601.445/645: Practical Cryptographic Systems

Protocols

Instructor: Matthew Green

Review

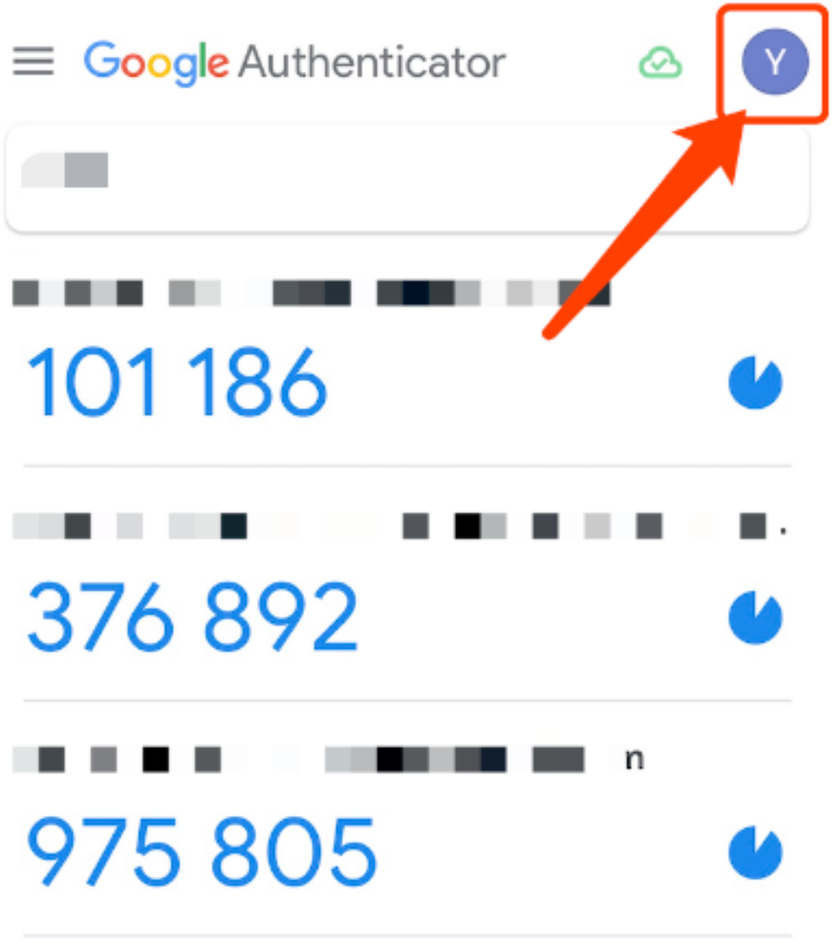
- Last time:
  - Finished up (most) primitives
  - Digital signatures
  - Almost there
- Today:
  - Finishing that stuff up
  - Protocols!

Reading and Midterm

- Midterm is on 3/10
- Do the reading, please
  - 20 years of attacks on RSA
  - Imperfect Forward Secrecy
  - Lucky13
  - Mining Ps and Qs (among others)

News?

News?



New assignment

- Some ingredients:
  - Static DH oracles
  - Subgroups of a cyclic groups
    (generators of subgroups)
  - Algorithms for computing the discrete logarithm
  - CRT

Static DH oracles

- Let a be a secret value
  - A “static” DH oracle is one that takes in a group element h and returns h^a mod p.
  - When do we get these in real life?
  - What’s the impact?

Subgroups

- For every finite cyclic group of order n:
  - For every divisor of n, there exists one subgroup of that order
  - These subgroups have generators
- What happens when the group order n has many divisors?

CRT (Sunzi's theorem)

- Let p1, p2, …, pN be divisors of a modulus N
- Then for some integer 0 <= X < N, given the integers:
  - a1 = (X mod p1)
    a2 = (X mod p2)
    ….
    aN = (X mod pN)
  - There exists an algorithm that can solve for X

CRT (algorithm)

- For i = 1 to n:
  - Compute $y_i = \frac{N}{p_i}$
  - Compute $z_i \equiv y_i^{-1} \ mod \ p_i$ <—extended Euclidian algorithm
- Compute $X = \sum_{i=1}^{n} a_i y_i z_i$

Digital Signatures (again)

- Hash-based signatures

SSL/TLS

- Transport-layer security protocol
  - Often used to secure reliable protocols (TCP)
  - Does not require pre-shared keys
  - Most common usage: https

-E-commerce ($200bn/2008), Banking, etc.

Bank of America

Bank of Opportunity™

Today

- Protocols
  - What is a protocol?
  - What is SSL/TLS?

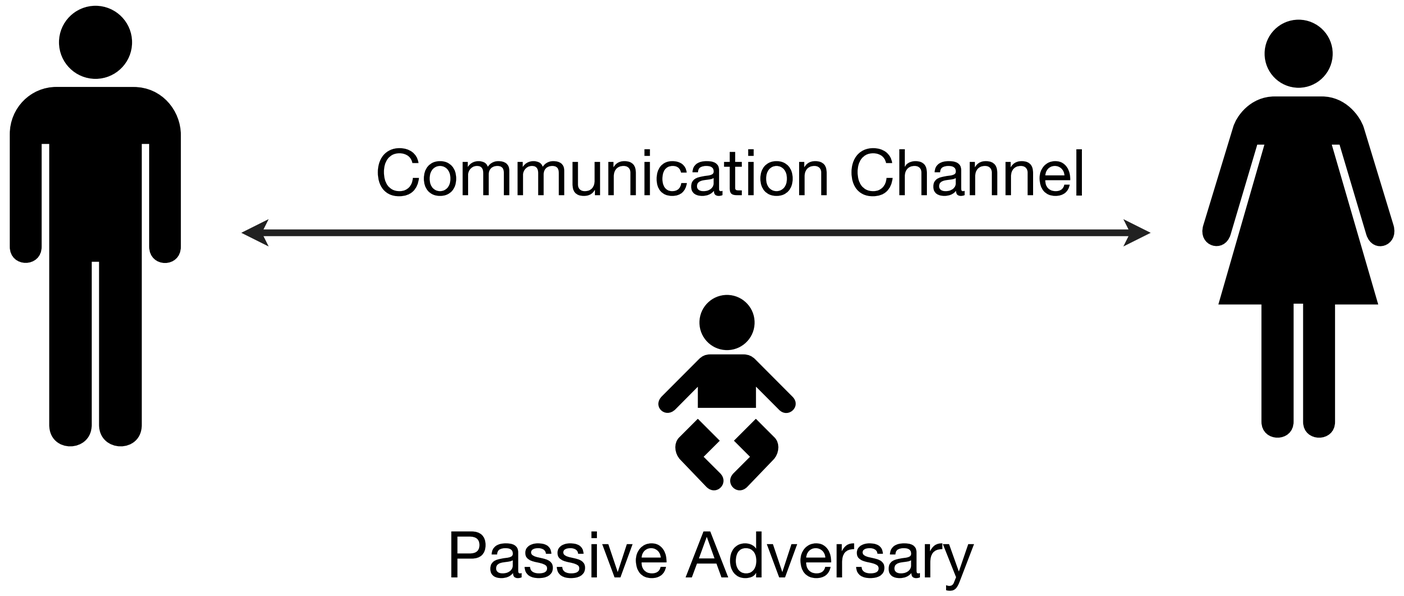
Protocols (definition)

- Definition
  - “A set of rules or procedures for transmitting data between electronic devices, such as computers”
  - “A security protocol (cryptographic protocol or encryption protocol) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods”

