Practical Cryptographic Systems

Protocols

Instructors: Matthew Green and Alishah Chator

Review

- Last time:
  - Protocols (TLS intro, problems in SSLv2)
- Today:
  - More TLS, attacks on SSL/TLS historically, TLS1.3!
  - Next: Signal protocol and forward secrecy

Logistics stuff

- Midterm at end of month
- Project proposal due today!
- Do the reading! We will be including more details on next assignment
- A2 MONDAY (we hope)

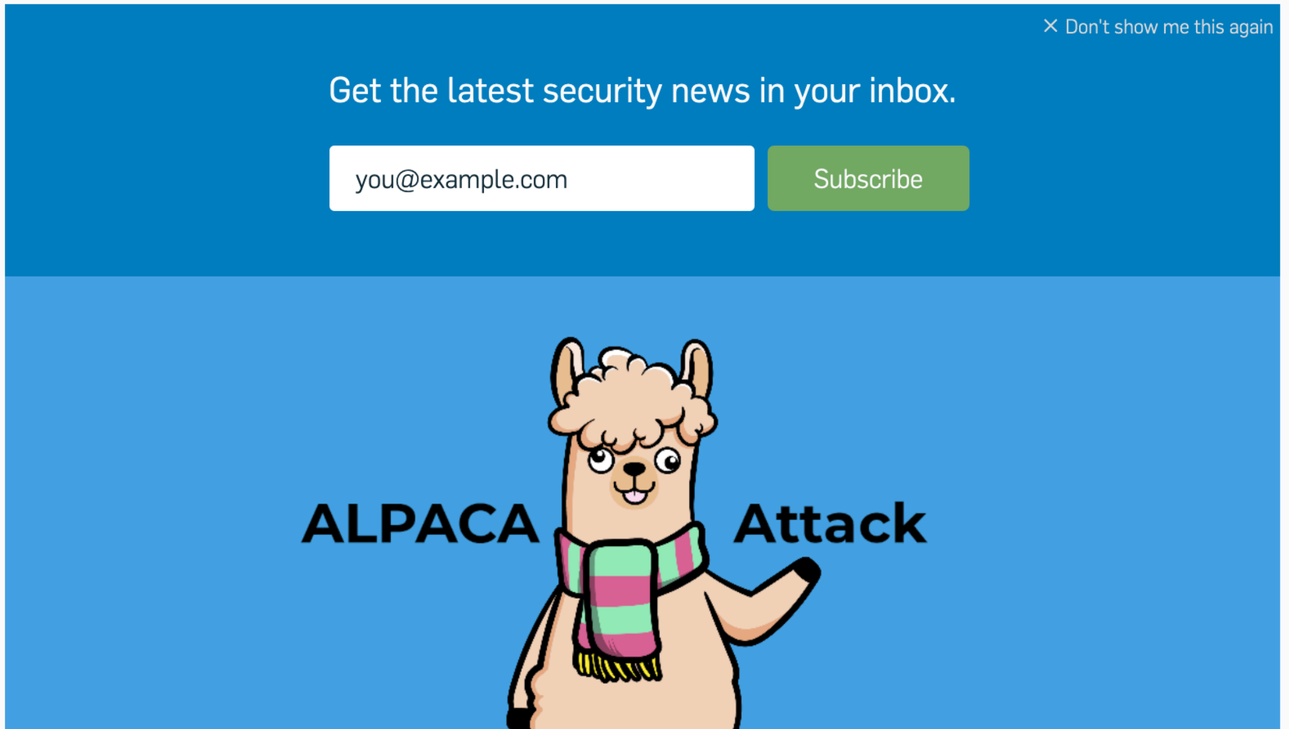
News?

News?

ALPACA – the wacky TLS security vulnerability with a funky name

11 JUN 2021 22

Vulnerability



News?

A huge security hole

XSS is a huge web security hole, because the reflected script can access data such as login cookies specific to the site you're currently visiting, and thereby steal your login, raid your shopping cart, or otherwise poke its nose into your online business.

Email servers, on the other hand, don't generally deal with JavaScript, and their replies are supposed to make sense to email sending applications, so there's a chance that aiming a browser at a mail server and sending a carefully crafted but fake web request…

…might cause the email server to produce, inamongst its output, an error message that **hasn't gone through the same scrupulous anti-XSS checking that would happen in a web server**.

You're probably once again thinking, "*So what? If the email server sends back some rogue, reflected JavaScript, what harm would that do? There aren't any session coookies, shopping carts or other private web data associated with the email server, so an attacker would get nowhere.*"

Except for one thing: the browser **thinks it's connected to the real web server**, and it made that decision because it was presented with a TLS certificate that would have been valid for the web server, if indeed that's where it had ended up.

Therefore the rogue script reflected by the well-meaning email server **would be able to read out the**

News?

DHS UNVEILS ROADMAP FOR POST-QUANTUM CRYPTOGRAPHY TRANSITION; SECRETARY ALEJANDRO MAYORKAS QUOTED

Carol Collins October 5, 2021 News, Technology, Wash100

Alejandro Mayorkas
Secretary DHS

The Department of Homeland Security has released a guidance to assist organizations in securing their data and systems and mitigating risks and in preparing for the transition to post-quantum cryptography.

The roadmap was developed in collaboration with the Department of Commerce's National Institute of Standards and Technology (NIST) and was meant to offer guidance on the identification, prioritization and protection of susceptible data and algorithms, DHS said Monday.

Alejandro Mayorkas, secretary of DHS and 2021 Wash100 Award recipient, noted that as quantum computing emerges as a scientific breakthrough, it also poses new risks to data privacy and cybersecurity.

One of the roadmap's recommendations is to instruct chief information officers to expand their engagement with standards developing institutions to gain information on the latest developments and changes in protocols.

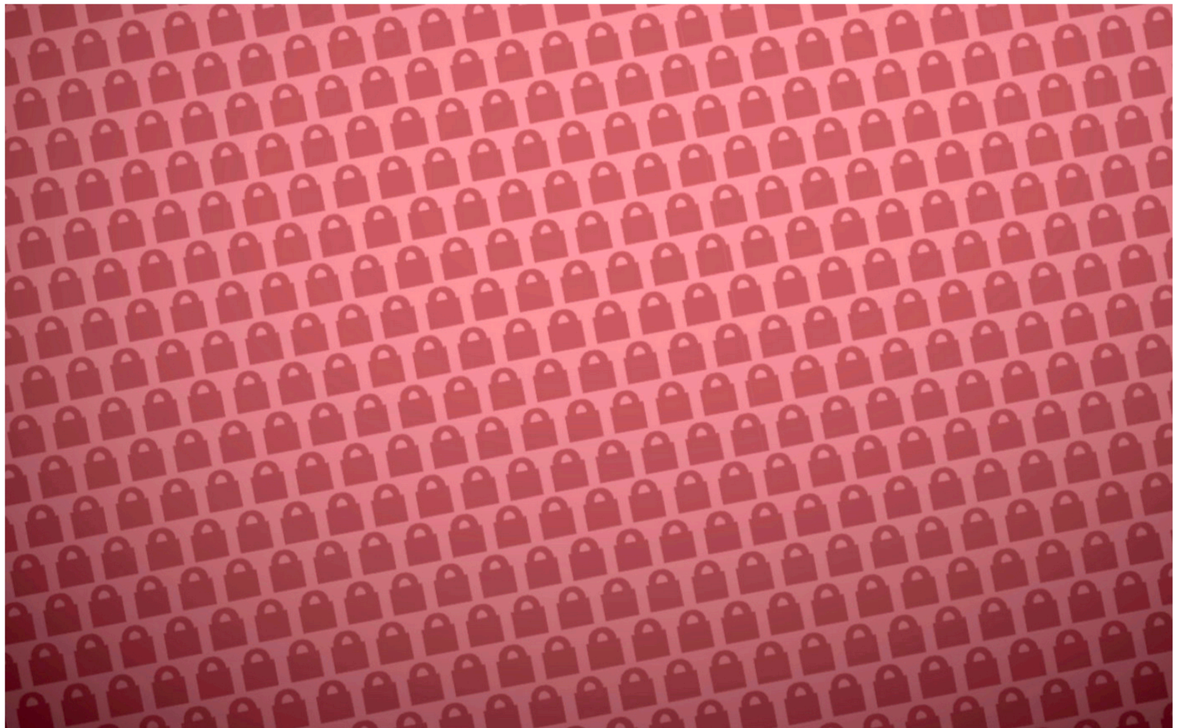
The guidance also suggested the creation of an inventory for the most sensitive and critical data needed to be secured for prolonged periods of time.

News?

