

650.445: Practical Cryptographic Systems Protocols

Instructor: Matthew Green

Review

- **Last time:**
 - **Weds: Attacks on protocols (TLS)**
 - **Sun: Submitted A2 (?)**

Reading and Midterm

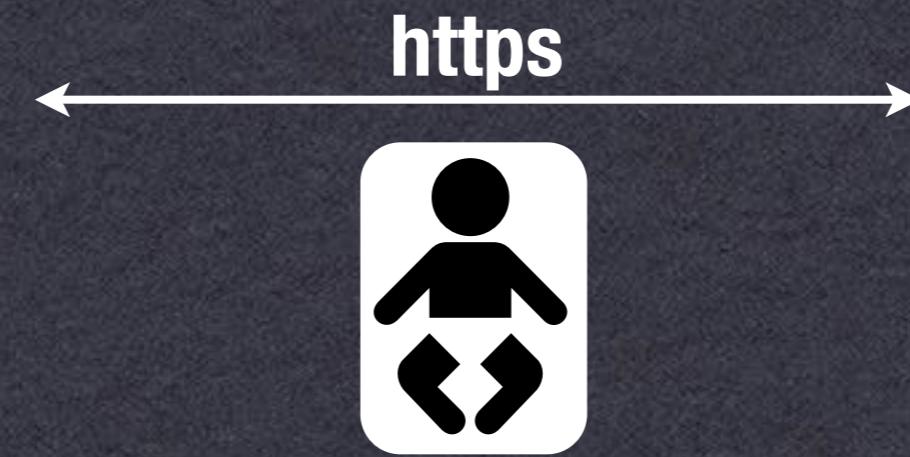
- 26th of October
- Do the reading, please QUIZ MONDAY
 - Anderson, Physical Tamper Resistance
 - Gutmann, Lessons Learned
 - Adam Langley, GotoFail
 - Cache timing attacks on AES
 - Kocher: Timing attacks
 - Bardou et al.: Efficient Padding Oracle Attacks

Reading and Midterm

- 26th of October [will not cover Bitcoin]
- Do the reading, please
 - Anderson, Physical Tamper Resistance
 - Gutmann, Lessons Learned
 - Adam Langley, GotoFail
 - Cache timing attacks on AES
 - Kocher: Timing attacks
 - Bardou et al.: Efficient Padding Oracle
 - Checkoway et al. Systematic analysis
 - ZRTP Protocol

SSL/TLS

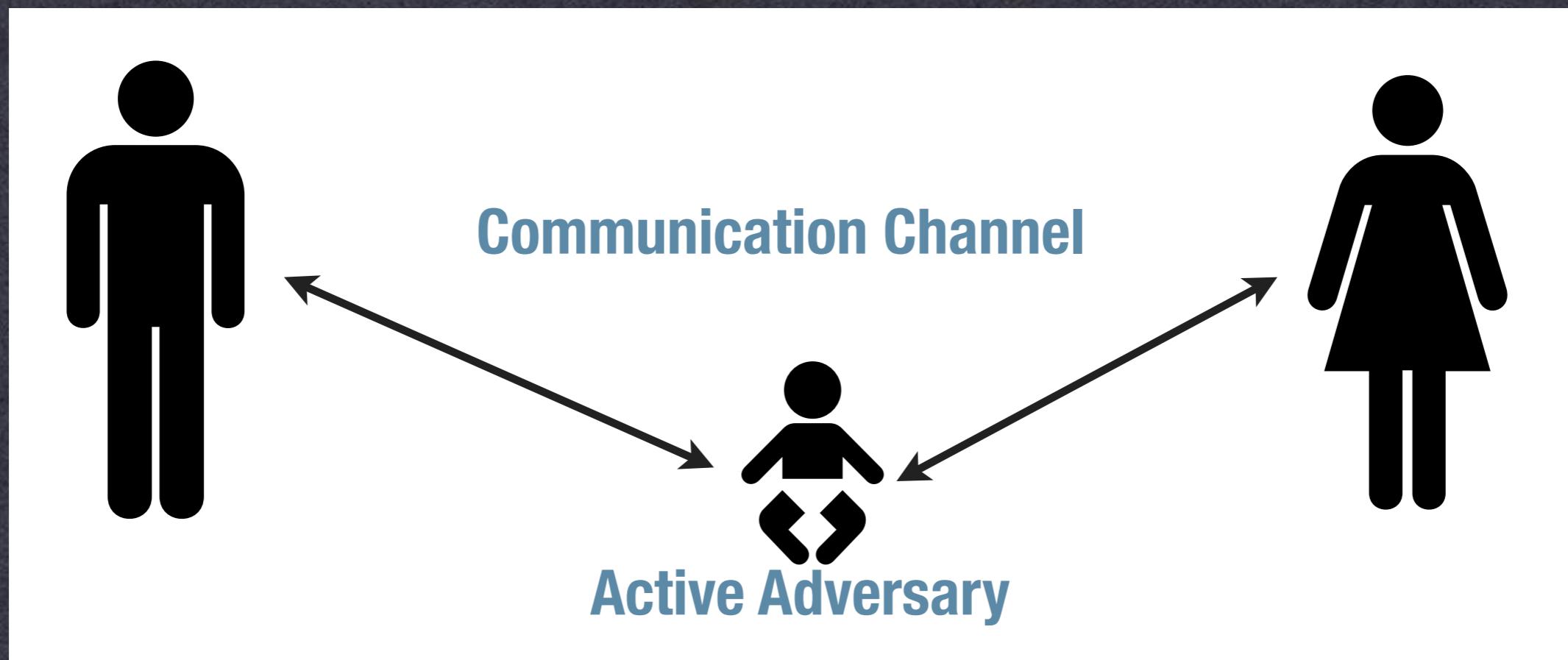
- Transport-layer security protocol
 - Often used to secure reliable protocols (TCP)
 - Does not require pre-shared keys
 - Most common usage: https
- E-commerce (\$200bn/2008), Banking, etc.