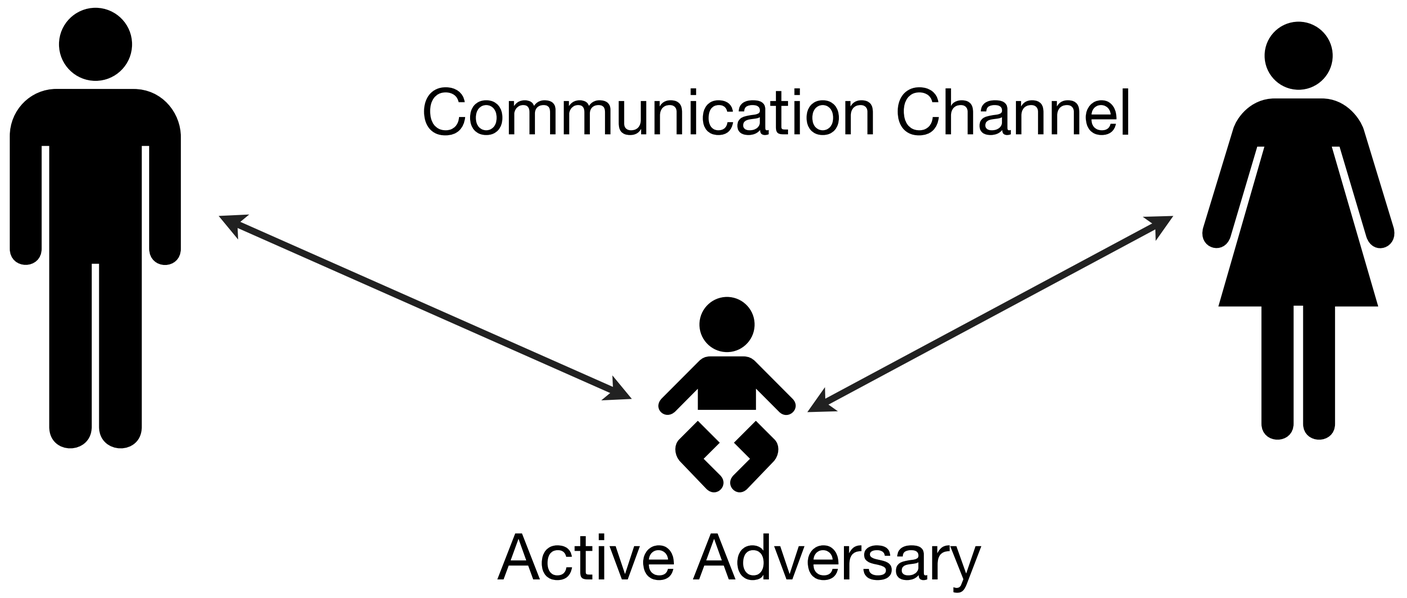
Why not just use primitives?

- A primitive (algorithm) can sometimes be a “protocol”
- But generally there’s more to a protocol
- E.g., TLS:
  - Negotiation (what version are you running?)
  - Authentication (who are you?)
  - Key exchange (let’s get a shared key)
  - Authenticated Encryption (let’s exchange data)

Threat Model

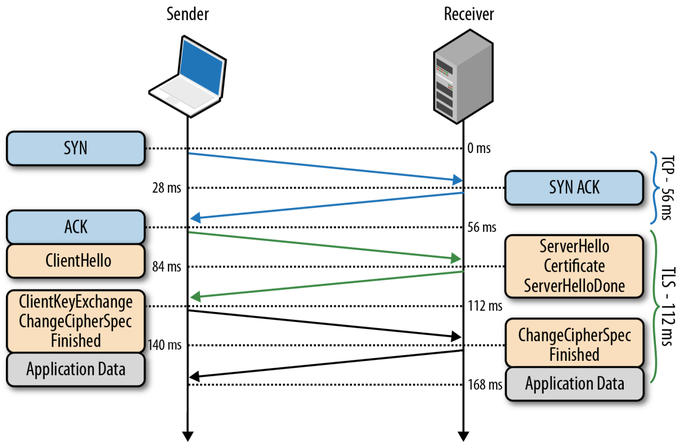


Threat Model



SSL/TLS

- Most important security protocol on the Internet
  - Allows secure connections between clients & servers
  - Current version: TLS 1.3 (RFC 8446)
    - (But browsers still support SSL 3
  - Not just web browsing!

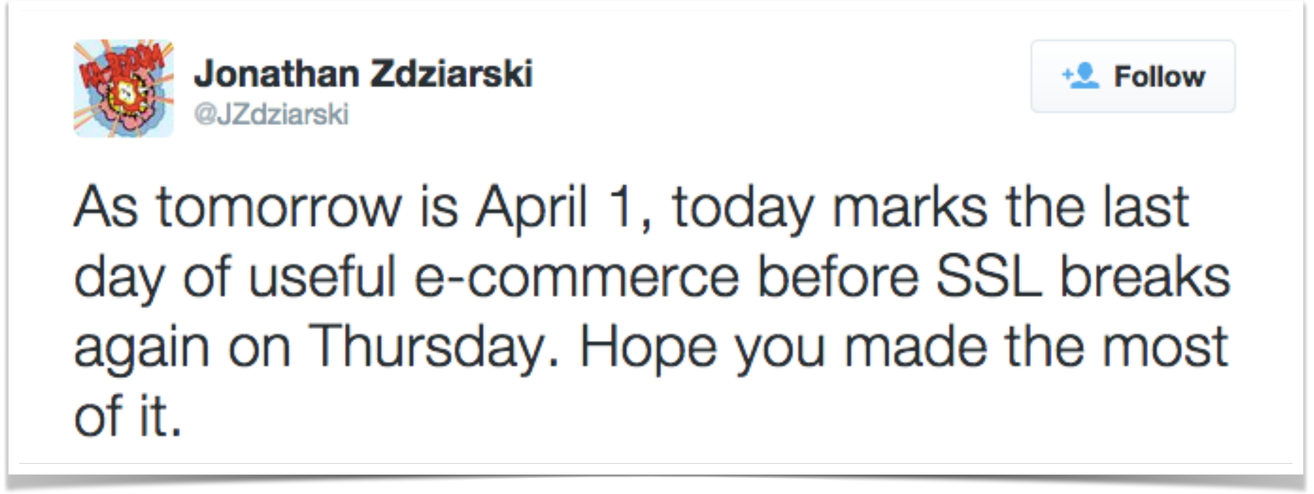


A brief history

- **SSLv1 born at Netscape. Never released. (~1994)**
- **SSLv2 released one year later**
- **SSLv3 (1996)**
- **TLS 1.0 (1998)**
  - Still widely deployed
- **TLS 1.1 (2006)**
- **TLS 1.2 (2008)**

How secure is TLS?

- **Many active attacks and implementation vulnerabilities**
  - Heartbleed, Lucky13, FREAK, CRIME, BEAST, RC4



Why these problems?

- Many problems result from TLS's use of "*pre-historic cryptography*" (- Eric Rescorla)
  - Export grade encryption
  - RSA-PKCS#1v1.5 encryption padding
  - RC4
  - DH parameter generation
  - Horrifying backwards compatibility requirements

Quite a bit

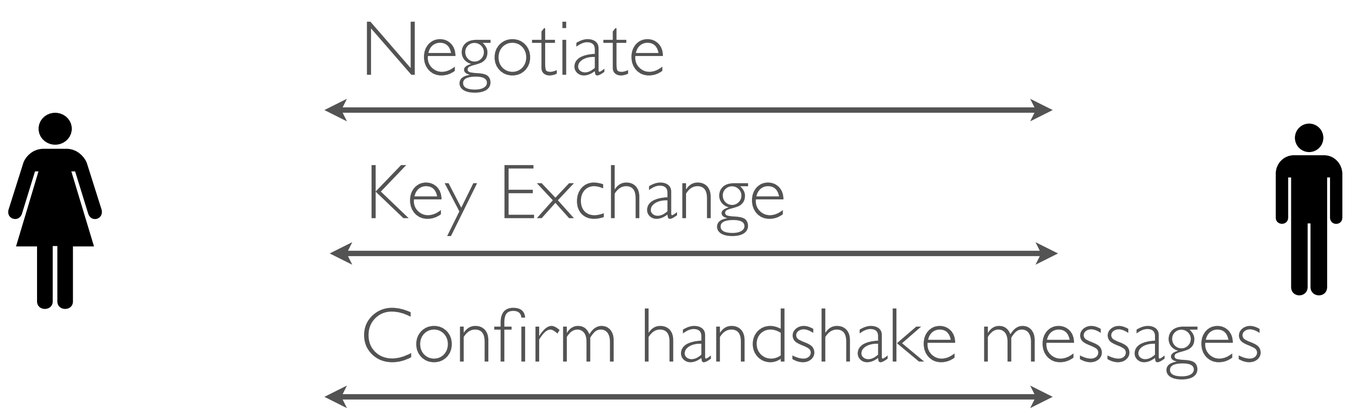
- Many problems result from TLS's use of "*pre-historic cryptography*" (- Eric Rescorla)
  - **Export**
  - RSA-P
  - RC4
  - DH par
  - Horrify

1995-~2000 (and onward)

Weakened "ciphersuites" with limited security
(e.g., 512-bit DH/RSA, 40-bit RC4)

TLS Negotiation

Each TLS handshake begins with a cipher suite negotiation that determines which key agreement protocol (etc.) will be used.