Duality nabs $30M for its privacy-focused data collaboration tools, built using homomorphic encryption

Ingrid Lunden @ingridlunden / 7:04 AM EDT • October 5, 2021

Comment



SSL/TLS

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

-E-comme[illegible]anking, etc.

https://bofa.com

https

Today

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

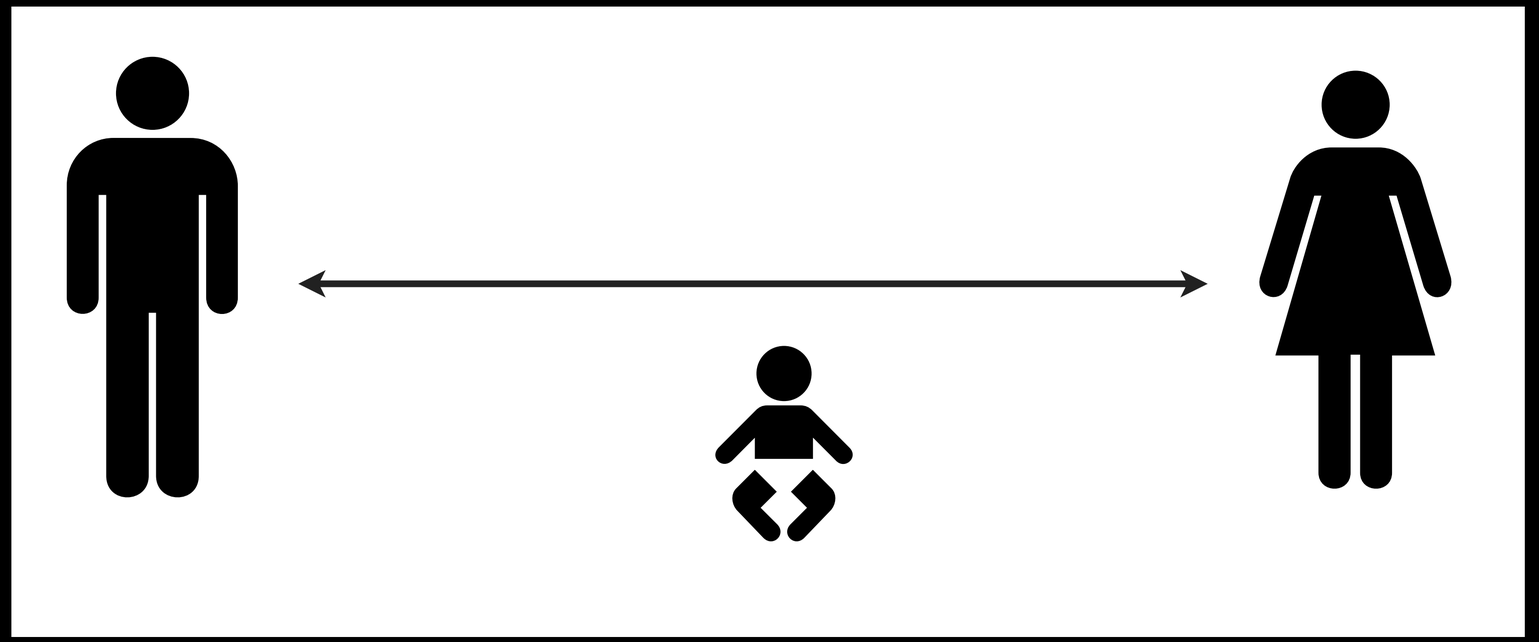
Protocols (definition)

- 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”

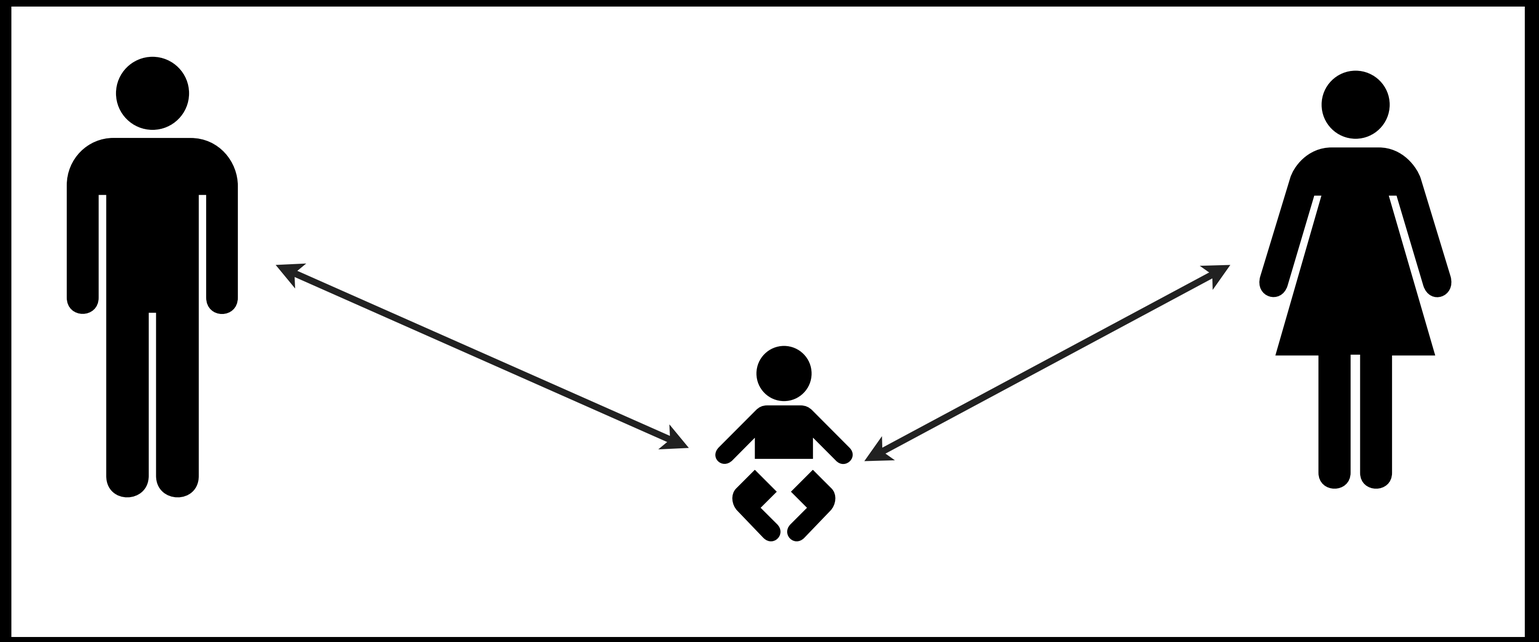
Why not just use primitives?

- 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

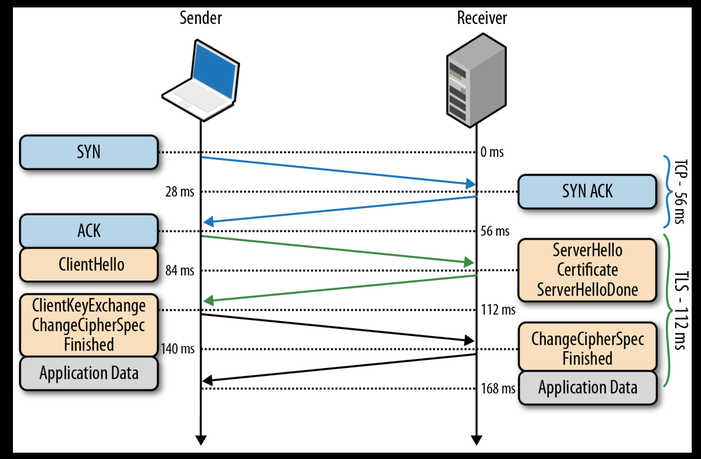


Threat Model



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, TLS 1.0/1.1/1.2)
- Not just web browsing!

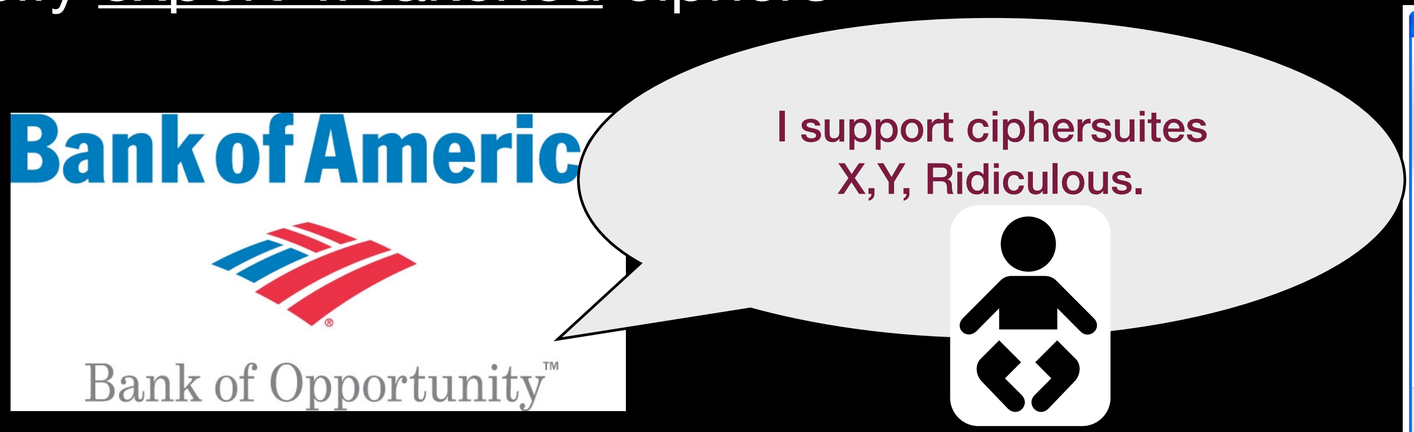


A brief history

- **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)**

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

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Negotiate

Key Exchange

Change cipher suit (AKA “start encrypting”)

Confirm handshake messages

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!