Threat Model

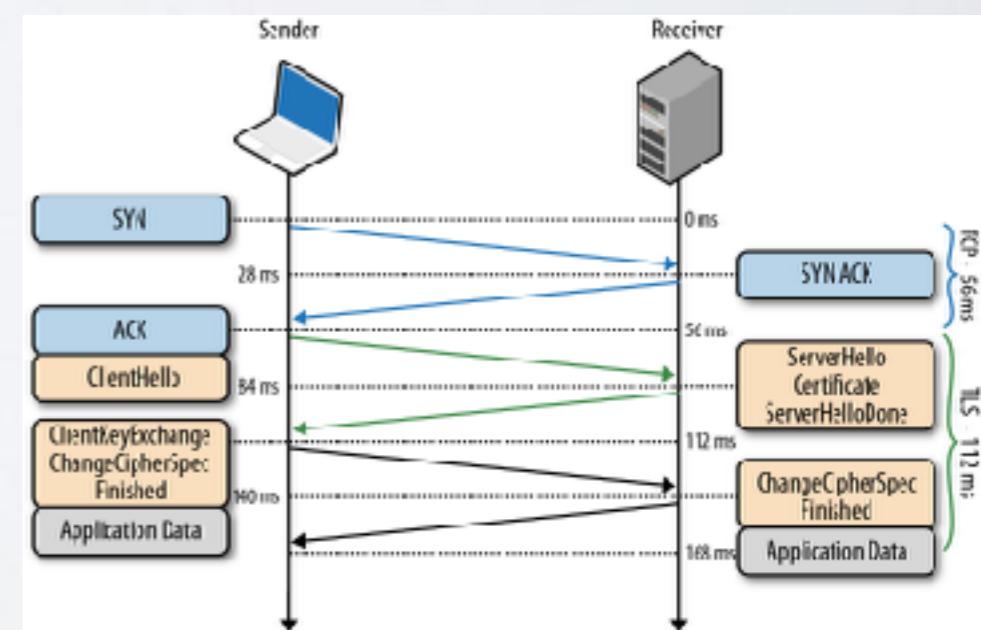


Threat Model



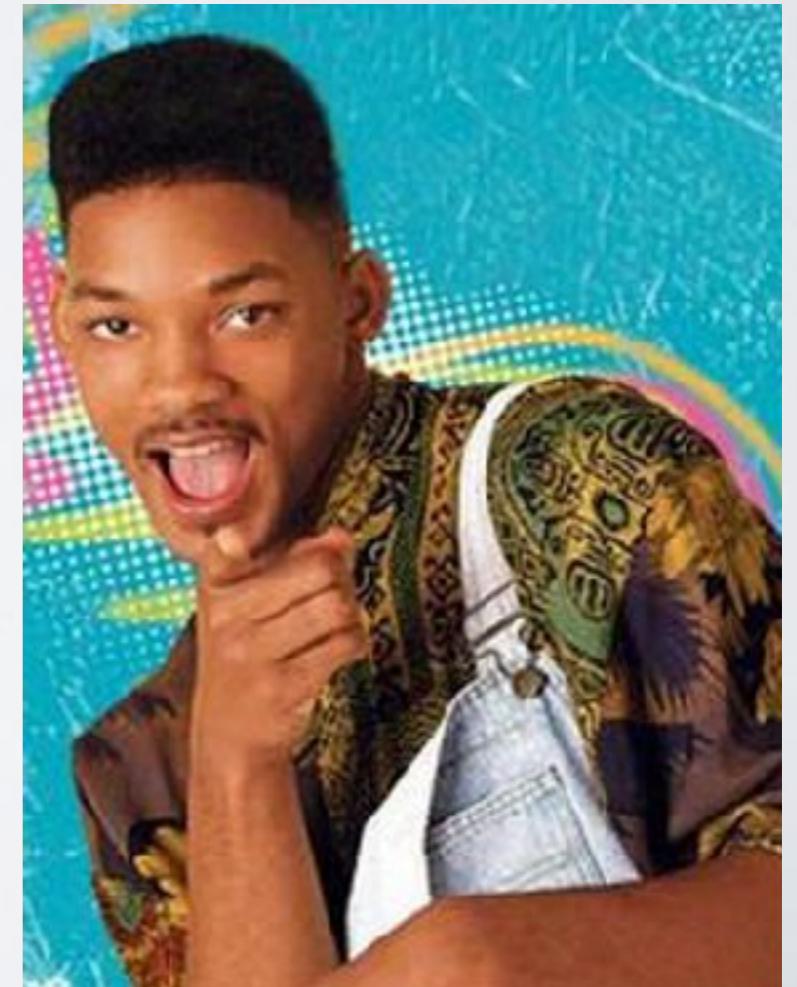
SSL/TLS

- **Most important security protocol on the Internet**
 - Allows secure connections between clients & servers
 - Current version: TLS 1.2
 - (But browsers still support SSL 3, TLS 1.0/1.1)
plus 1.3 coming soon!
 - 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



Jonathan Zdziarski
@JZdziarski

 Follow

As tomorrow is April 1, today marks the last day of useful e-commerce before SSL breaks again on Thursday. Hope you made the most of it.

Why these problems?

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

Quite a bit

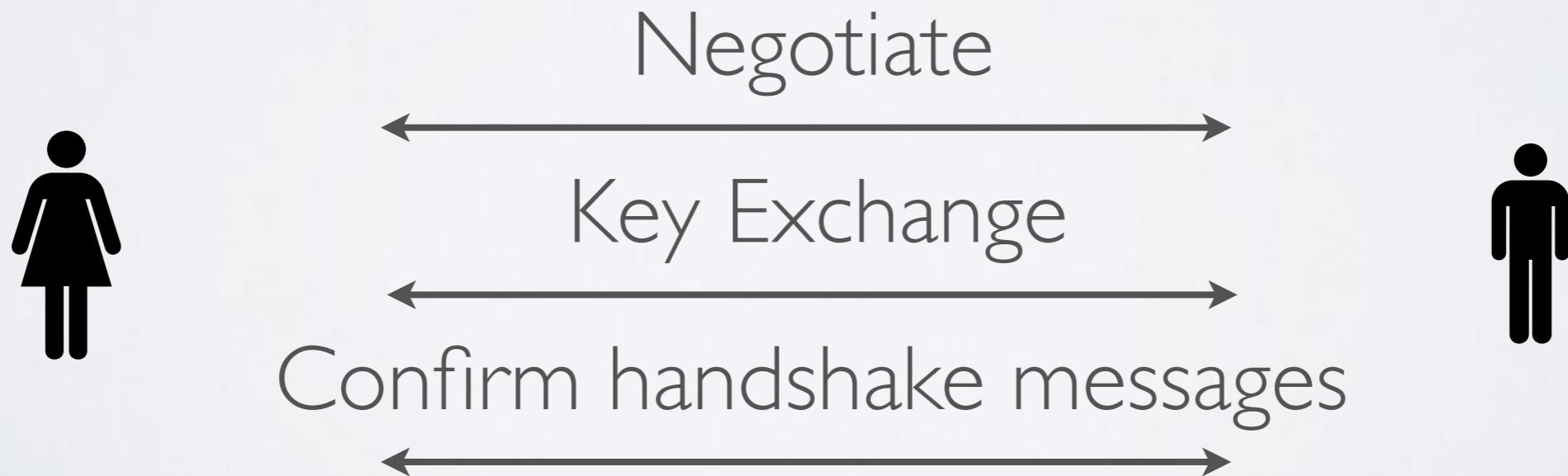
- Many problems result from TLS's use of “*pre-historic cryptography*” (- Eric Rescorla)
- **Export grade encryption**

1995-~2000 (and onward)

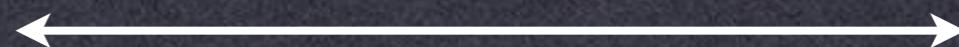
Weakened “ciphersuites” with limited security
(e.g., 512-bit DH/RSA, 40-bit RC4)

TLS Negotiation

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



SSL/TLS



- 1. Negotiate peer capabilities**
- 2. Exchange certificates**
- 3. Session key establishment**
- 4. Secure communications**
- 5. Session expiration/rekeying**



SSL/TLS

- Negotiation:



I choose TLS 1.0
I choose ciphersuite X.

1. Negotiate peer capabilities

2. E

I speak SSL 3.0, TLS 1.0.
I support cipher suites X, Y.
I don't have a client cert.



SSL/TLS

- Certificate Exchange



SSL/TLS

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



$$C = \text{RSA-ENC}_{pk}(\text{seed}_3)$$

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

$$\begin{aligned}\text{seed}_3 &= \text{RSA-DEC}(sk, C) \\ k_s &= H(\text{seed}_1 \parallel \text{seed}_2 \parallel \text{seed}_3)\end{aligned}$$

1. Secure communication
2. Session expiration

$$k_s = H(\text{seed}_1 \parallel \text{seed}_2 \parallel \text{seed}_3)$$



SSL/TLS

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



- ← → Communicate under k_s
1. Negotiate peer capabilities
 2. Exchange certificates
 3. Session key establishment
 4. Secure communications
 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



1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment
4. Secure communications
5. Session expiration/rekeying



Attacks on SSL2

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



I support ciphersuites
X,Y, Ridiculous.