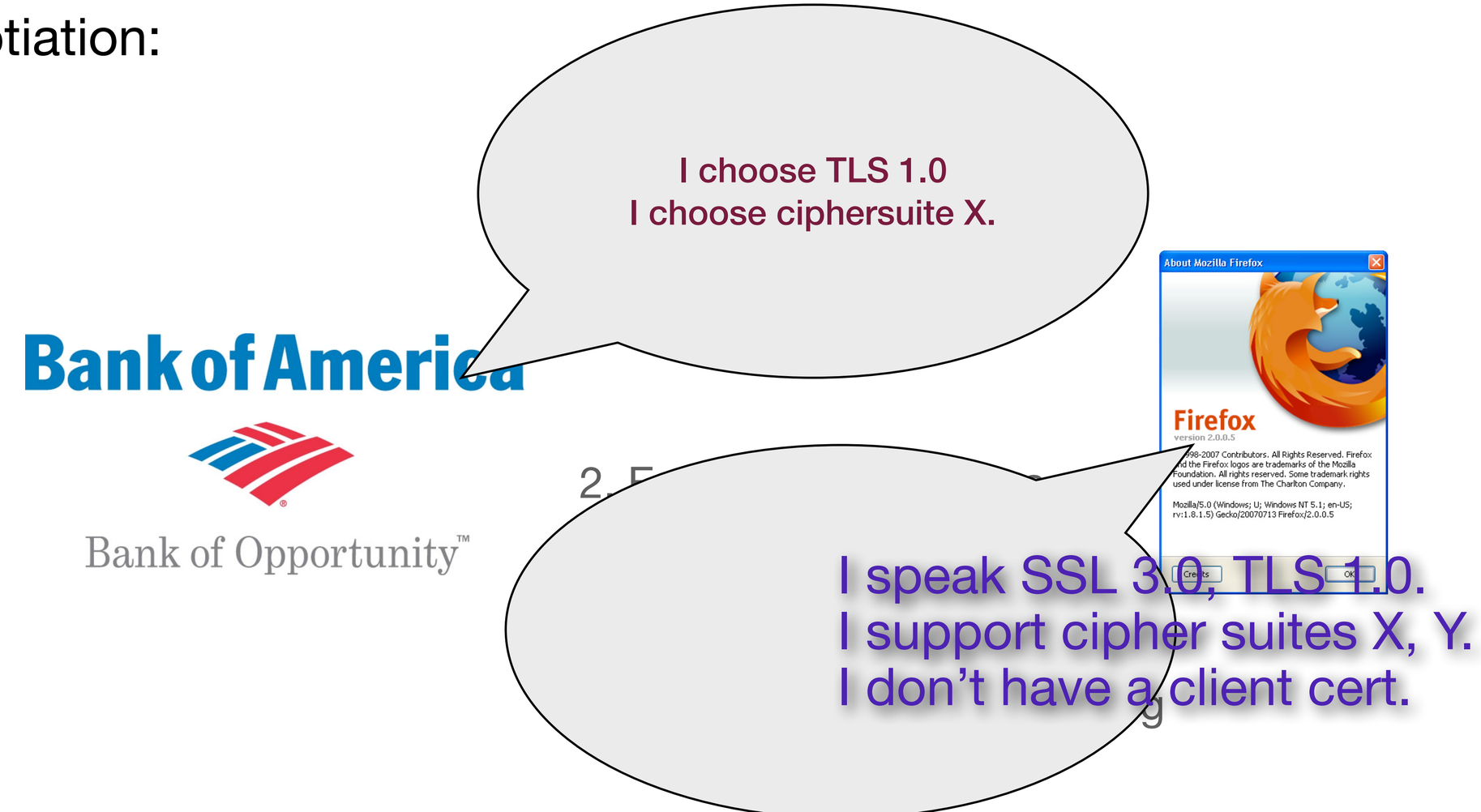
SSL/TLS

Bank of America

Bank of Opportunity™

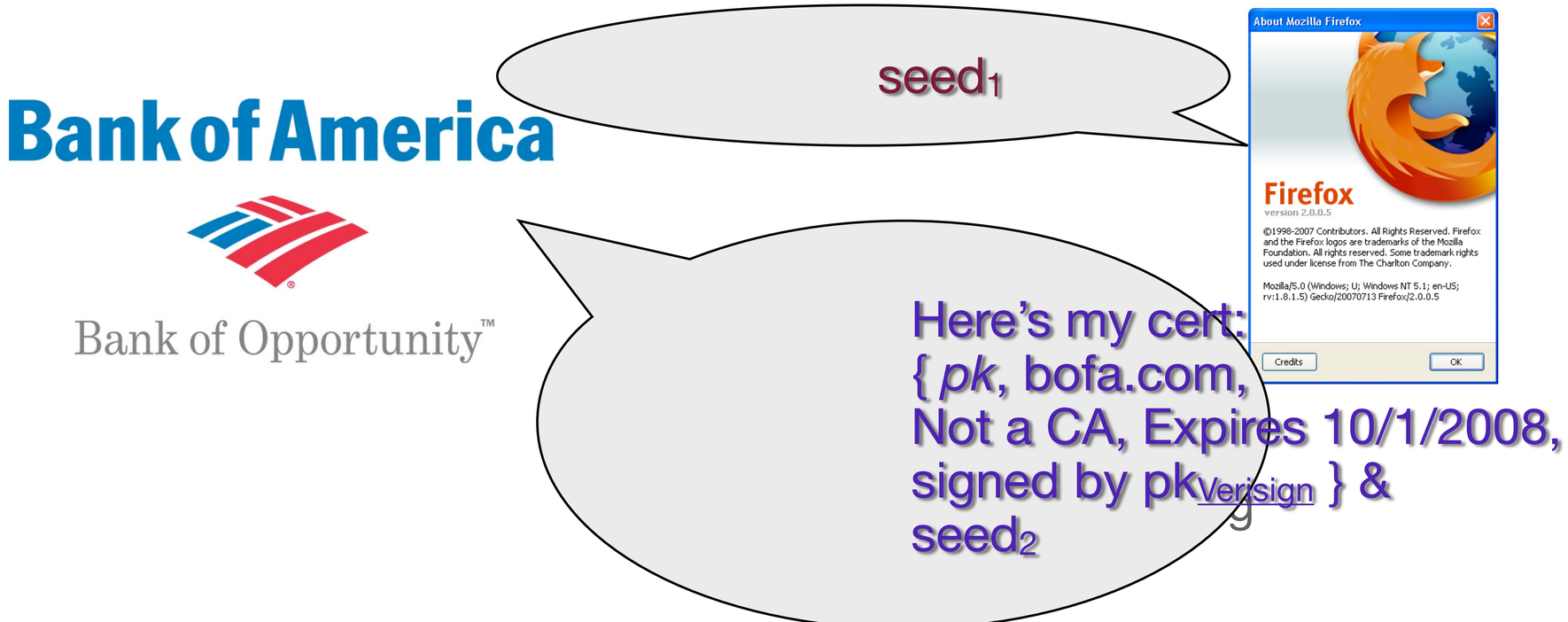
SSL/TLS

- Negotiation:



SSL/TLS

- Certificate Exchange



SSL/TLS

- Session key establishment
  - Various options
  - Common approach: RSA based

$C = RSA\text{-}ENC_{pk}(seed_3)$

1. Negotiate peer capabilities
2. Exchange certificates
3. Secure communi
4. Session expira

$seed_3 = RSA\text{-}DEC(sk, C)$

$k_s = H(seed_1 \,||\, seed_2 \,||\, seed_3)$

$k_s = H(seed_1 \,||\, seed_2 \,||\, seed_3)$

SSL/TLS

- Secure communication
  - In practice, we derive separate MAC & encryption keys

Bank of America

Bank of Opportunity™

1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment

5. Session expiration/rekeying

SSL/TLS

- Key expiration/rekeying
  - Key has a defined lifetime
  - If session drops within that lifetime, we restart:

•This shortcut saves PK operations

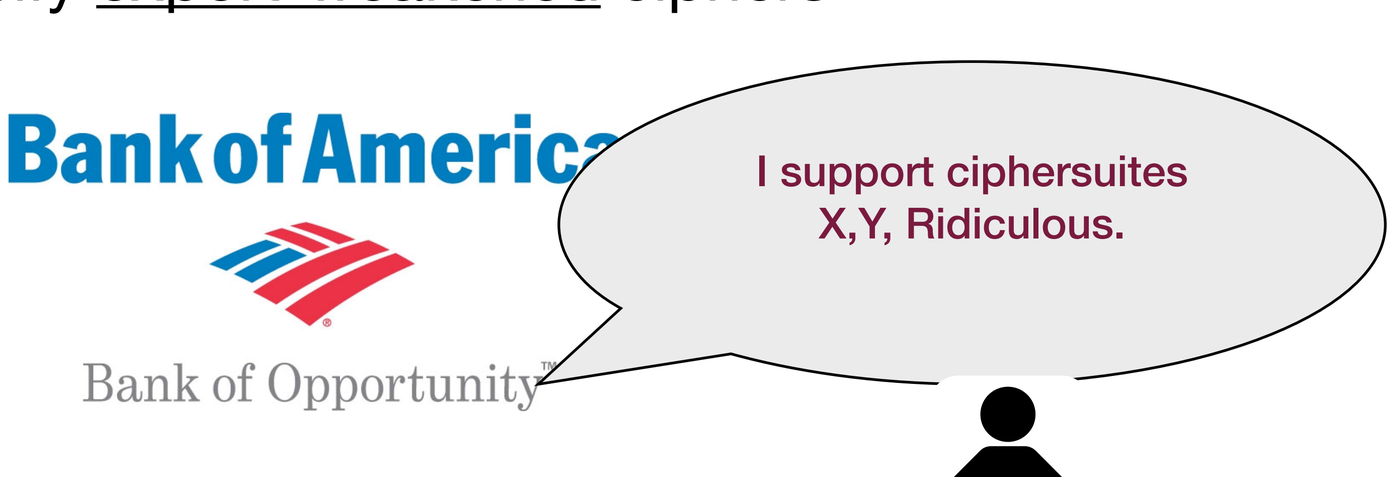
Bank of America

Bank of Opportunity™

1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment
4. Secure communications

Attacks on SSL2

- Many and varied...
- Major vulnerability:
  - Ciphersuite list not authenticated
  - Active attacker could modify the message to specify export-weakened ciphers



SSL3

- All of the problems with SSL2 fixed!
- Well, not quite:
  - Ciphersuite rollback attack (weaker)
  - Key-exchange algorithm rollback
  - Version rollback
  - (Weak) traffic analysis
  - Also, uses some non-standard primitives

CCS Rollback

- Most messages sent during client/server handshake are authenticated
  - Final MAC is sent at finish message
  - However, [change cipher spec] message is not included in the MAC
  - Tells the other party to start using encryption/authentication
  - Attacker can modify/drop this message!

CCS Rollback

- Normal protocol:

$$
\begin{array}{lll}
\ldots & & \\
1. & C \rightarrow S: & [\textbf{change cipher spec}] \\
2. & C \rightarrow S: & [\textbf{finished:}]\,\{a\}_k \\
3. & S \rightarrow C: & [\textbf{change cipher spec}] \\
4. & S \rightarrow C: & [\textbf{finished:}]\,\{a\}_k \\
5. & C \rightarrow S: & \{m\}_k \\
\ldots & &
\end{array}
$$

CCS Rollback

- MITM attack:

$$
\begin{array}{lll}
\ldots & & \\
1. & C \rightarrow M: & [\textbf{change cipher spec}] \\
2. & C \rightarrow M: & [\textbf{finished:}]\, \{a\}_k \\
2'. & M \rightarrow S: & [\textbf{finished:}]\, a \\
3. & S \rightarrow M: & [\textbf{change cipher spec}] \\
4. & S \rightarrow M: & [\textbf{finished:}]\, \{a\}_k \\
4'. & M \rightarrow C: & [\textbf{finished:}]\, a \\
5. & C \rightarrow M: & \{m\}_k \\
5'. & M \rightarrow S: & m \\
\ldots & &
\end{array}
$$

Key-Exchange Rollback

- SSL3 standard supports two ephemeral key exchange modes:
  - 1. Server publishes ephemeral RSA parameters (signed under its certified signing key)
  - 2. Server publishes ephemeral DH parameters
  - Client may be able to pick which to use
- Why ephemeral key exchange?
  - Advantages of Diffie-Hellman? RSA?

Key Exchange Rollback

Bank of America

Bank of Opportunity™

Normal RSA parameters:
(N,e)

I assume *p* is the RSA modulus, and *g* is the RSA exponent. I ignore the extra value.

Since *p* is a prime, we can compute inverses. Recover k.

Version Rollback

- Release of SSL3 didn’t make SSL2 browsers go away
  - Servers still accepted SSL2 requests
  - Attacker could modify [client hello] message to specify SSL2
  - Server continues with SSL2 connection, attacker uses SSL2 attacks

Version Rollback

- Version rollback is a big problem!
  - SSL, SSH, IPSEC...
  - Example: PPTP

•Can disable encryption, force use of a weaker password authentication protocol

  - Example: L2TP

•Better! But many implementations automatically downgrade to PPTP if L2TP connection fails

Traffic Analysis: SSL3

- Example:
  - First HTTP request typically looks like:

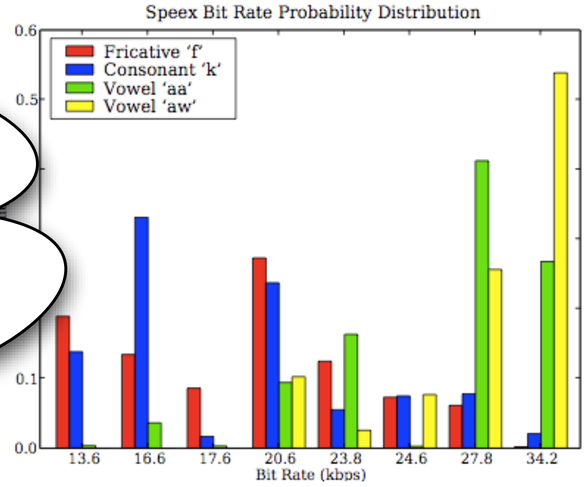
```
/
cnn.com
```

  - From ciphertext length, we may be able to work out URL information

Traffic Analysis++

- Digression: The case of encrypted VoIP
  - Some VoIP protocols use VBR encoding, size of data packets depends on signal
  - Also include “silence suppression” (VAD)
  - Therefore, total traffic is [illegible] related to the contents of