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

CCS Rollback

- Normal protocol:

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

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

CCS Rollback

- MITM attack:

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

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

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?

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Key-Exchange Rollback

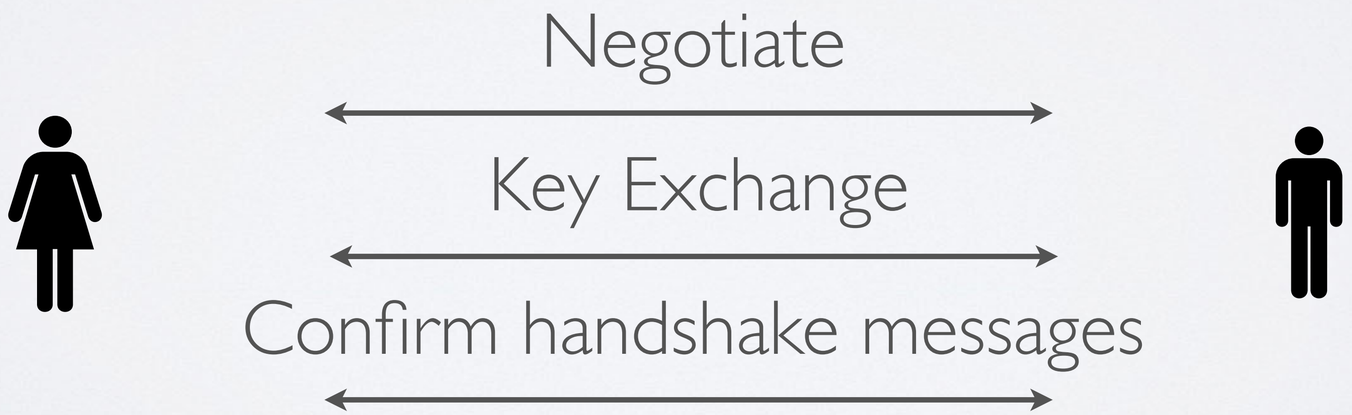
- SSL3 stand
  key exchan
  - 1. Server
    (signed
  - 2. Server
  - Client ma
- Why ephen
  - Advantages of Diffie-Hellman? RSA?

```
struct {
    select (KeyExchangeAlgorithm) {
        case dh_anon:
            ServerDHParams params;
        case dhe_dss:
        case dhe_rsa:
            ServerDHParams params;
            digitally-signed struct {
                opaque client_random[32];
                opaque server_random[32];
                ServerDHParams params;
            } signed_params;
        case rsa:
        case dh_dss:
        case dh_rsa:
            struct {} ;
           /* message is omitted for rsa, dh_dss, and dh_rsa */
        /* may be extended, e.g., for ECDH -- see [TLSECC] */
    };
} ServerKeyExchange;
```

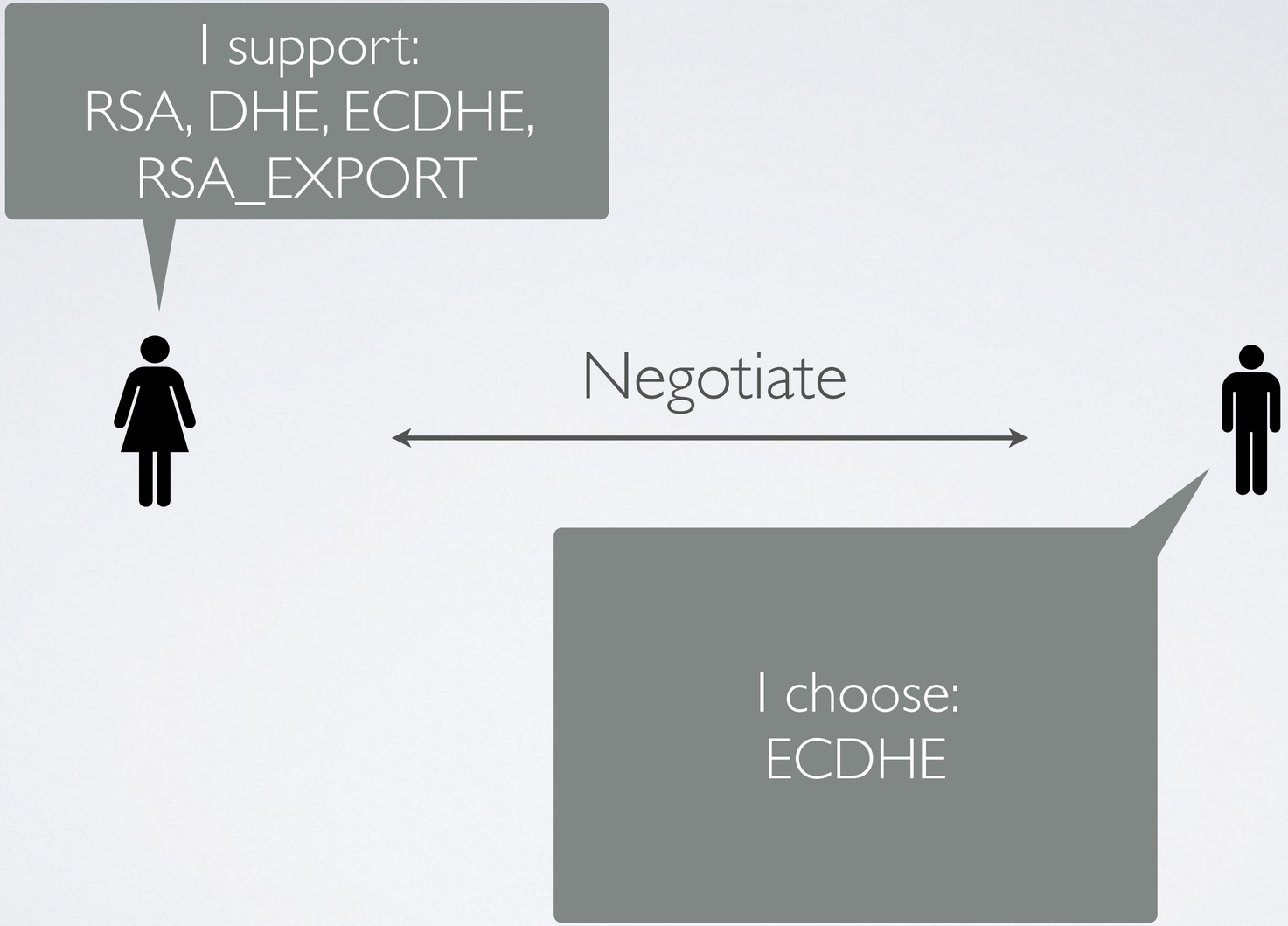
Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Downgrade attacks!

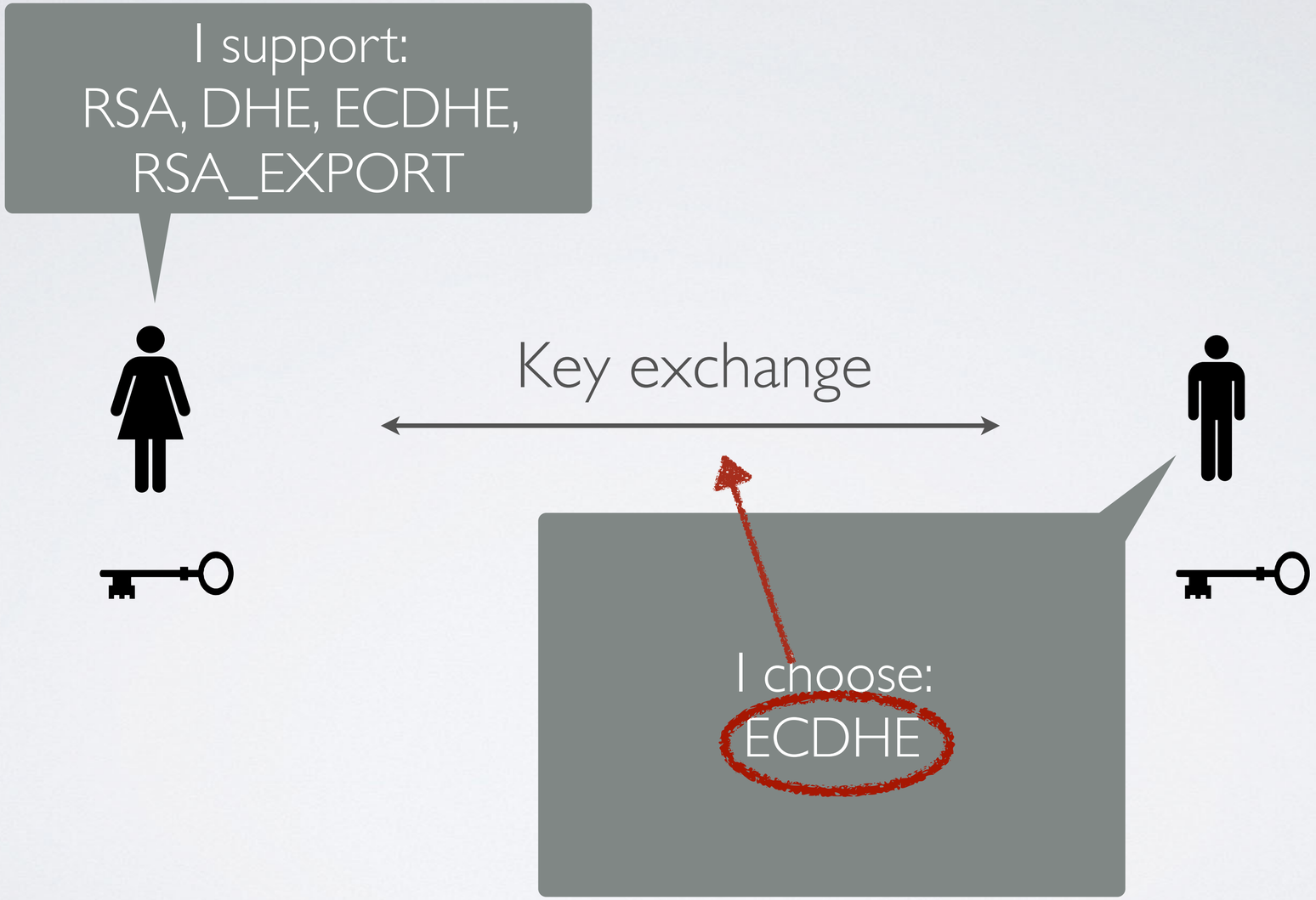
Each TLS handshake begins with a cipher suite negotiation that determines which key agreement protocol (etc.) will be used.