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

SSL3 Handshake

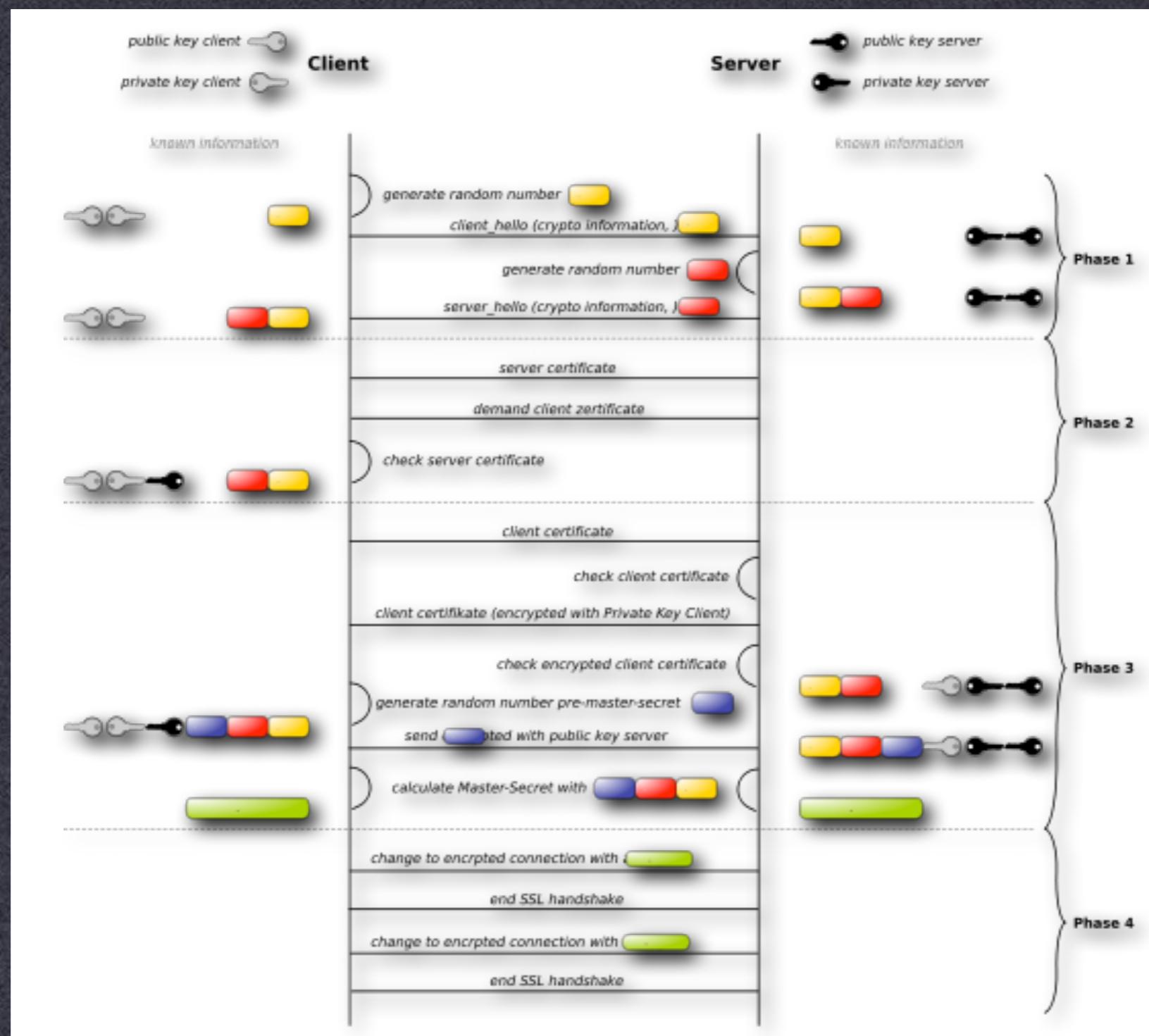


Image from Wikimedia Commons used under a Creative Commons license:
http://commons.wikimedia.org/wiki/File:Ssl_handshake_with_two_way_authentication_with_certificates.svg

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:

```
...
1. C → S : [change cipher spec]
2. C → S : [finished:] {a}k
3. S → C : [change cipher spec]
4. S → C : [finished:] {a}k
5. C → S : {m}k
...
```

CCS Rollback

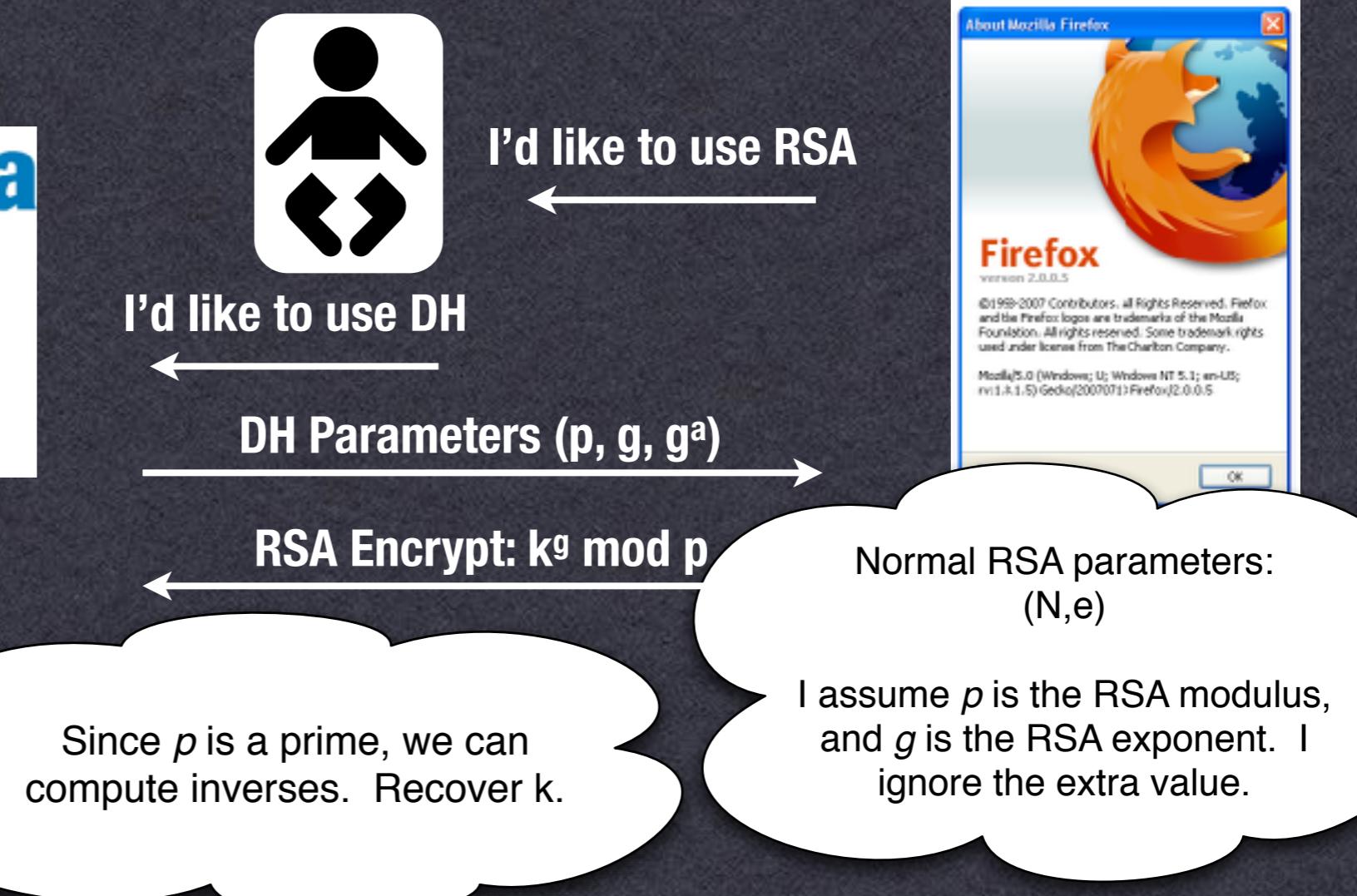
- MITM attack:

```
...
1.  C → M : [change cipher spec]
2.  C → M : [finished:] {a}k
2'. M → S : [finished:] a
3.  S → M : [change cipher spec]
4.  S → M : [finished:] {a}k
4'. M → C : [finished:] a
5.  C → M : {m}k
5'. M → S : m
...
...
```

