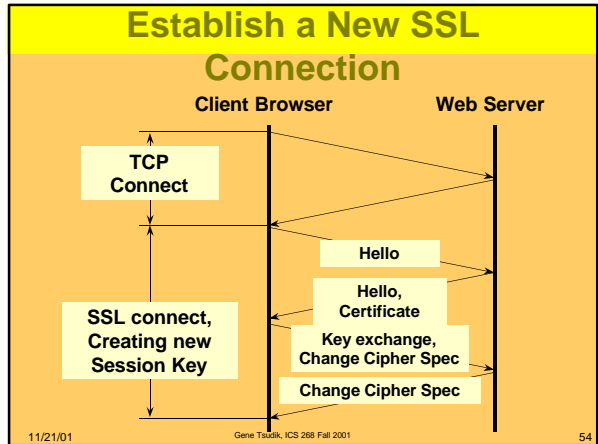
• Insecure sites show:



• Secure sites show:



Copyright 1997, 1998 Beyond Software Inc. Page3
Gene Tsudik, ICS 268 Fall 2001



SSL Handshake Protocol

- Consists of two phases
- Phase I: exchange of master key and authentication of server
- Phase II: client authentication, if requested, and finish handshaking
- Each party can support multiple ciphers and client/server must have at least one in common. Need to exchange sets of supported mechanisms.

11/21/01 Gene Tsudik, ICS 268 Fall 2001 56

Using SSL

- Requires installed CA certificate base
- If hosting internal private sites, you can be your own CA by using Certificate Server
- If hosting Internet-accessible sites, need a reputable CA such as VeriSign

11/21/01

Gene Tsudik, ICS 268 Fall 2001

57

Obtaining Server Certificate

- Create certificate request file (self-signed)
- Send request file to CA (how?)
- Obtain certificate
- Install certificate on server

11/21/01

Gene Tsudik, ICS 268 Fall 2001

58

Error Message

- If SSL is required for a resource, the client must use a properly formatted URL and support the appropriate encryption strength
- Otherwise: "HTTP/1.1 403 Access Forbidden (Secure Channel Required)"

11/21/01

Gene Tsudik, ICS 268 Fall 2001

59

Client SSL Features

- Client certificates allow SSL-hosted site operators to control access based on identity
- Client certificates operate in same manner as server certificates
- Requiring client certificates prevents clients without certificates or with invalid certificates from accessing the site
- Can map certificates to user accounts thus associating access permissions

11/21/01

Gene Tsudik, ICS 268 Fall 2001

60

Secure Sockets Layer (SSL)

- An industry standard protocol
- Used to establish secure communications between server and client browsers
- Includes a public key certification system (but not a PKI!)
- Establishes identity of server, and, optionally, client
- Allows server and client to agree on level of encryption for subsequent communication

11/21/01

Gene Tsoulik, ICS 268 Fall 2001

61

Secure Sockets Layer (SSL)

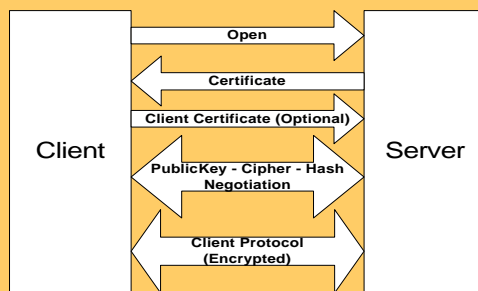
- SSL allows two parties who have never met to securely communicate.
- Asymmetric ciphers → secure key exchange
- Symmetric ciphers → secure data exchange
- Certificates signed by CA-s → prevent man-in-the-middle attacks

11/21/01

Gene Tsoulik, ICS 268 Fall 2001

62

SSL theory of operation

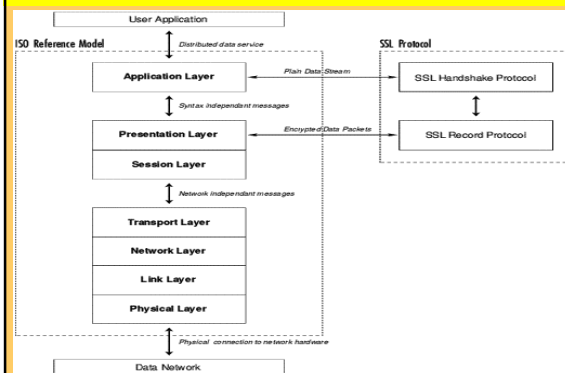


11/21/01

Gene Tsoulik, ICS 268 Fall 2001

63

SSL and the ISO model



11/21/01

Gene Tsoulik, ICS 268 Fall 2001

64

Secure Sockets Layer (SSL) v3

- **Version 3 (old!)**
 - Asymmetric Ciphers
 - ▶ RSA
 - ▶ Diffie-Hellman (KE only)
 - Digital Signatures
 - ▶ RSA
 - ▶ DSS
 - Message Digests
 - ▶ MD5
 - ▶ SHA1
 - Symmetric Ciphers
 - ▶ RC4 - 128 bit
 - ▶ RC2 - 128 bit
 - ▶ IDEA - 128 bit
 - ▶ 3DES - 168 bit
 - ▶ DES - 56 bit
 - ▶ RC4 - 40 bit (98 clear)
 - ▶ RC2 - 40 bit (98 clear)

11/21/01 Gene Tsudik, ICS 268 Fall 2001 65

Certificates

- **contain information about the server**
 - Public Key (RSA, DH)
 - Company
 - Division/Group (Organizational Division)
 - Location - City/State/Country
 - Site name → must match DNS reverse lookup