Good news:
Most VoIP implementations don't actually use VBR/ supression

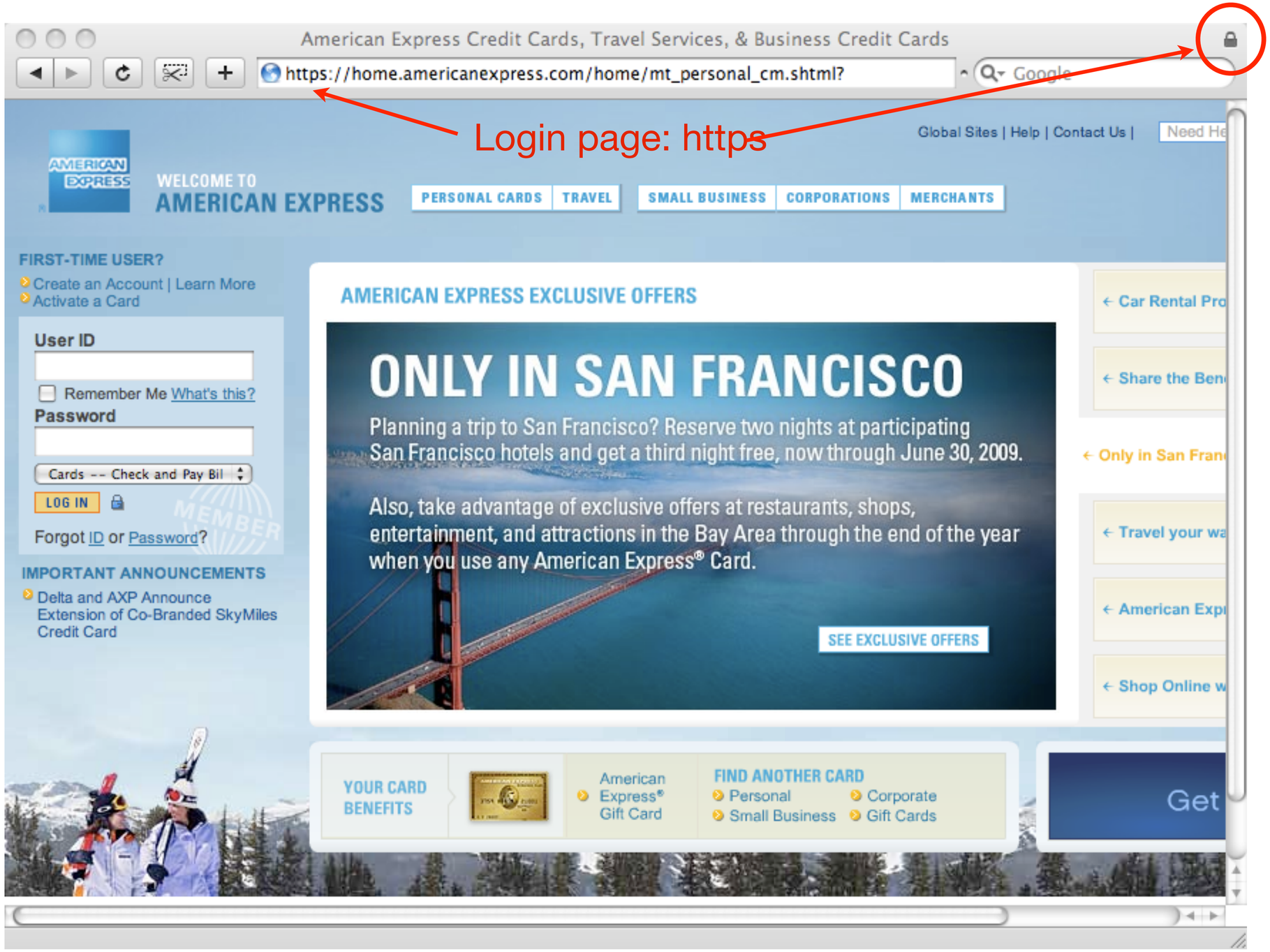


SSL Stripping & Pinning

- Moxie Marlinspike: SSLStrip
- Does not break SSL
- Instead: takes advantage of the way SSL is used

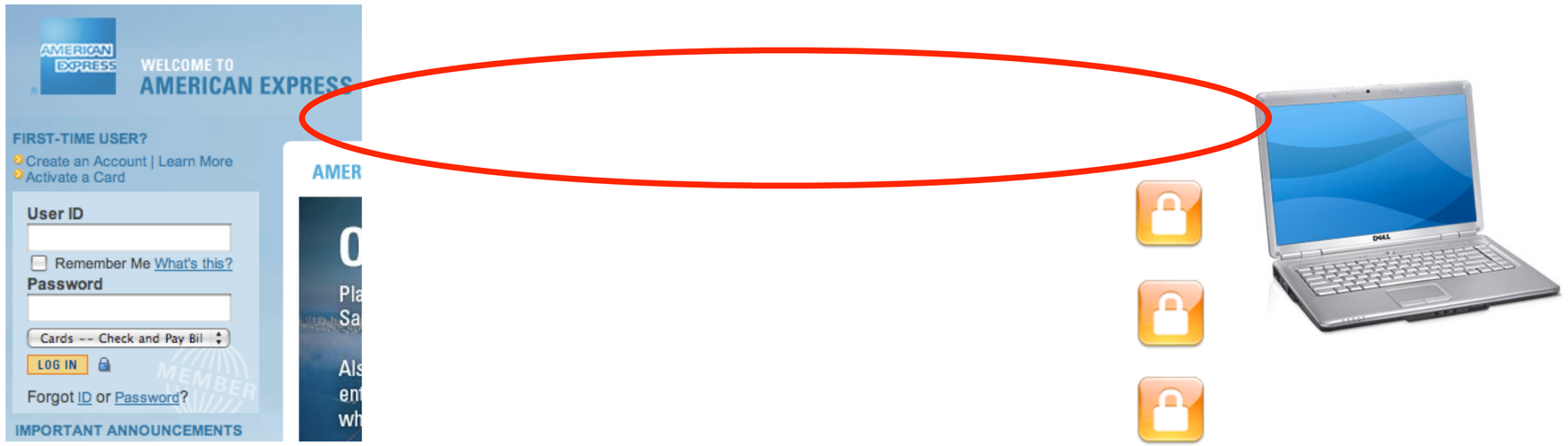
HTTP->HTTPS

- Typical Banking Experience:
  - SSL URLs begin with https://
  - But users rarely type the prefix


American Express Credit Cards, Travel Services, & Business Credit Cards
https://home.americanexpress.com/home/mt_personal_cm.shtml?
Google
Login page: https
Global Sites | Help | Contact Us |
WELCOME TO
AMERICAN EXPRESS
PERSONAL CARDS
TRAVEL
SMALL BUSINESS
CORPORATIONS
MERCHANTS
FIRST-TIME USER?
Create an Account | Learn More
Activate a Card
User ID
Remember Me What's this?
Password
LOG IN
Forgot ID or Password?
IMPORTANT ANNOUNCEMENTS
Delta and AXP Announce Extension of Co-Branded SkyMiles Credit Card
AMERICAN EXPRESS EXCLUSIVE OFFERS
ONLY IN SAN FRANCISCO
Planning a trip to San Francisco? Reserve two nights at participating San Francisco hotels and get a third night free, now through June 30, 2009.
Also, take advantage of exclusive offers at restaurants, shops, entertainment, and attractions in the Bay Area through the end of the year when you use any American Express® Card.
SEE EXCLUSIVE OFFERS
YOUR CARD BENEFITS
American Express® Gift Card
FIND ANOTHER CARD
Personal
Corporate
Small Business
Gift Cards
Get

HTTP->HTTPS

- If you can intercept the user's connection:
  - Don't redirect, or:
  - Redirect to malicious site, unsecured (http)