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



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:

GET / HTTP/1.1

Host: cnn.com

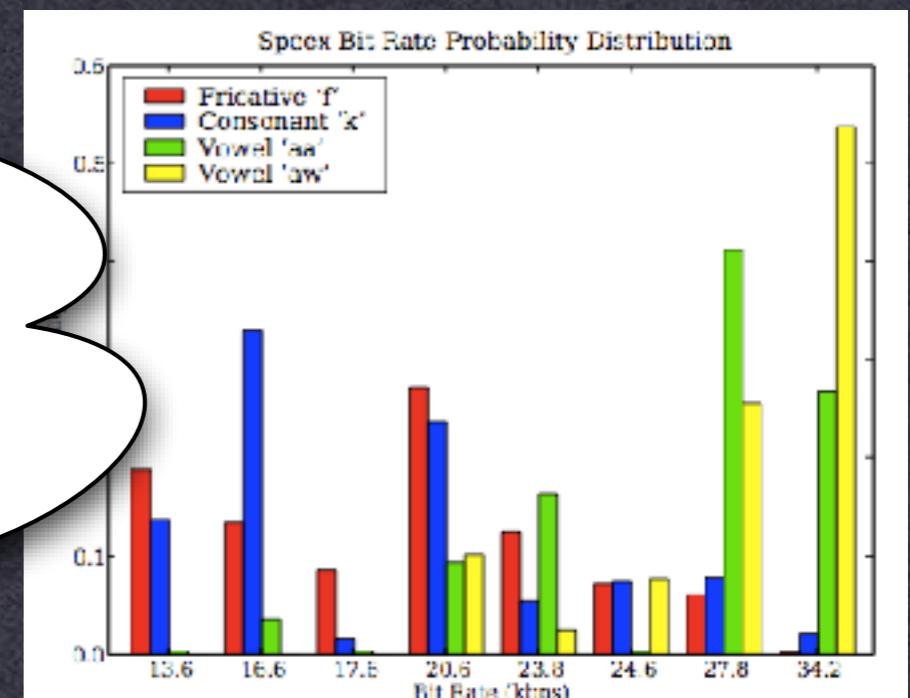
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_6; en-us) AppleWebKit/525.27.1 (KHTML, like Gecko) Version/3.2.1 Safari/525.27.1

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

Traffic Analysis++

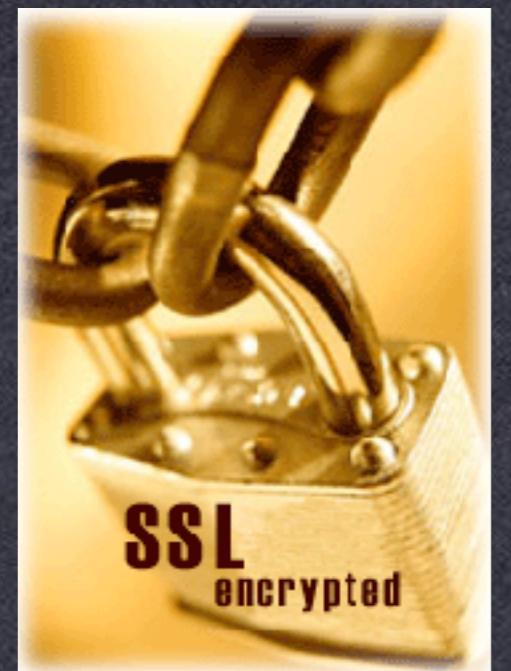
- Digression: The case of encrypted VoIP
 - Some VoIP protocols use VBR encoding, size of data packets depends on signal
 - Also include “silence suppression” (VAD)
 - Therefore, total traffic is highly correlated to the contents of the line.

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



SSL Stripping & Pinning

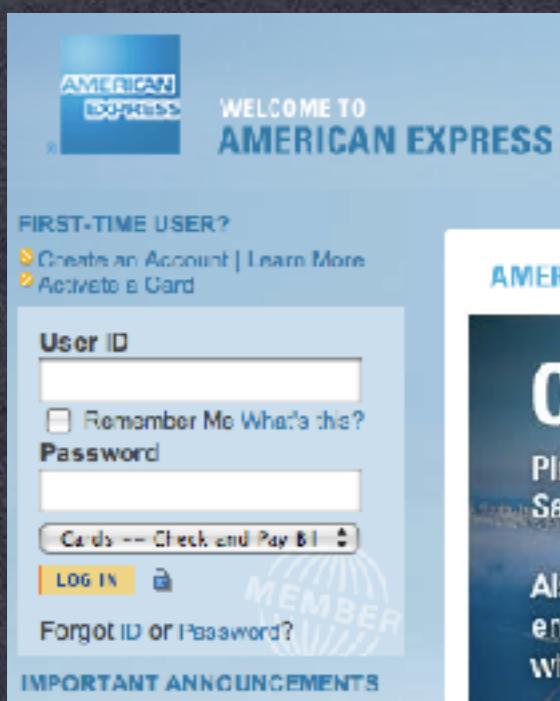
- Moxie Marlinspike: SSLStrip
- Does not break SSL
- Instead: takes advantage of the way SSL is used



HTTP->HTTPS

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

User enters: americanexpress.com



GET http://americanexpress.com

REDIRECT https://americanexpress.com

GET https://americanexpress.com

SSL secured web page

User login info





https://home.americanexpress.com/home/mt_personal_cm.shtml?



Login page: https



WELCOME TO
AMERICAN EXPRESS

PERSONAL CARDS

TRAVEL

SMALL BUSINESS

CORPORATIONS

MERCHANTS

Global Sites | Help | Contact Us |

Need Help?

FIRST-TIME USER?