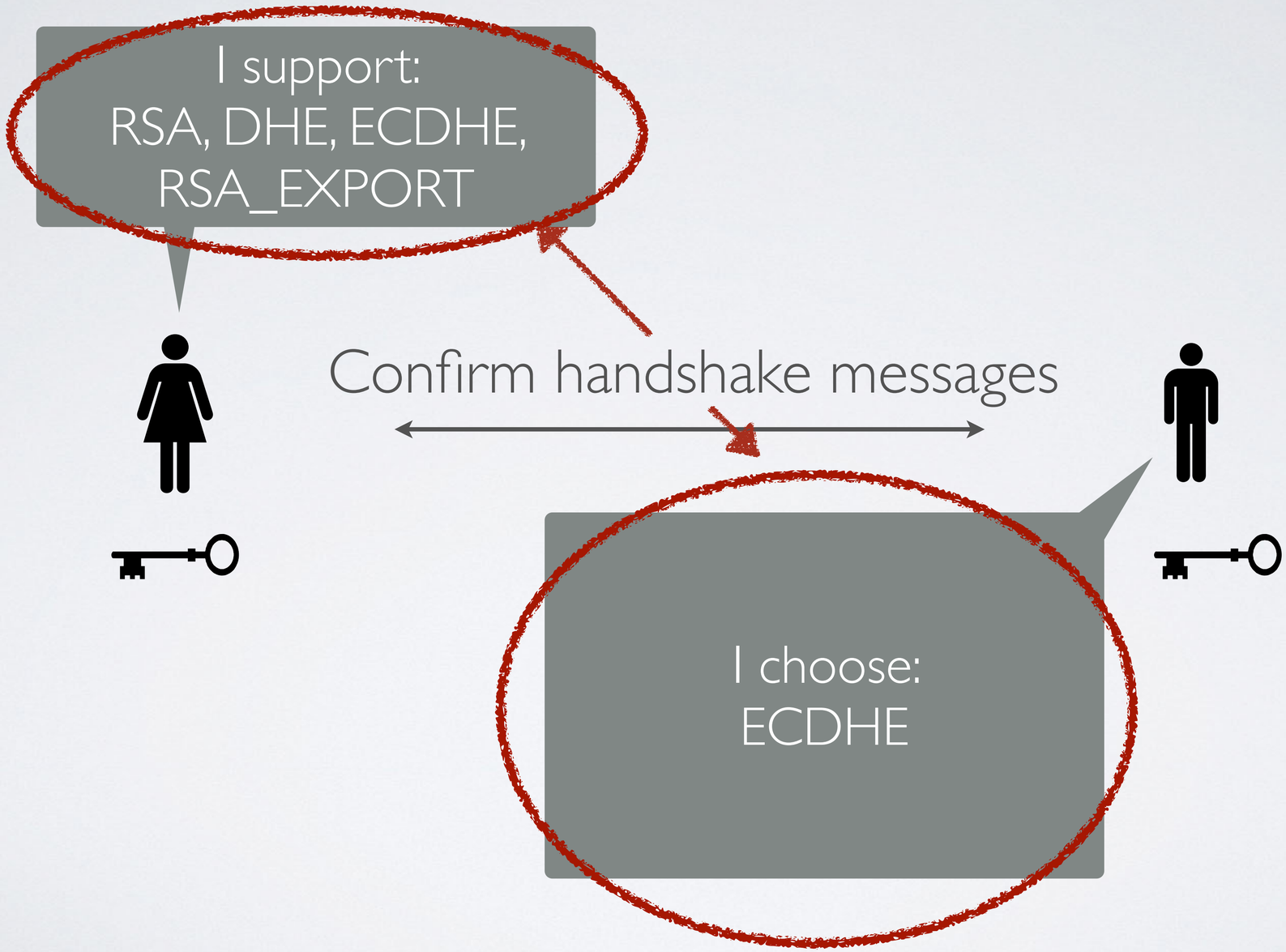
Ciphersuite Negotiation



Ciphersuite Negotiation



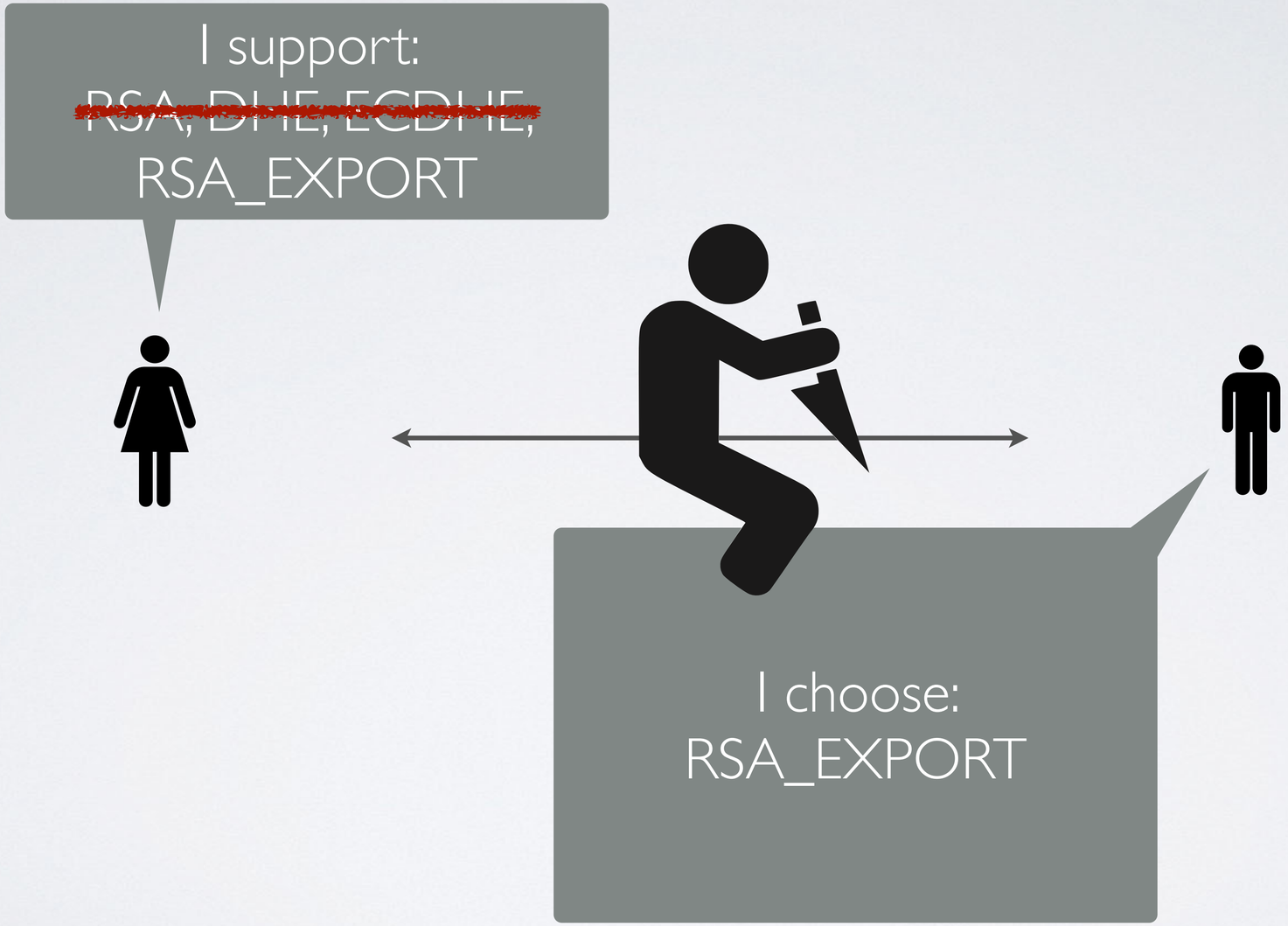
Ciphersuite Negotiation



MITM Negotiation

MITM Negotiation

MITM Negotiation



MITM Negotiation

MITM Negotiation

I support:
~~RSA, DHE, ECDHE,~~
RSA_EXPORT

Attacker can break RSA export key

MITM Negotiation

MITM Negotiation

As of Mar '15,
30+% of TLS hosts supported
export suites!