11/21/01 Gene Tsudik, ICS 268 Fall 2001 66

Certificate Authority

- **Certificates signed by a recognized CA**
- **CA-s are trusted "neutra" third parties, e.g.:**
 - Verisign (RSA Certificate Authority)
 - Thawte Consulting (South Africa)
 - CertiSign Certificadora Digital

11/21/01 Gene Tsudik, ICS 268 Fall 2001 67

Legal Issues - Patents/Trade Secrets

- **Patent**
 - RSA - Patent 4405829
 - ▶ Covers use of RSA
 - ▶ RSAREF toolkit is only legal noncommercial use of RSA in the US
 - ▶ Patent expired September 20, 2000
 - DH - Patent 4200770
 - ▶ Covers use of all asymmetric ciphers
 - ▶ Patent expired April 29, 1997
 - IDEA - Patent 5214703
 - ▶ Noncommercial use ok
 - ▶ Patent expires May 25, 2010
 - DSS - Patent 4995082
 - ▶ Patent contention with NSA
 - ▶ Patent expires February 19, 2009
- **Trade Secrets**
 - RC2, RC4
 - ▶ Check with RSA for licensing

11/21/01 Gene Tsudik, ICS 268 Fall 2001 68

Products


- **Web Servers**
 - Apache-SSL
 - ▶ Publicly available
 - ▶ Noncommercial use only due to patents
 - Stronghold / Raven
 - ▶ Commercial version of Apache
 - ▶ Patent licenses included
 - Netscape Fasttrack / Enterprise
 - ▶ Fasttrack only supports export encryption (40 bits)
- **Toolkits**
 - SSLeay
 - ▶ Written by Eric Young
 - ▶ Available from <http://www.sseay.org>
 - ▶ Used in Apache-SSL, Stronghold, Raven
 - ▶ Publicly available
 - ▶ Commercial use requires printed notice only
 - ▶ Does not include licenses to use patented ciphers

11/21/01 Gene Tsudik, ICS 268 Fall 2001 69


SSL Mechanics

- URLs start with **HTTPS, not HTTP**
 - <https://www.bs.com>
- The default port is **443, not 80**
- Everything else is the same

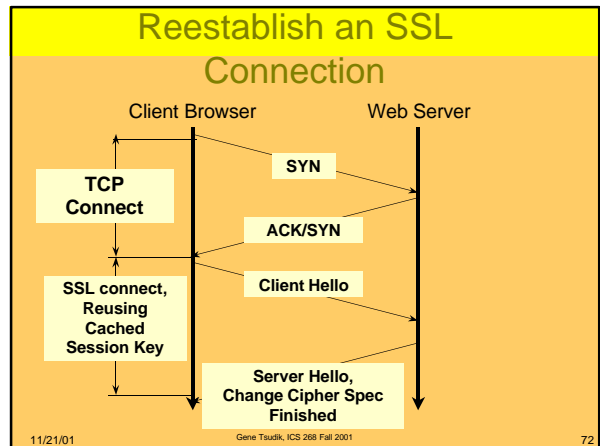
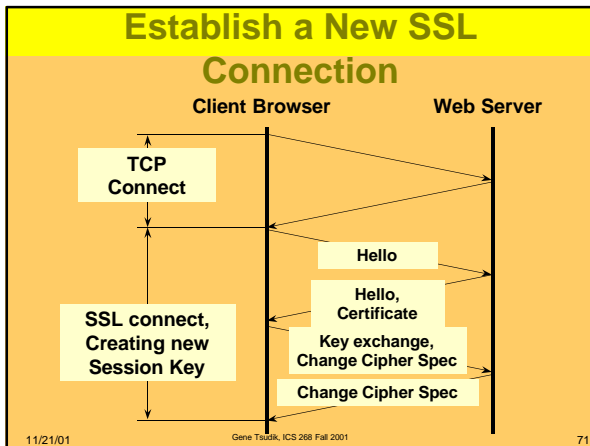
• Insecure sites show:



• Secure sites show:



Copyright 1997, 1998 Beyond Software Inc Page3
Gene Tsudik, ICS 268 Fall 2001 70



SSL Handshake Protocol

- Consists of two phases
- Phase I: exchange of master key and authentication of server
- Phase II: client authentication, if requested, and finish handshaking
- Each party can support multiple ciphers and client/server must have at least one in common. Need to exchange sets of supported mechanisms.

11/21/01

Gene Tsudik, ICS 268 Fall 2001

73

Using SSL

- Requires installed CA certificate base
- If hosting internal private sites, you can be your own CA by using Certificate Server
- If hosting Internet-accessible sites, need a reputable CA such as VeriSign

11/21/01

Gene Tsudik, ICS 268 Fall 2001

74

Obtaining Server Certificate

- Create certificate request file (self-signed)
- Send request file to CA (how?)
- Obtain certificate
- Install certificate on server

11/21/01

Gene Tsudik, ICS 268 Fall 2001

75

Error Message

- If SSL is required for a resource, the client must use a properly formatted URL and support the appropriate encryption strength
- Otherwise: "HTTP/1.1 403 Access Forbidden (Secure Channel Required)"

11/21/01

Gene Tsudik, ICS 268 Fall 2001

76

Client SSL Features

- Client certificates allow SSL-hosted site operators to control access based on identity
- Client certificates operate in same manner as server certificates
- Requiring client certificates prevents clients without certificates or with invalid certificates from accessing the site
- Can map certificates to user accounts thus associating access permissions