- [Create an Account](#) | [Learn More](#)
- [Activate a Card](#)

User ID

Remember Me [What's this?](#)

Password

Cards -- Check and Pay Bill



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



← Car Rental Pro

← Share the Ben

← Only in San Fran

← Travel your wa

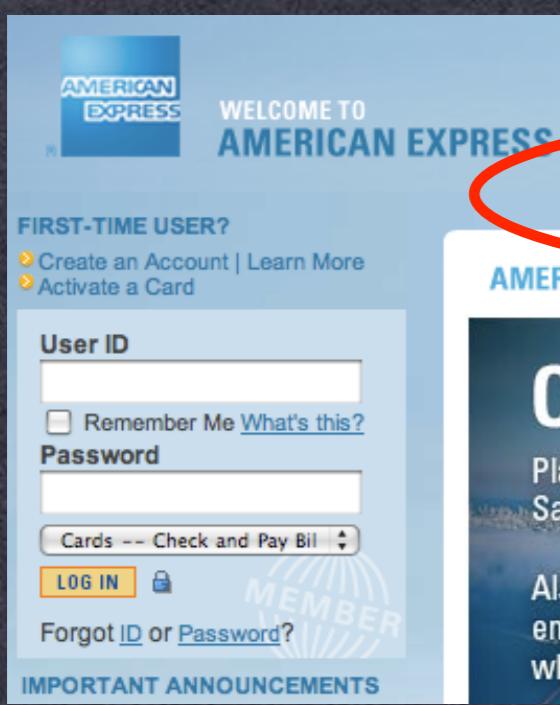
← American Expl

← Shop Online w

HTTP->HTTPS

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

User enters: americanexpress.com



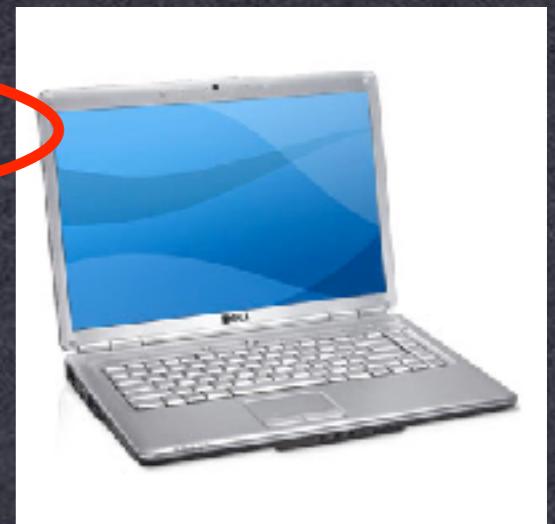
GET http://amex.com

REDIRECT http://secure.amex.com

GET https://secure.amex.com

SSL secured web page

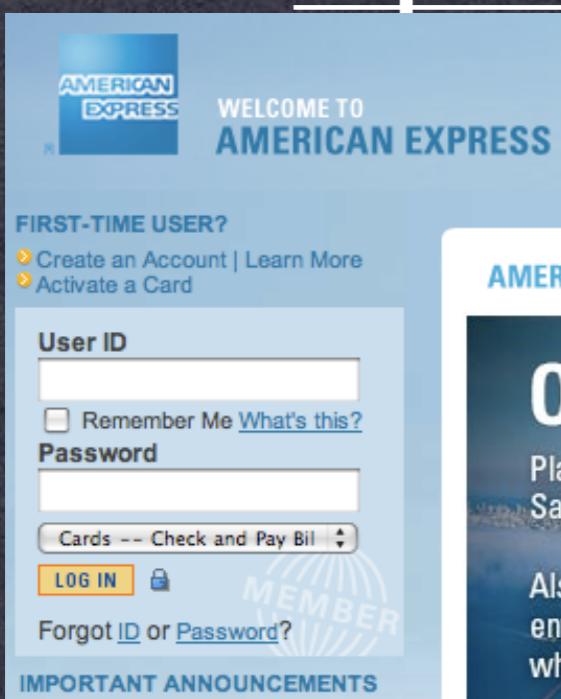
User login info



HTTP->HTTPS

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

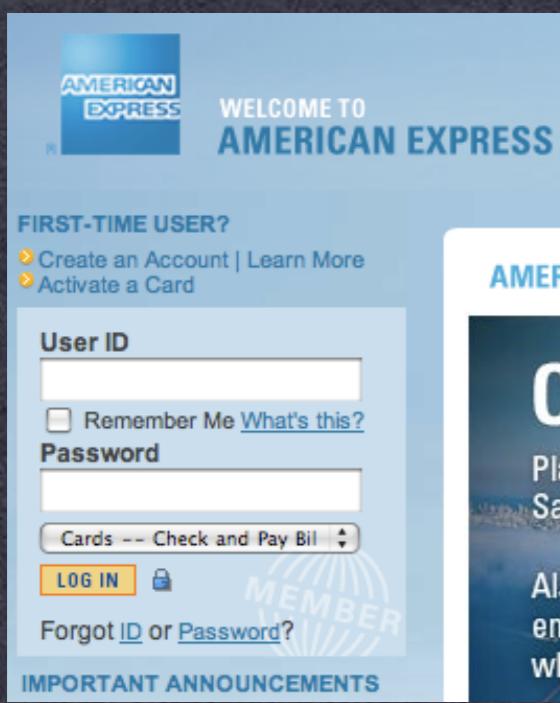
<https://www.gmail.com/accounts/ServiceLogin!f.ijjk.cn>



HTTP->HTTP->HTTPS

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

User enters: americanexpress.com



A screenshot of the American Express login page. The URL in the address bar is http://americanexpress.com. The page features the American Express logo and a "WELCOME TO AMERICAN EXPRESS" header. It includes fields for "User ID" and "Password", and a "LOG IN" button. A lock icon is present next to the login button, indicating that the connection is unsecured.

GET http://americanexpress.com



Unsecured http web page

User login info



 http://wachovia.com/

Google

[Customer Service](#) | [Contact Us](#) | [Locations](#)

Login page: http

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 PlusSM](#)[Online Services Guarantee](#)**Sign Up for Online Banking**[Sign Up](#) | [Learn More](#) | [Demo](#)**LOCATIONS**ZIP: **Find**[More Search 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 >>](#)

Great News
about Free Online Statements—
Now with up to 7 years of
Online Statement history.

[See More >](#)**En español****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