MITM Negotiation

I support:
RSA_DHE_EGDHE

Solution:

Modern clients won't offer broken cipher suites like RSA_EXPORT

(unless they're wget or curl!)

I choose:
A_EXPORT

As of Mar '15,
30+% of TLS hosts supported export suites!

Question

Is it sufficient for the client to support only “strong” ciphersuites, even if the server supports weak ones?

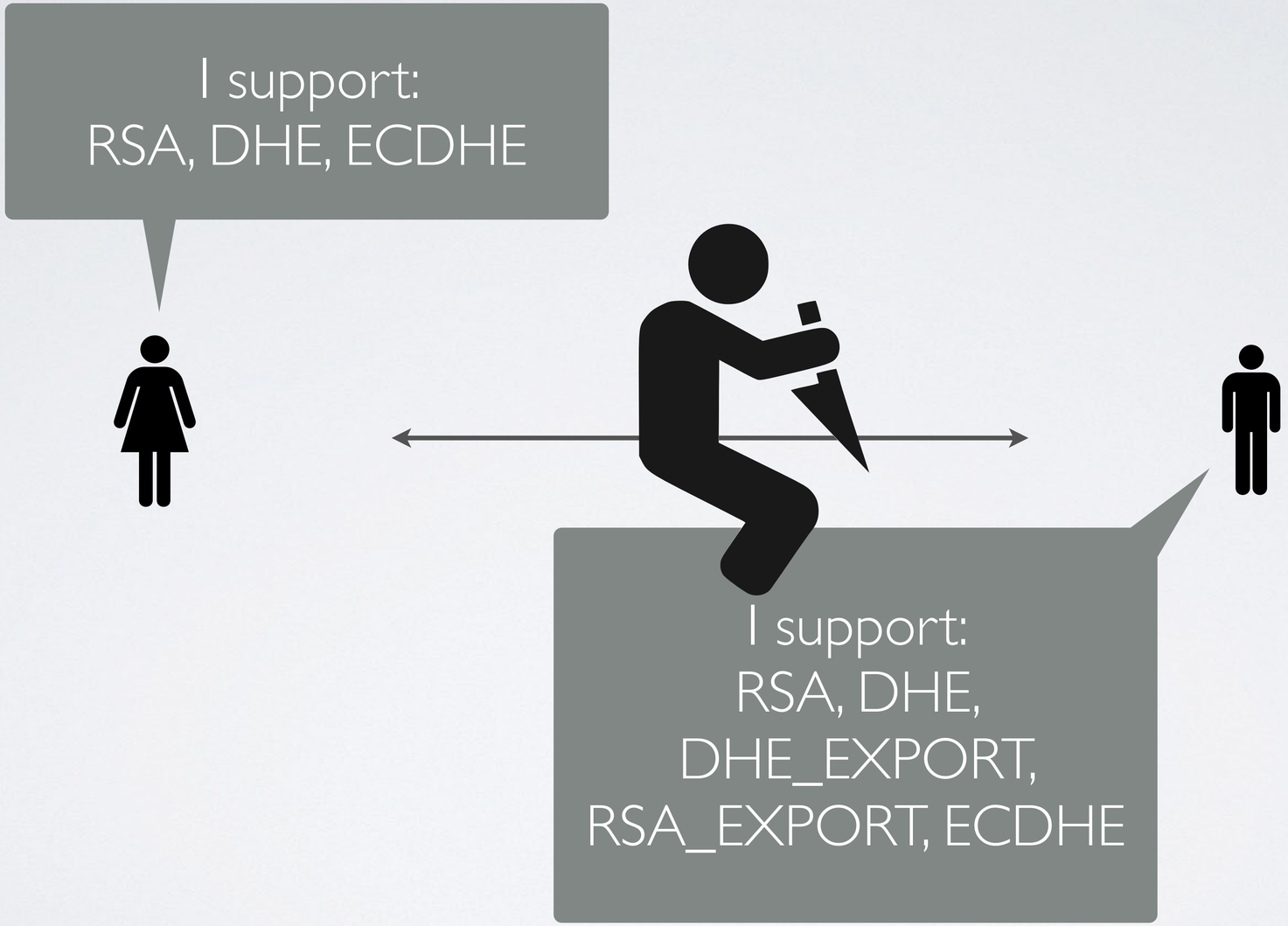
Question

Is it sufficient for the client to support only “strong” ciphersuites, even if the server supports weak ones?

- Let ***A*** be the set of KA protocols supported by Client
  Let ***B*** be the set of KA protocols supported by Server

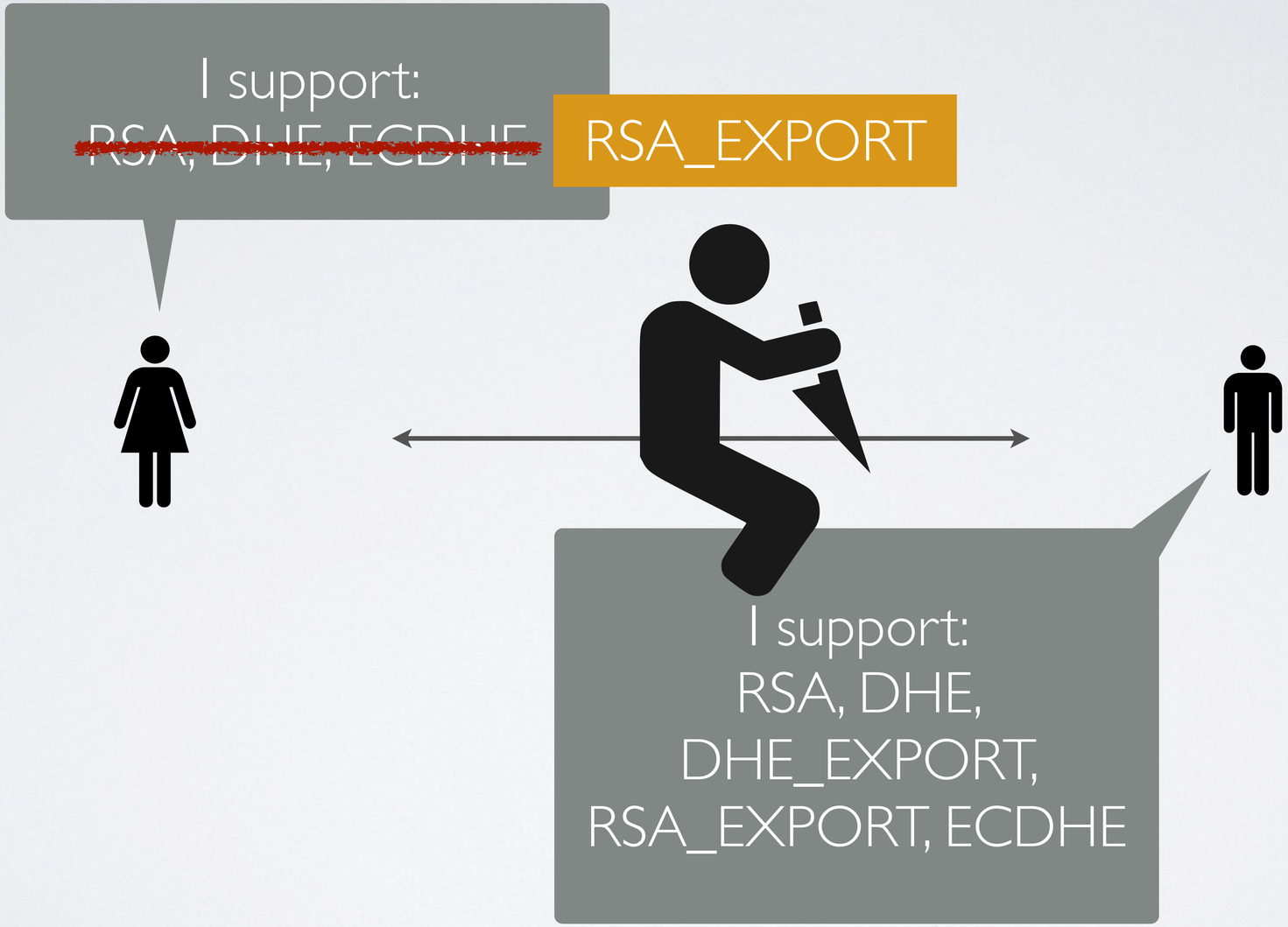
- If each KA protocol in $A \cap B$ is a secure KA protocol, is the TLS handshake secure