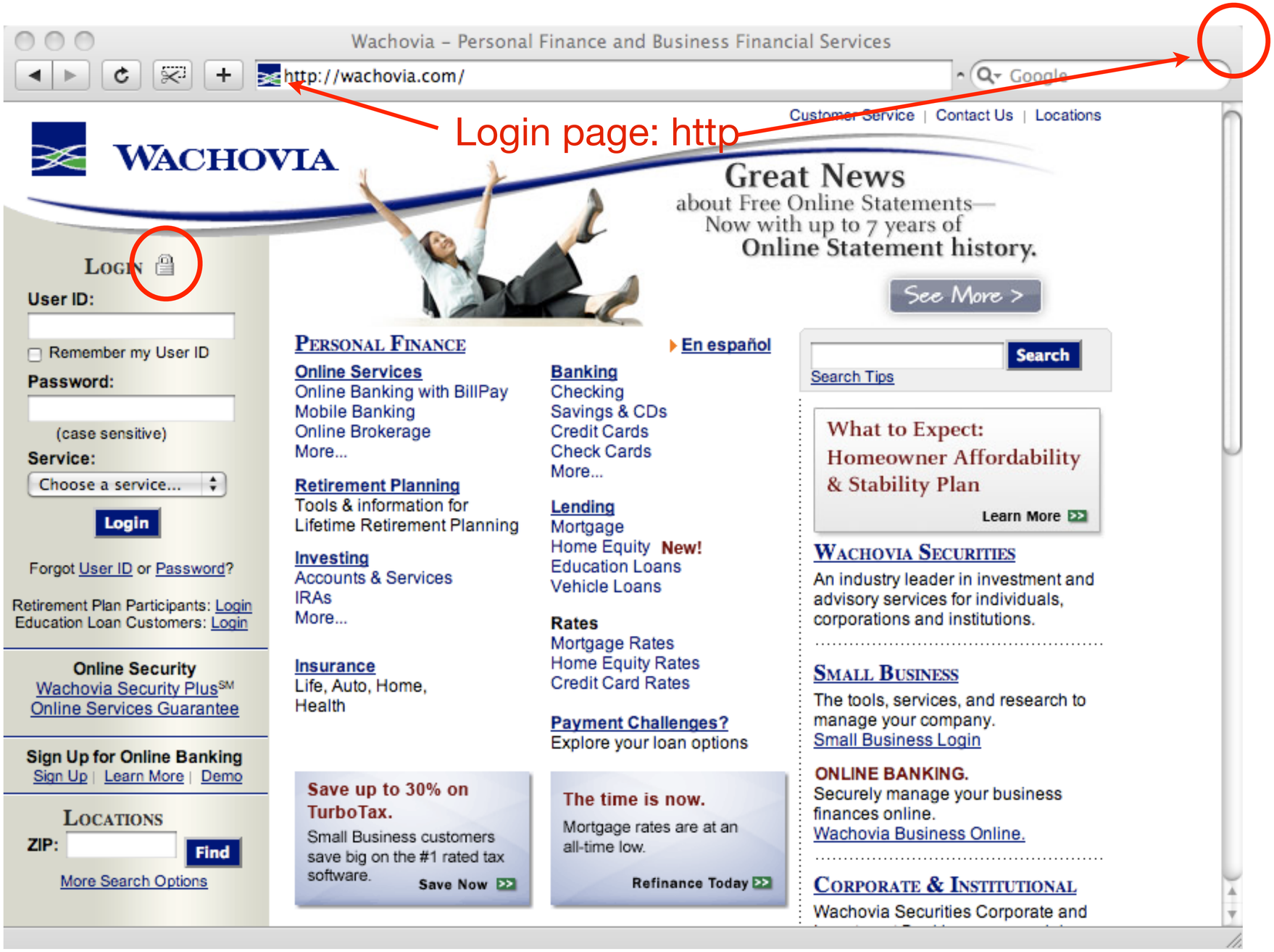
HTTP->HTTPS

- If you can intercept the user's connection:
  - Homograph site: paypaI.com (with a capital i), or:
  - Use clever IDN tricks e.g.,

    https://www.gmail.com/accounts/ServiceLogin!f.ijjk.cn

HTTP->HTTP->HTTPS

- It can be worse:
  - Some sites give an http page with a form that submits via https


Wachovia – Personal Finance and Business Financial Services
http://wachovia.com/
Google
Login page: http
Customer Service | Contact Us | Locations
WACHOVIA
Great News
about Free Online Statements—
Now with up to 7 years of
Online Statement history.
See More >
LOGIN
User ID:
Remember my User ID
Password:
(case sensitive)
Service:
Choose a service...
Login
Forgot User ID or Password?
Retirement Plan Participants: Login
Education Loan Customers: Login
Online Security
Wachovia Security Plus℠
Online Services Guarantee
Sign Up for Online Banking
Sign Up | Learn More | Demo
LOCATIONS
ZIP:
Find
More Search Options
PERSONAL FINANCE
En español
Online Services
Online Banking with BillPay
Mobile Banking
Online Brokerage
More...
Retirement Planning
Tools & information for
Lifetime Retirement Planning
Investing
Accounts & Services
IRAs
More...
Insurance
Life, Auto, Home,
Health
Banking
Checking
Savings & CDs
Credit Cards
Check Cards
More...
Lending
Mortgage
Home Equity New!
Education Loans
Vehicle Loans
Rates
Mortgage Rates
Home Equity Rates
Credit Card Rates
Payment Challenges?
Explore your loan options
Save up to 30% on TurboTax.
Small Business customers save big on the #1 rated tax software.
Save Now
The time is now.
Mortgage rates are at an all-time low.
Refinance Today
Search
Search Tips
What to Expect:
Homeowner Affordability & Stability Plan
Learn More
WACHOVIA SECURITIES
An industry leader in investment and advisory services for individuals, corporations and institutions.
SMALL BUSINESS
The tools, services, and research to manage your company.
Small Business Login
ONLINE BANKING.
Securely manage your business finances online.
Wachovia Business Online.
CORPORATE & INSTITUTIONAL
Wachovia Securities Corporate and