 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

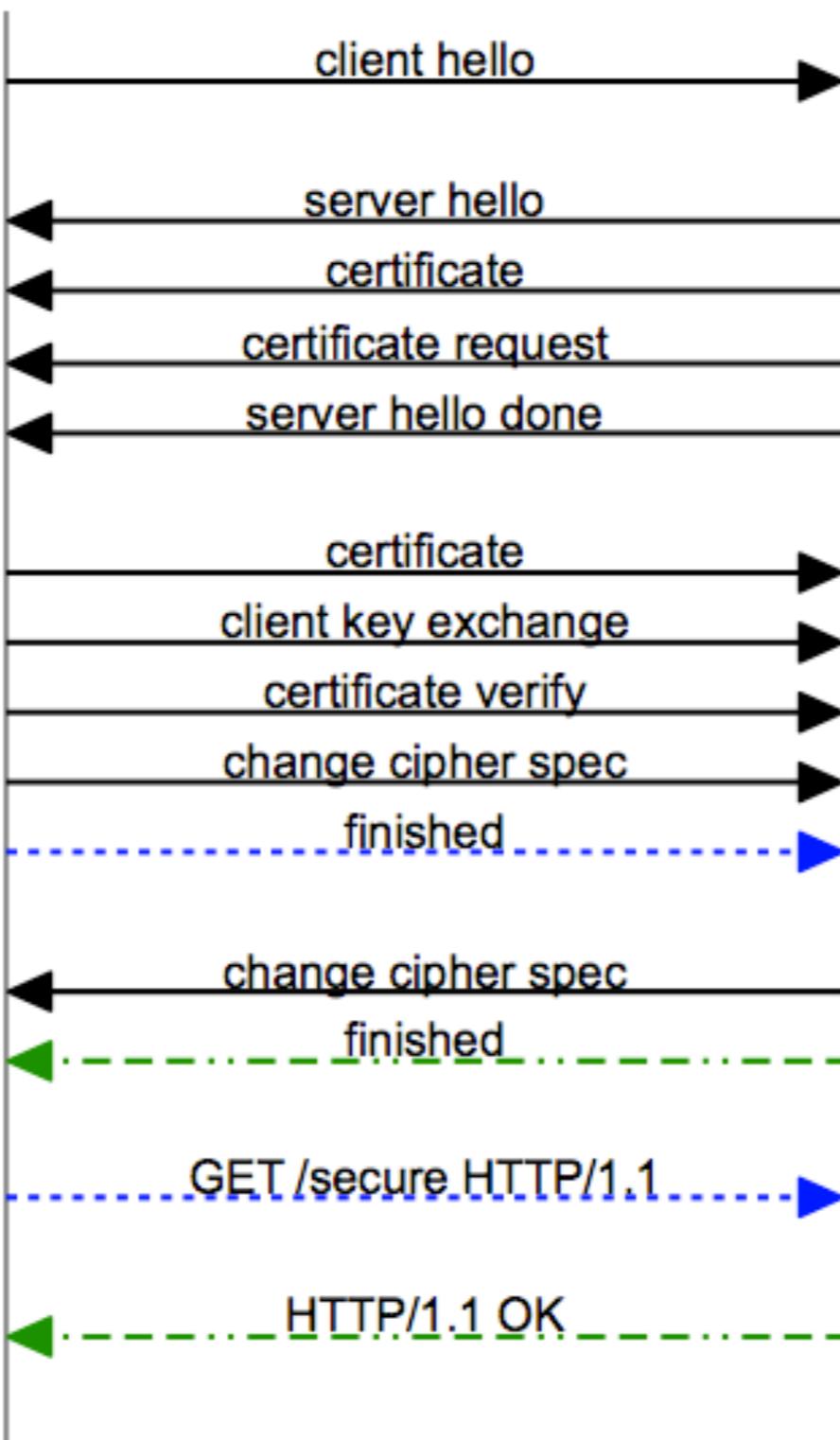
Injecting Prefixes

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

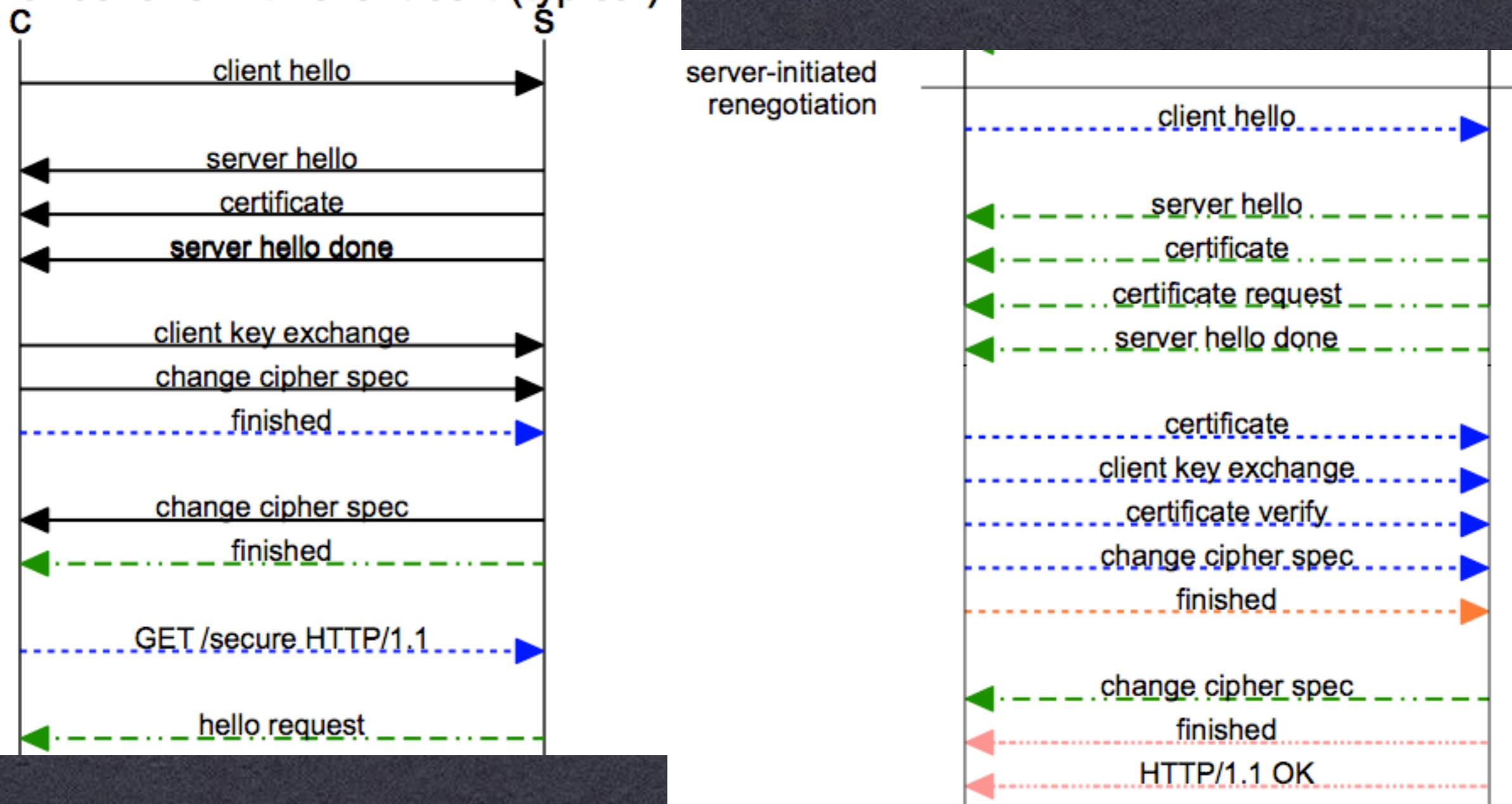
```
GET /highsecurity/index.html HTTP/1.1
Host: example.com
Connection: keep-alive
```

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

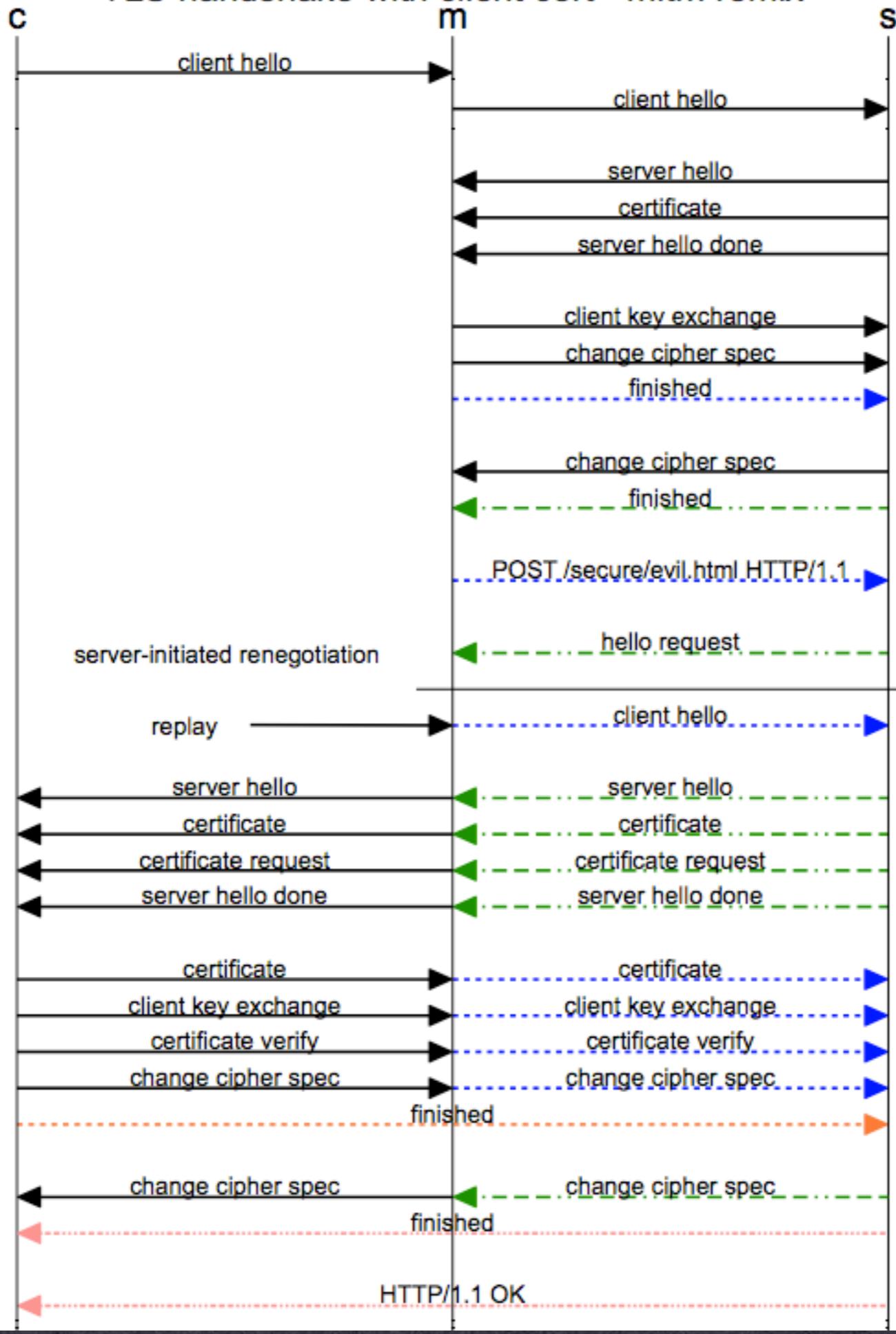
TLS handshake with client cert (ideal)