Example 2: Negotiation



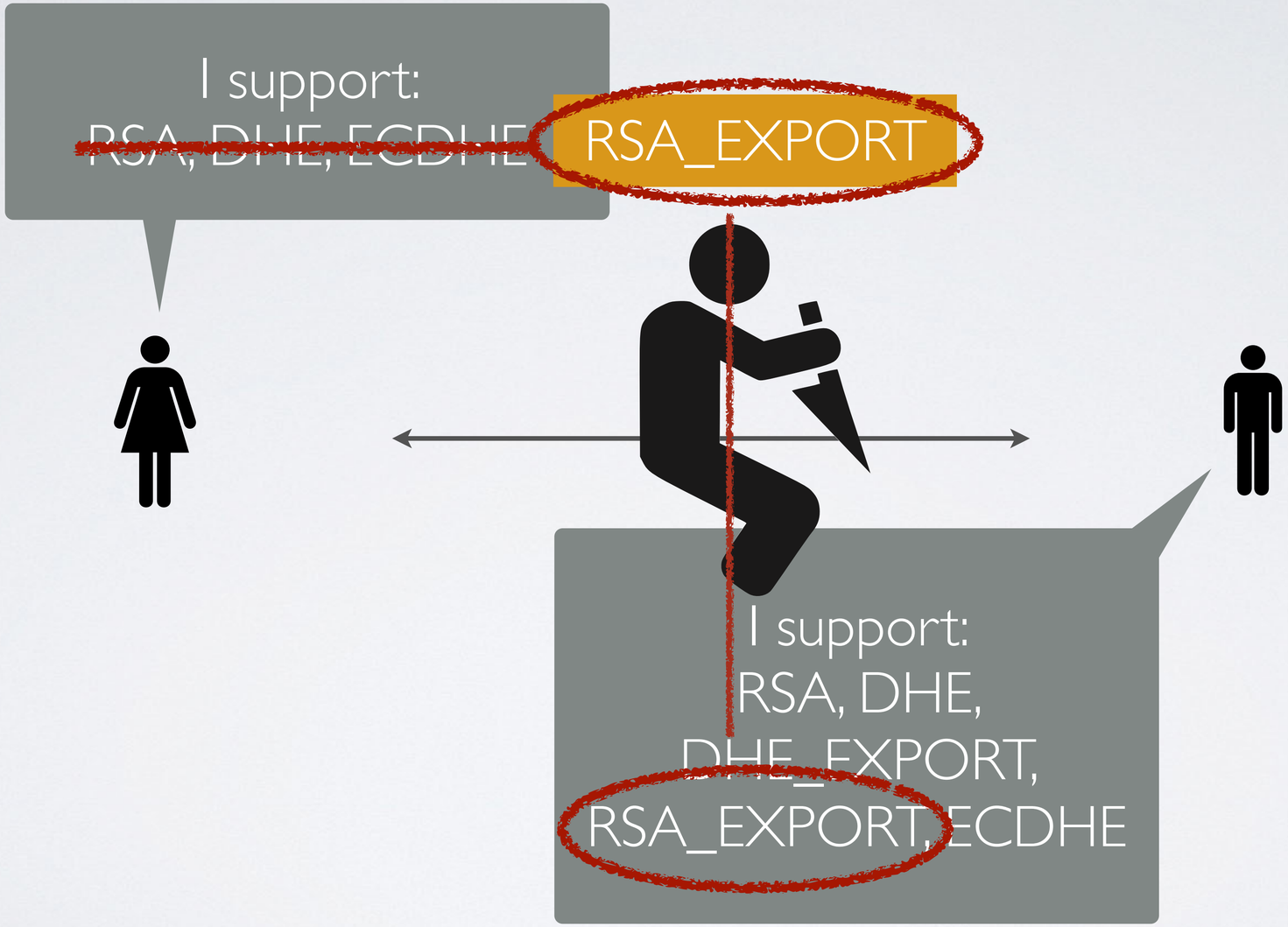
Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 2: Negotiation



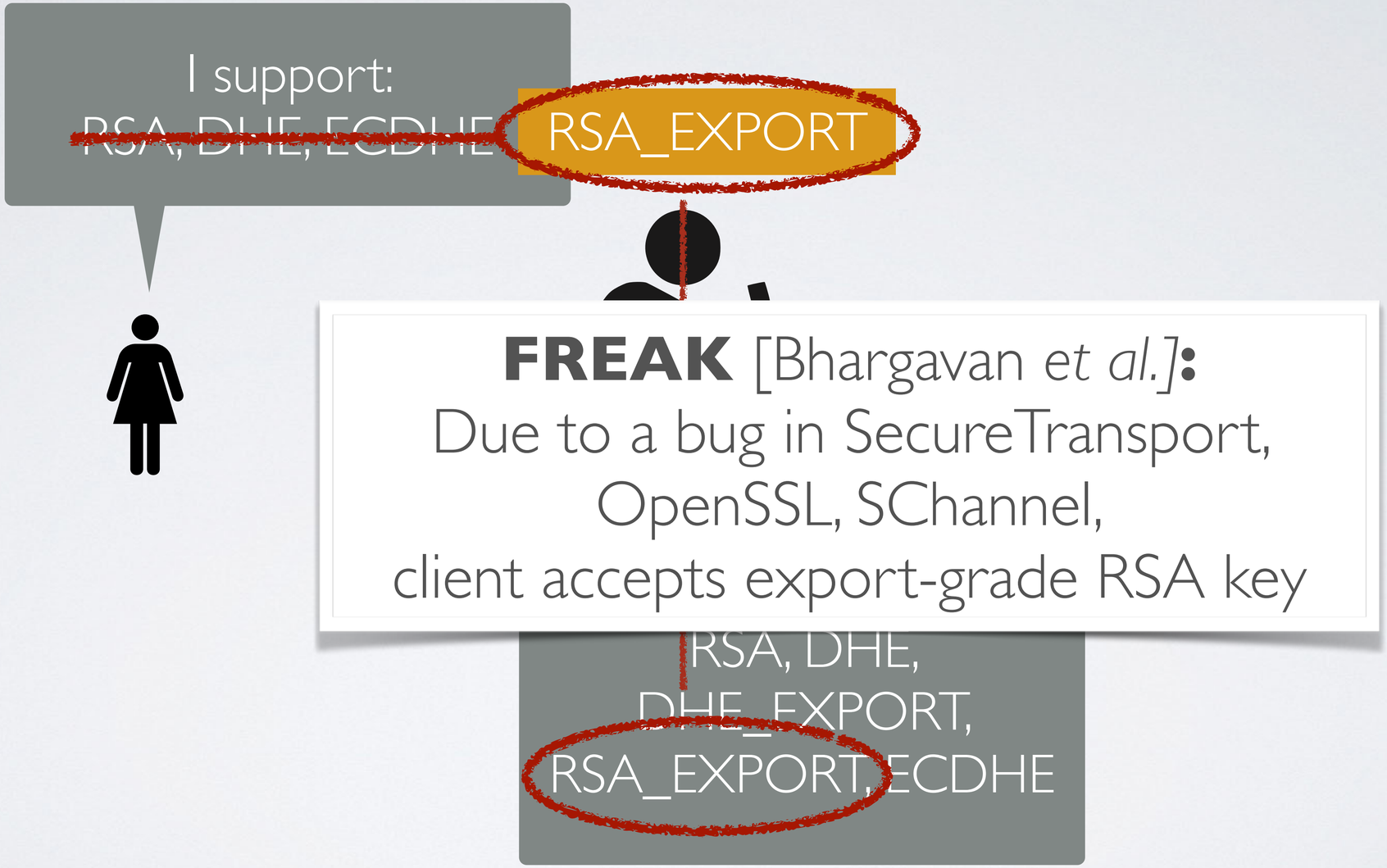
Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 2: Negotiation