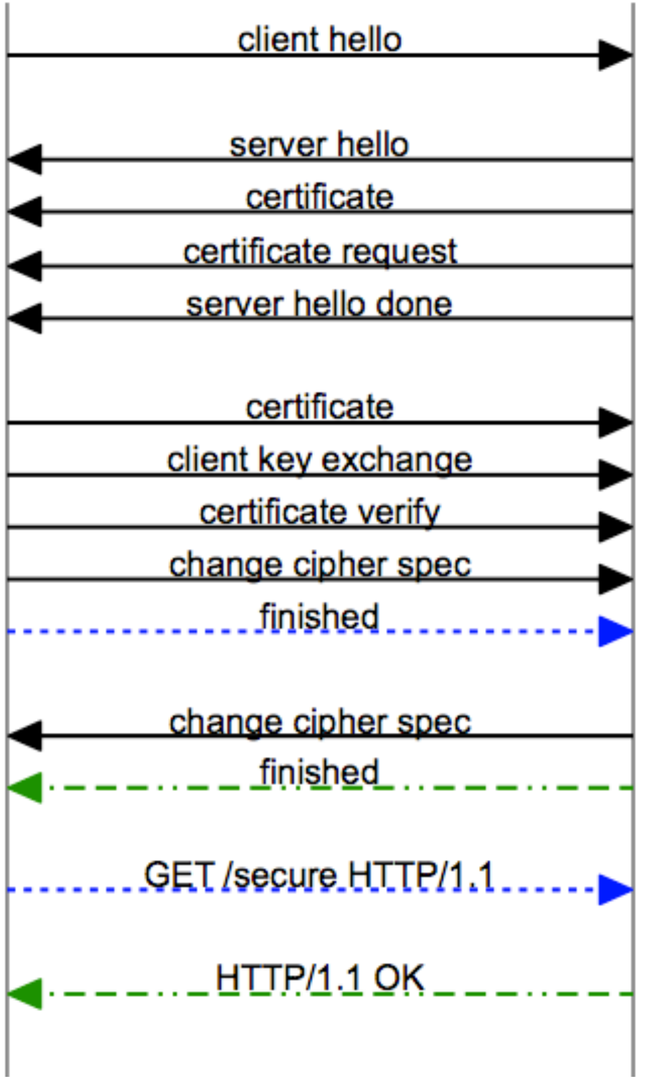
Injecting Prefixes

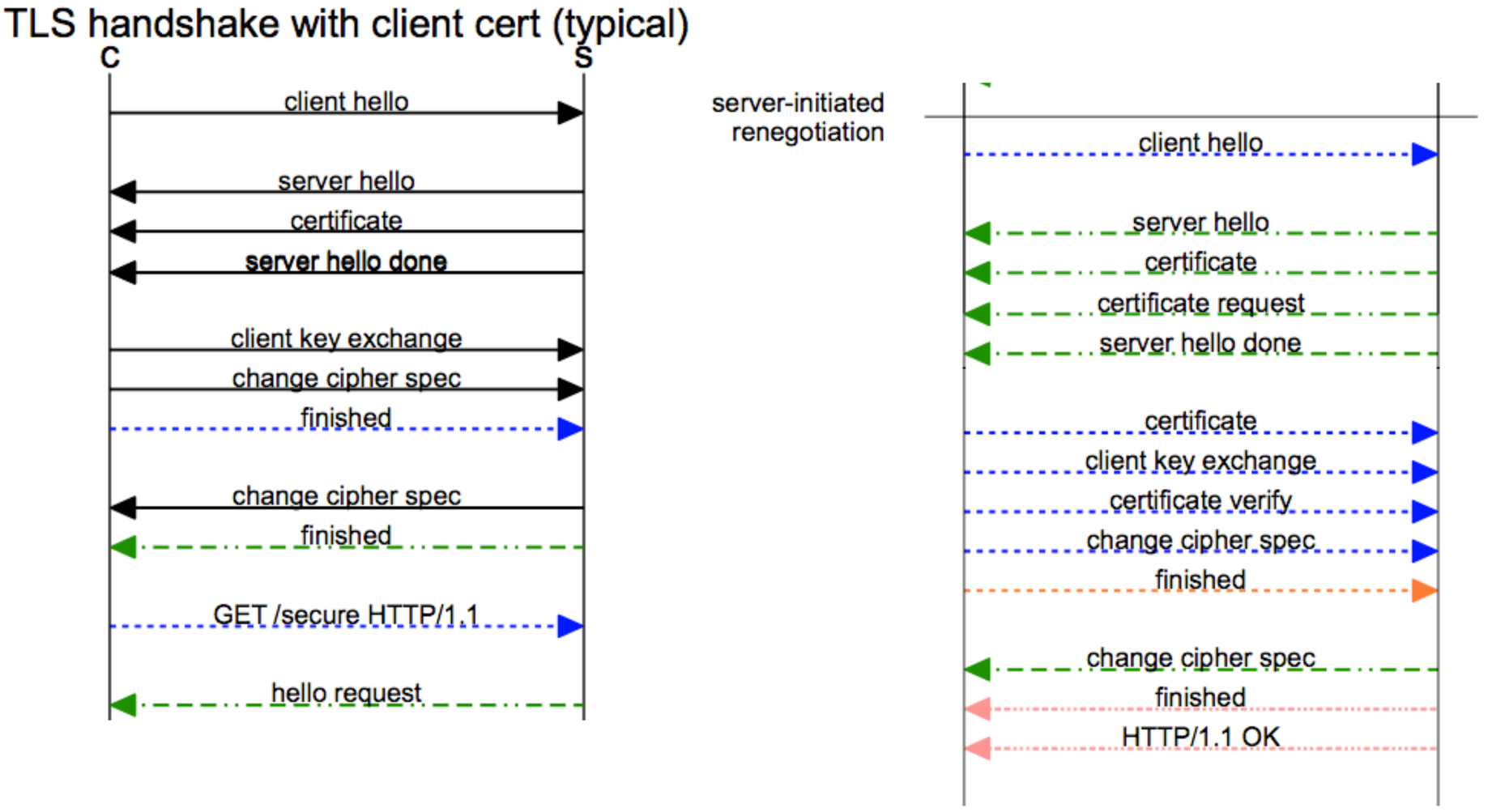
- Ray, Dispensa, 11/2009:
  - Many web servers require client-side auth, but only for certain resources

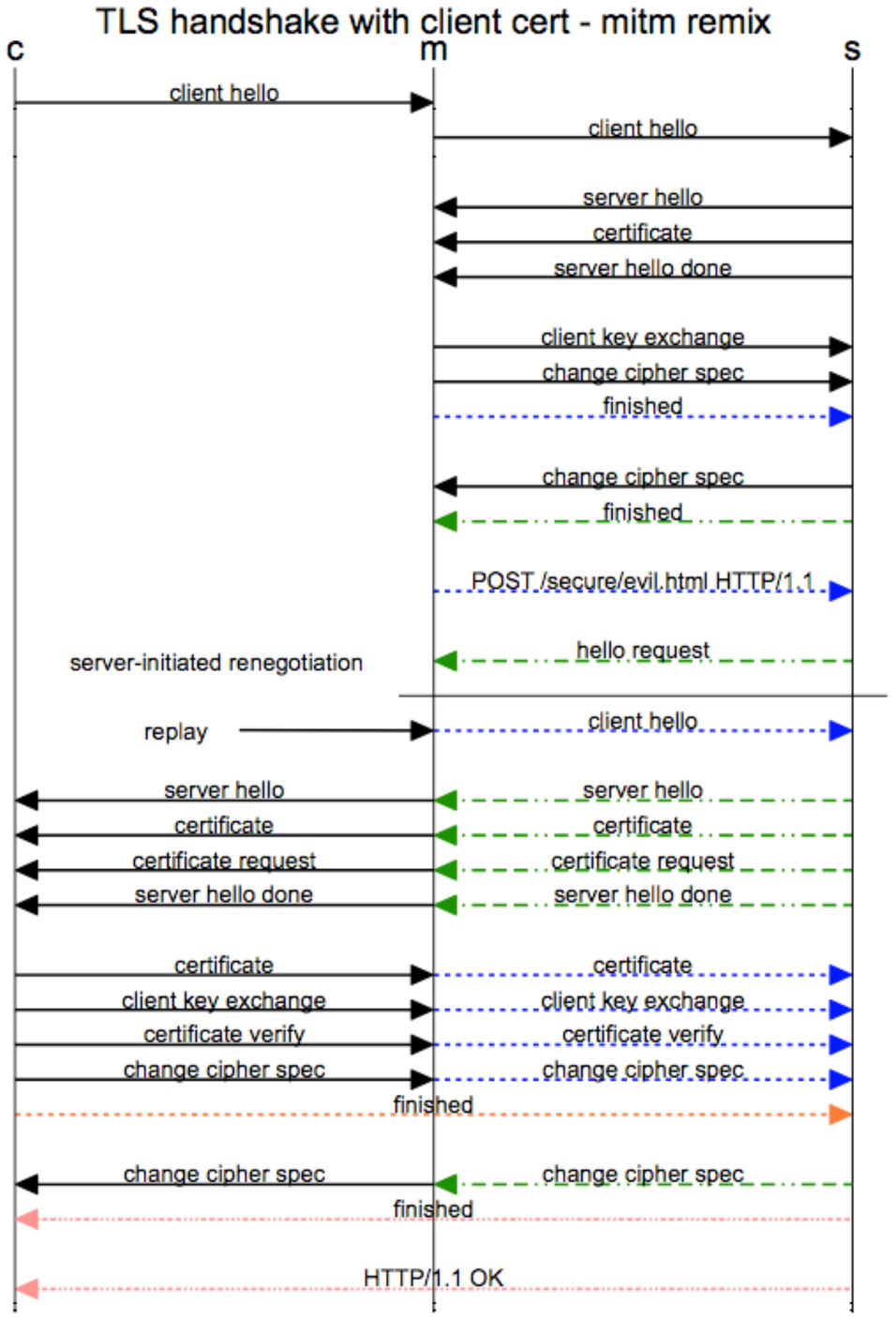
```
GET /highsecurity/index.html HTTP/1.1
Host: example.com
Connection: keep-alive
```

  - This may require an on-the-fly TLS re-negotiation

TLS handshake with client cert (ideal)