TLS handshake with client cert (typical)



TLS handshake with client cert - mitm remix



DECT

- **Digital Enhanced Cordless Telephone protocol**
 - European standard, now in US
 - Interoperable devices
 - Connects base station (FT) to handset (DT)
- 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/response handshake

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



DECT

- Step 2: Authentication
 - Two protocols, recommended one:



$\text{AS} = \text{A11(UAK, RS)}$
 $k, \text{SRES} = \text{A12(AS, RAND_F)}$

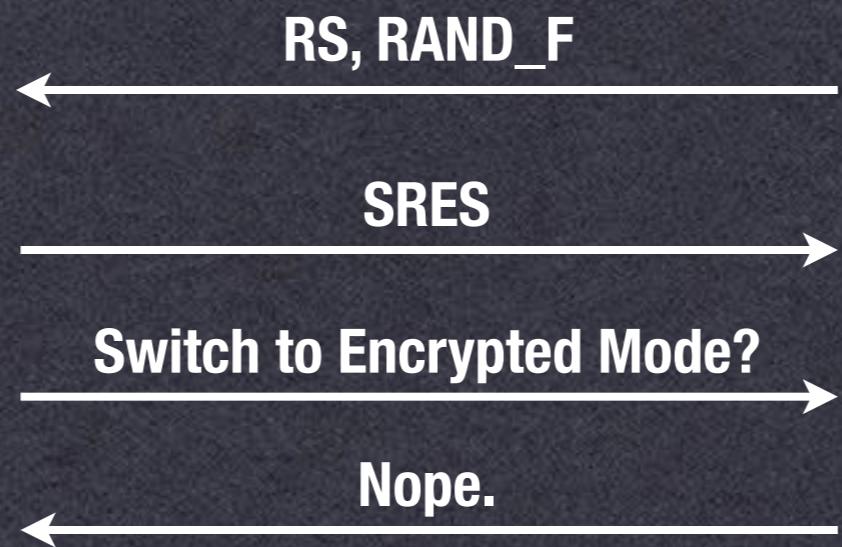


$\text{AS} = \text{A11(UAK, RS)}$
 $k, \text{XRES} = \text{A12(AS, RAND_F)}$

$\text{SRES} == \text{XRES?}$

DECT Attack

- Step 2: Authentication
 - Two protocols, recommended one:



$AS = A11(UAK, RS)$
 $k, SRES = A12(AS, RAND_F)$



$AS = A11(UAK, RS)$
 $k, XRES = A12(AS, RAND_F)$

$SRES == XRES?$

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

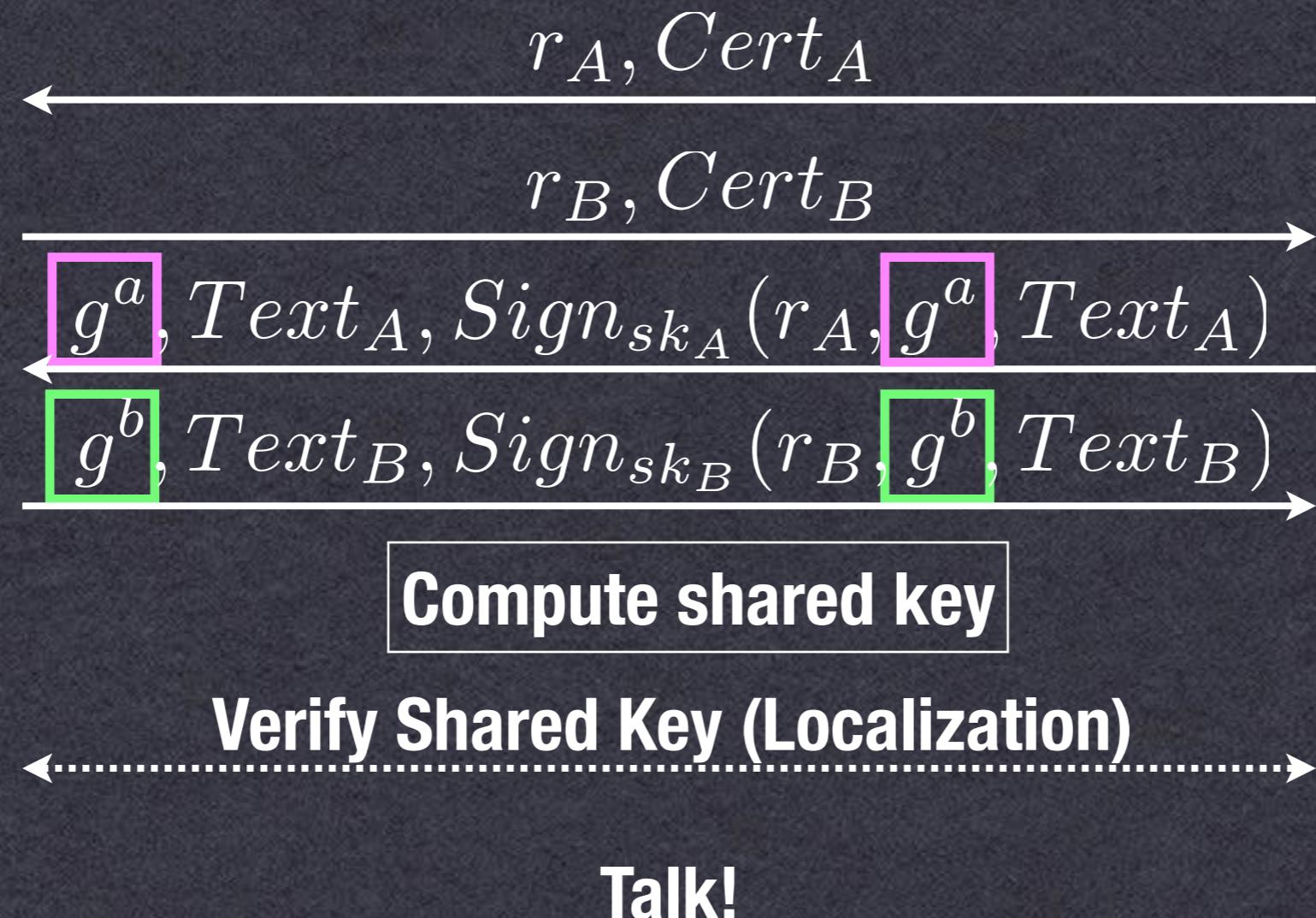
- One layer of protection for HD-DVD/BluRay
 - Encrypts/authenticates content traversing unprotected bus lines