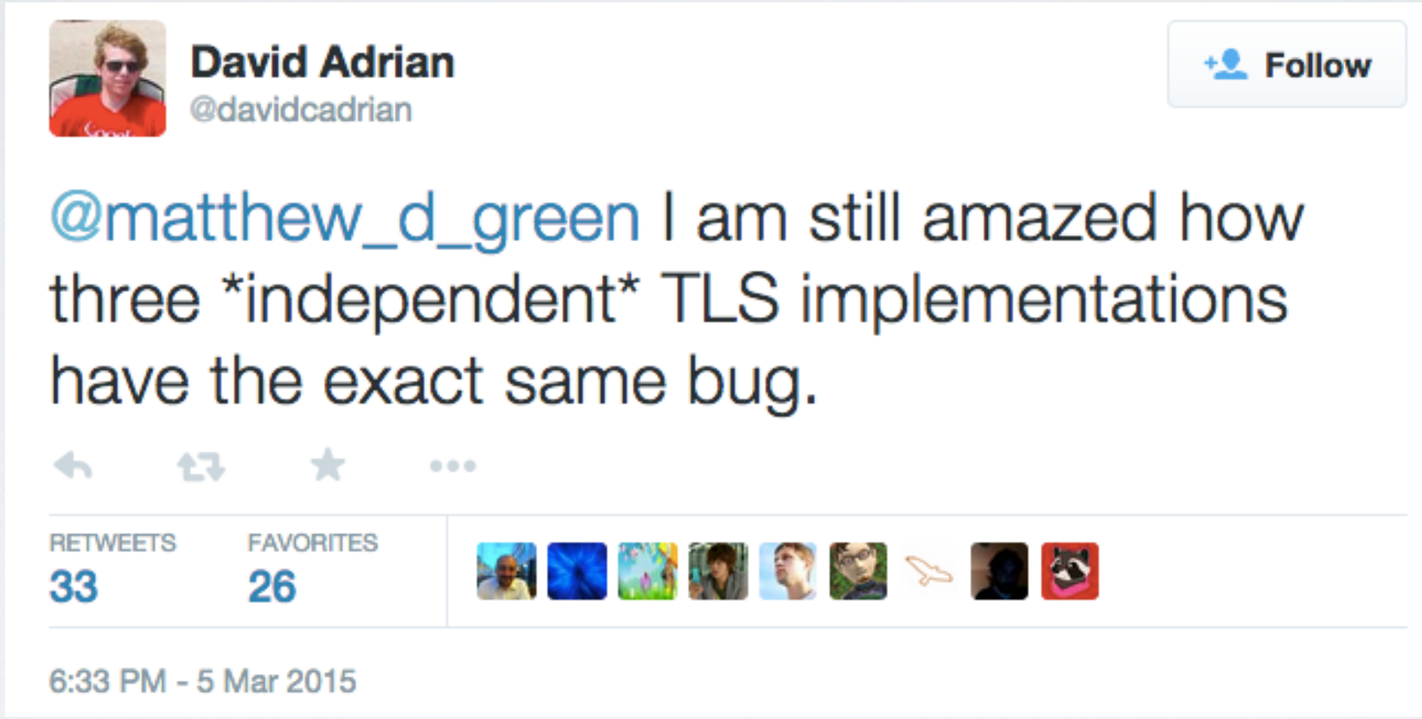


Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 2: Negotiation



Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010



Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 2: Negotiation

Solution: Fix implementations

Patch OpenSSL, SecureTransport, SChannel so they will recognize an RSA export key exchange message, barf

(patches rolled out March 2015)

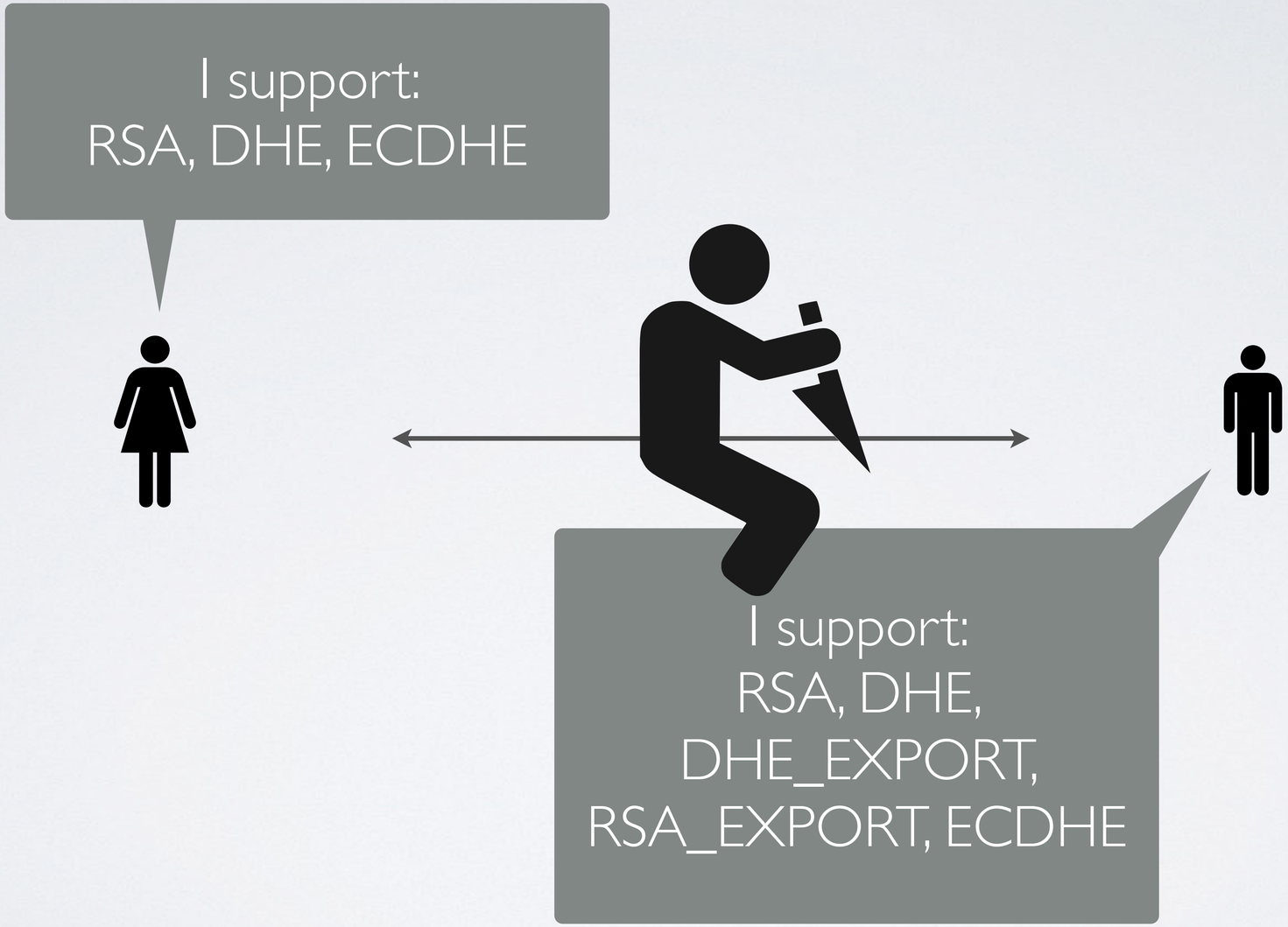
RSA_DHE

Apple issues security patches to protect devices from the FREAK bug

by Mariella Moon | @mariella_moon | 22 days ago

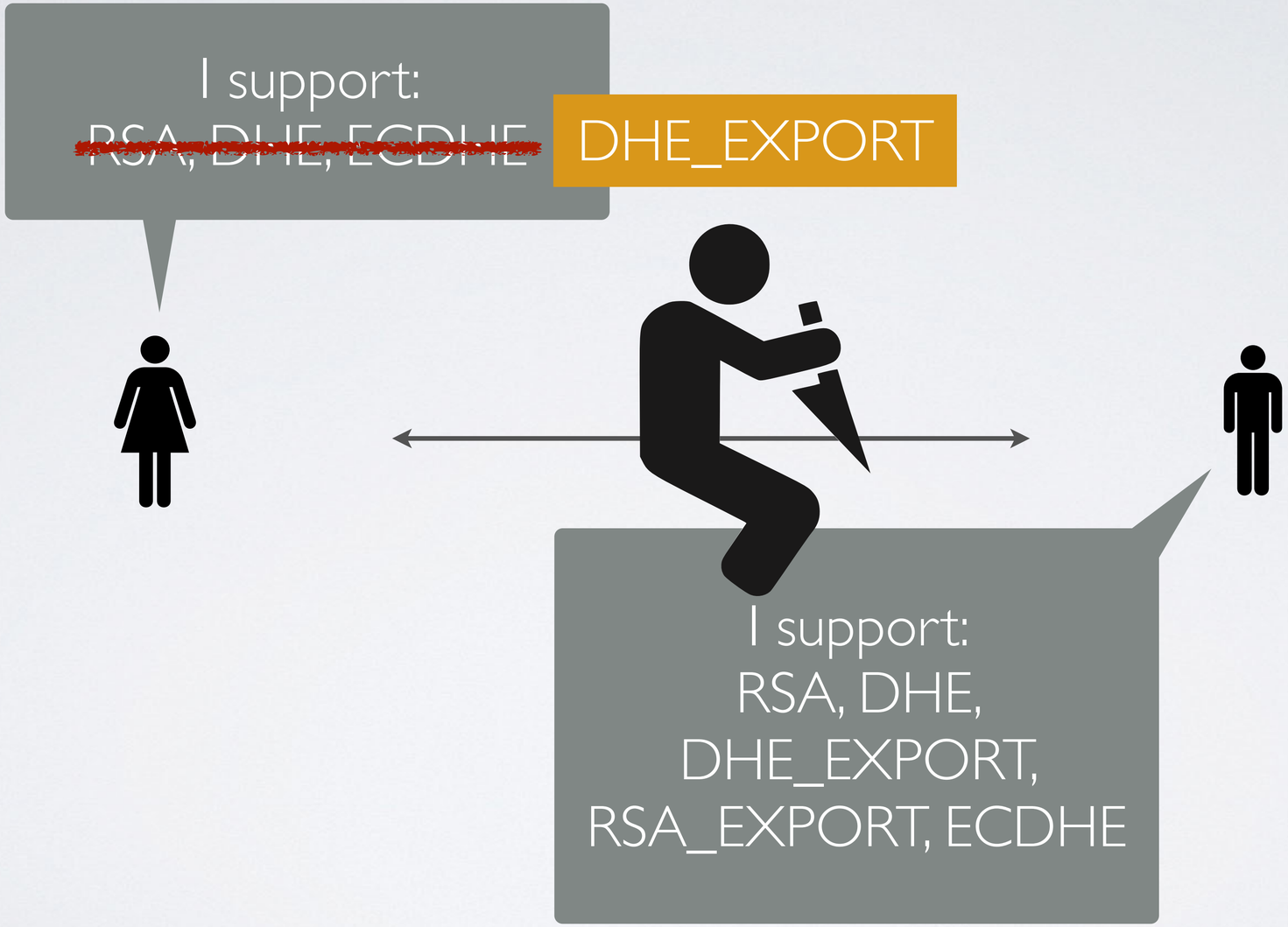
Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 3: Negotiation