TLS handshake with client cert (typical)
C
S
client hello
server hello
certificate
server hello done
client key exchange
change cipher spec
finished
change cipher spec
finished
GET /secure HTTP/1.1
hello request
server-initiated
renegotiation
client hello
server hello
certificate
certificate request
server hello done
certificate
client key exchange
certificate verify
change cipher spec
finished
change cipher spec
finished
HTTP/1.1 OK


TLS handshake with client cert - mitm remix
c
m
s
client hello
client hello
server hello
certificate
server hello done
client key exchange
change cipher spec
finished
change cipher spec
finished
POST /secure/evil.html HTTP/1.1
server-initiated renegotiation
hello request
replay
client hello
server hello
certificate
certificate request
server hello done
server hello
certificate
certificate request
server hello done
certificate
client key exchange
certificate verify
change cipher spec
finished
certificate
client key exchange
certificate verify
change cipher spec
change cipher spec
finished
HTTP/1.1 OK

DECT

- Digital Enhanced Cordless Telephone protocol
  - European standard, now in US
  - Interoperable devices
  - Connects base station (FT) to handsets (PT)
- Tools:
  - DECT Standard Cipher (DSC)
  - DECT Standard Authentication Algorithm (DSAA)

DECT

- Step 1: Pairing
  - User enters a 4-digit PIN into handset and base
  - Base generates a 64-bit seed, combined with PIN to generate shared key (UAK)
  - Base and handset conduct challenge/re

Total entropy of UAK:
77.288 bits (64-bit seed + PIN)
Much less if PRNG is bad!

DECT

- Step 2: Authentication
  - Two 

commended one:

In common mode,
only the handset is
authenticated!

DECT Attack

- Step 2: Authentication
  - Two commended one:

ode?

DECT, other

- A11, A12 built from weak cipher
  - Authors show how this cipher can be inverted using some clever attacks
  - Leaves room for attacks
    even if protocol bug fixed
  - Eerily reminiscent of GSM...

•Weak protocols

•Weak homebrew ciphers

Example: DTCP

- BluRay & HD-DVD Disks
  - Contains “protected” area that can’t be read using normal Drive protocol
  - Embeds secret “Binding Nonce”
- 

DTCP Protocol

- Digital Transmission Content Protection
  - Runs between Drive and Host
  - Encrypts & Authenticates Communications

DTCP

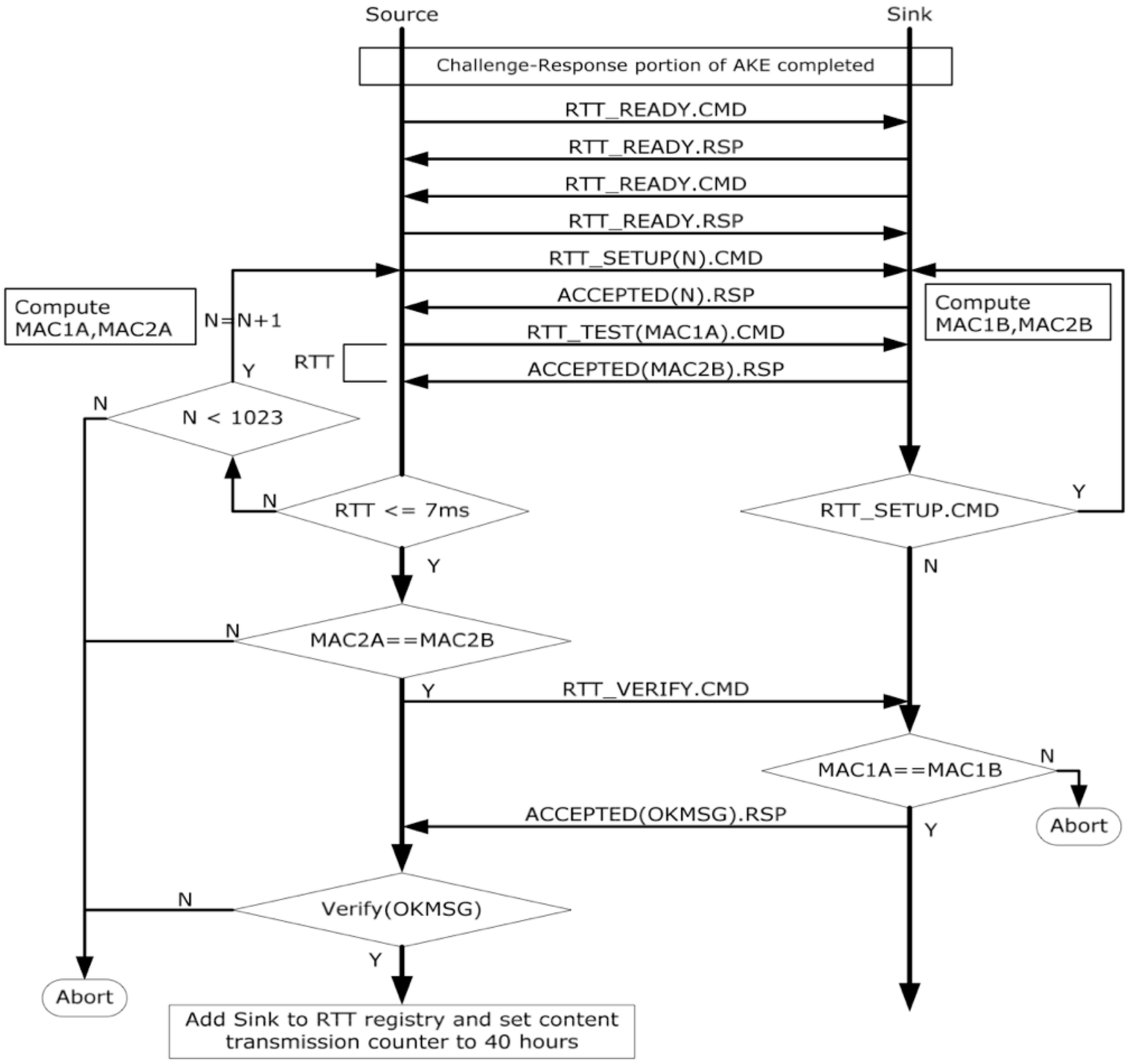
- One layer of protection for HD-DVD/BluRay
  - Encrypts/authenticates content traversing unprotected bus lines

Attacker

DTCP AKE

- Authenticated Key Exchange
  - EC Diffie-Hellman Protocol
  - Each device has a certificate & secret key
  - Devices also have a certificate revocation list, to prevent communication with hacked devices

DTCP AKE (v1.4)


Source
Sink
Challenge-Response portion of AKE completed
RTT_READY.CMD
RTT_READY.RSP
RTT_READY.CMD
RTT_READY.RSP
RTT_SETUP(N).CMD
ACCEPTED(N).RSP
RTT_TEST(MAC1A).CMD
ACCEPTED(MAC2B).RSP
Compute MAC1A,MAC2A
N=N+1
RTT
Compute MAC1B,MAC2B
Y
N
N < 1023
N
RTT <= 7ms
RTT_SETUP.CMD
Y
Y
N
N
MAC2A==MAC2B
Y
RTT_VERIFY.CMD
MAC1A==MAC1B
N
Abort
ACCEPTED(OKMSG).RSP
Y
N
Verify(OKMSG)
Y
Abort
Add Sink to RTT registry and set content transmission counter to 40 hours

Other Attacks

- Replay Attacks
  - Attacker replays older messages
  - Can be countered with timestamps, nonces and sequence counters
- Cut & Paste
  - Malleable encryption scheme like CBC
  - Can be countered with MACs
- Reflection
  - If party A sends a message, just bounce it back

Discussion

- We’ve seen standards with problems
  - Usually the cryptanalysis comes after the standard is released, and products in the field
  - Why?

Next Time

- Next lecture:
  - How do we design secure protocols?

END

Ciphersuite Rollback

Bank of America

Bank of Opportunity™

Ciphersuite Rollback

Bank of America

Bank of Opportunity™

Ciphersuite Rollback

- Big caveat:
  - Only works when client asks for authentication <u>without</u> encryption

Bank of America

Bank of Opportunity™

Server thinks encryption is disabled, but gets an encrypted MAC