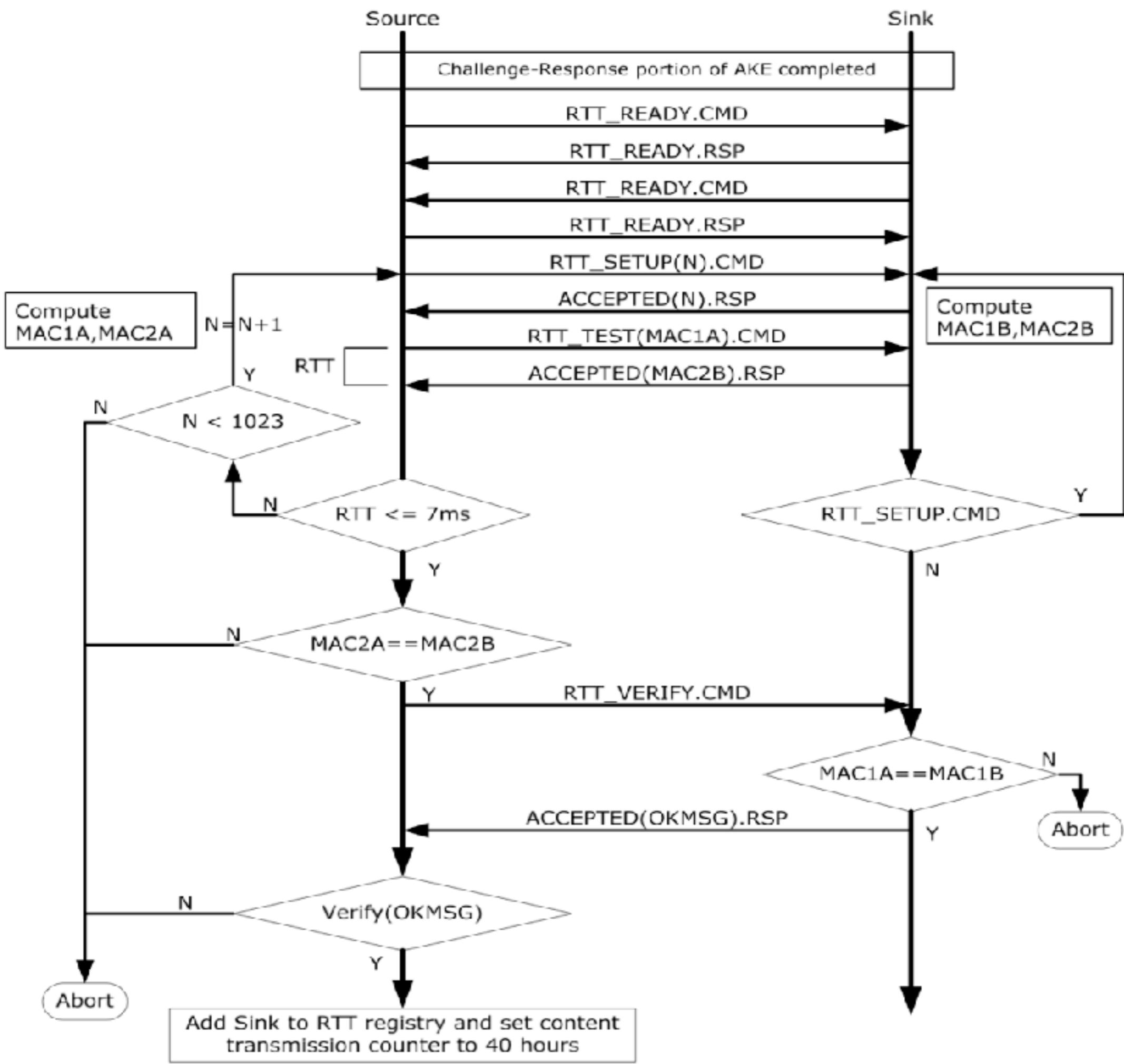


DTCP AKE

- **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)





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

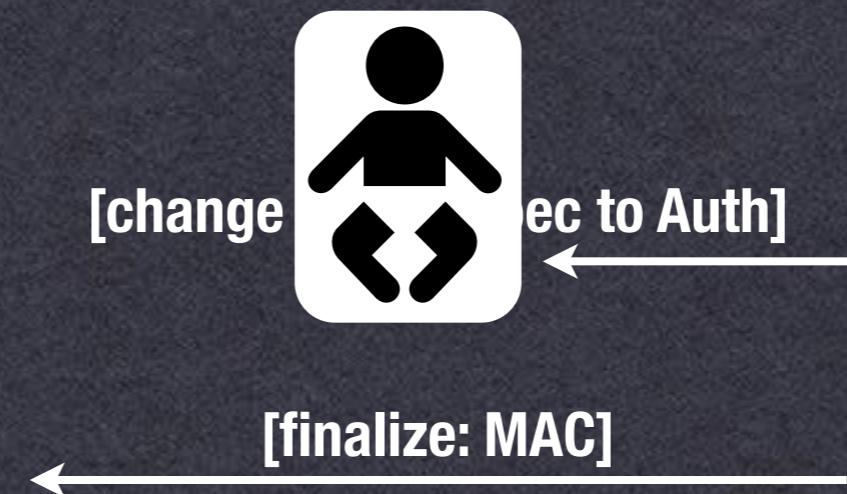


[change cipher spec to Auth]

[finalize: MAC]

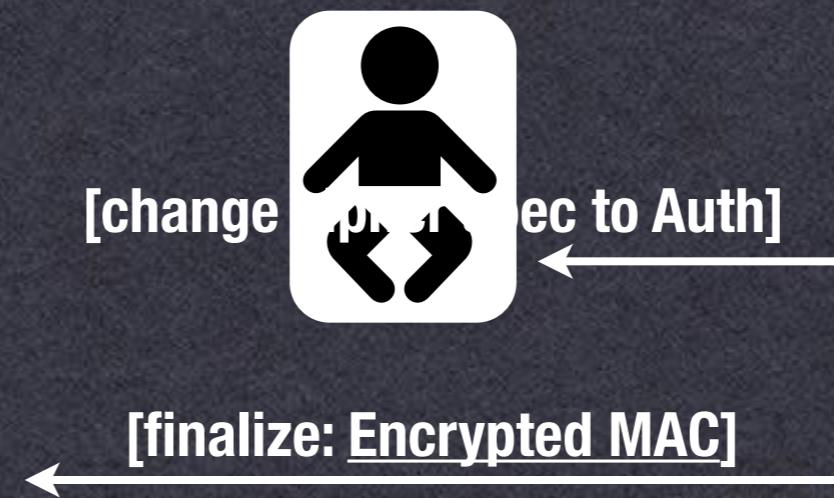


Ciphersuite Rollback



Ciphersuite Rollback

- Big caveat:
 - Only works when client asks for authentication without encryption



Server thinks encryption is disabled, but gets an encrypted MAC