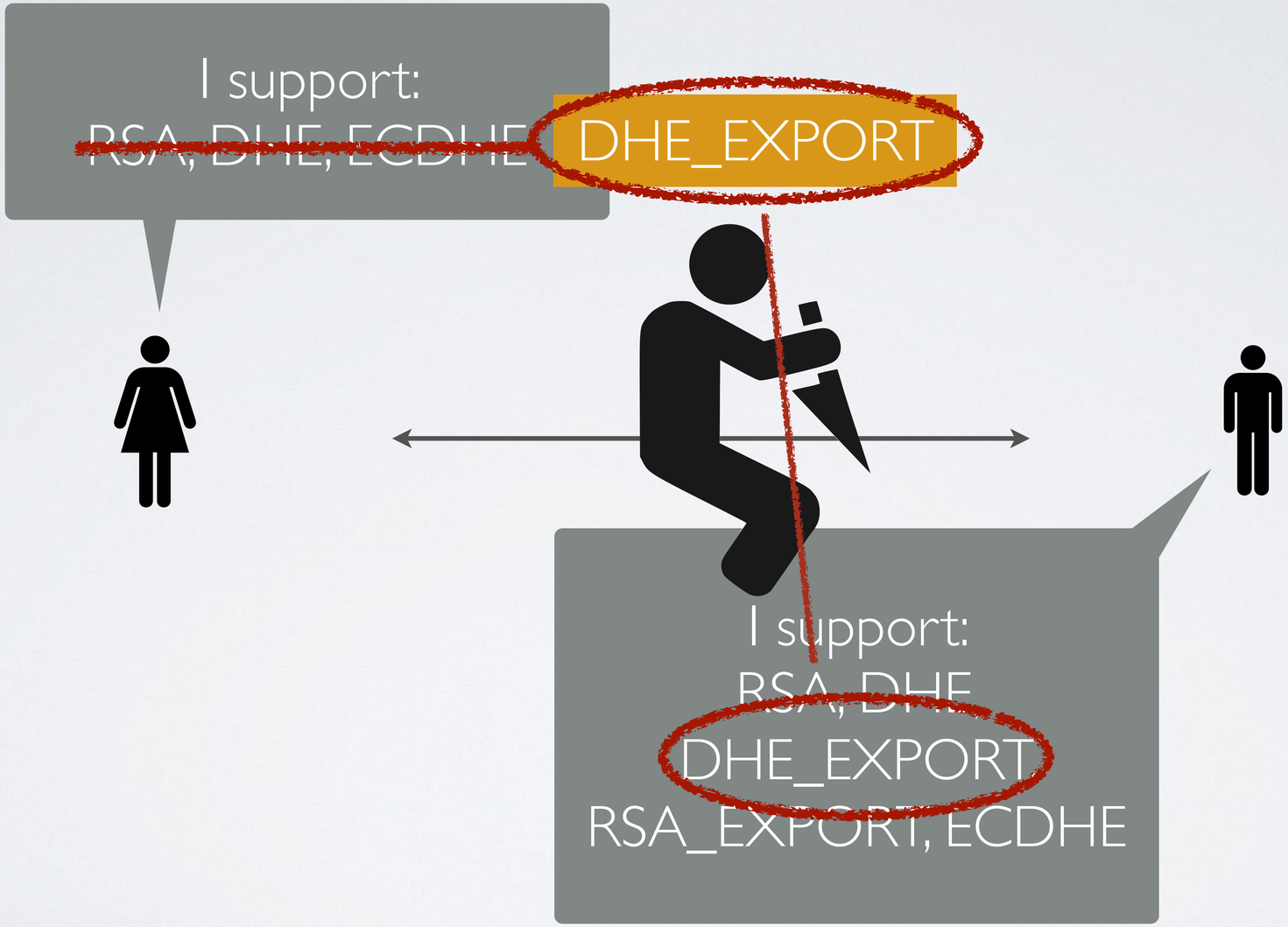
Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 3: Negotiation



Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 3: Negotiation



Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 3: Negotiation

I support:

```
struct {
    select (KeyExchangeAlgorithm) {
        case dh_anon:
            ServerDHParams params;
        case dhe_dss:
        case dhe_rsa:
            ServerDHParams params;
            digitally-signed struct {
                opaque client_random[32];
                opaque server_random[32];
                ServerDHParams params;
            } signed_params;
        case rsa:
        case dh_dss:
        case dh_rsa:
            struct {} ;
           /* message is omitted for rsa, dh_dss, and dh_rsa */
        /* may be extended, e.g., for ECDH -- see [TLSECC] */
    };
} ServerKeyExchange;
```

Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Example 3: Negotiation

LogJam [Adrian *et al.*]**:**
Due to a bug in *the TLS* ***protocol***
client accepts export-grade DHE key

Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

TLS design/deployment assumptions were wrong, and we knew this for years —
but failed to properly communicate to the community.

TLS design/deployment assumptions were wrong, and we knew this for years —
but failed to properly communicate to the community.

The community made terrible assumptions and didn't ask us what we thought of them. Then they got mired in backwards compatibility issues and only responded to attacks.

Exploiting LogJam

(Joint work: Adrian, Bhargavan, Durumeric, Gaudry, Green, Halderman, Heninger, Springall, Thomé, Valenta, VanderSloot, Wustrow, Zanella-Beguelin, Zimmermann) *in* 'CCS 2015

Exploiting LogJam

- To exploit the downgrade attack, requires solving a 512-bit DL in real time
  - Initially this seems challenging, but NFS algorithm can be heavily optimized for pre-computation using only prime (p)
  - "Oversieving" increases cost of sieving and storage, but reduces cost of linear algebra step & final "descent"

Exploiting LogJam

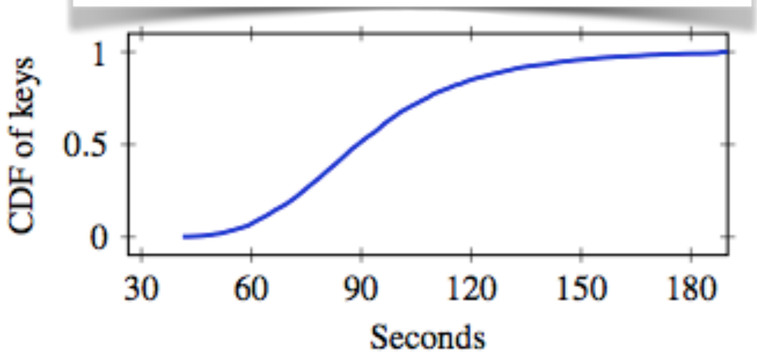
- To exploit the downgrade attack, requires solving a 512-bit DL in real time
  - **92% of DHE_EXPORT servers use one of two hard-coded primes (*p*) (*Mod_SSL, Apache*)**

Exploiting LogJam

- To exploit the downgrade attack, requires solving a 512-bit DL in real time
  - **92% of DHE_EXPORT servers use one of two hard-coded primes (*p*) (*Mod_SSL, Apache*)**

Sieving/Linear Alg:
1 week (wall clock) for each *p*

Descent on (g, h)



Exploiting LogJam

Example 3: Negotiation

Short term (hack) solution:

Fix OpenSSL, SecureTransport, SChannel
so they refuse DHE keys <768 bits

patched in NSS, SChannel, BoringSSL, LibreSSL,
SecureTransport

(Took months to accomplish this, since it breaks
~1% of the Internet to make this fix)

RSA_EXPORT, ECDHE

Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

Server has a weak, ephemeral Diffie-Hellman public key

ERR_SSL_WEAK_SERVER_EPHEMERAL_DH_KEY

Hide details

This error can occur when connecting to a secure (HTTPS) server. It means that the server is trying to set up a secure connection but, due to a disastrous misconfiguration, the connection wouldn't be secure at all!

In this case, the server needs to be fixed. Google Chrome won't use insecure connections in order to protect your privacy.

Learn more about this problem.

Long(er) term solutions:

Eliminate 1024-bit DHE (but Java).

Stop using common DHE primes.

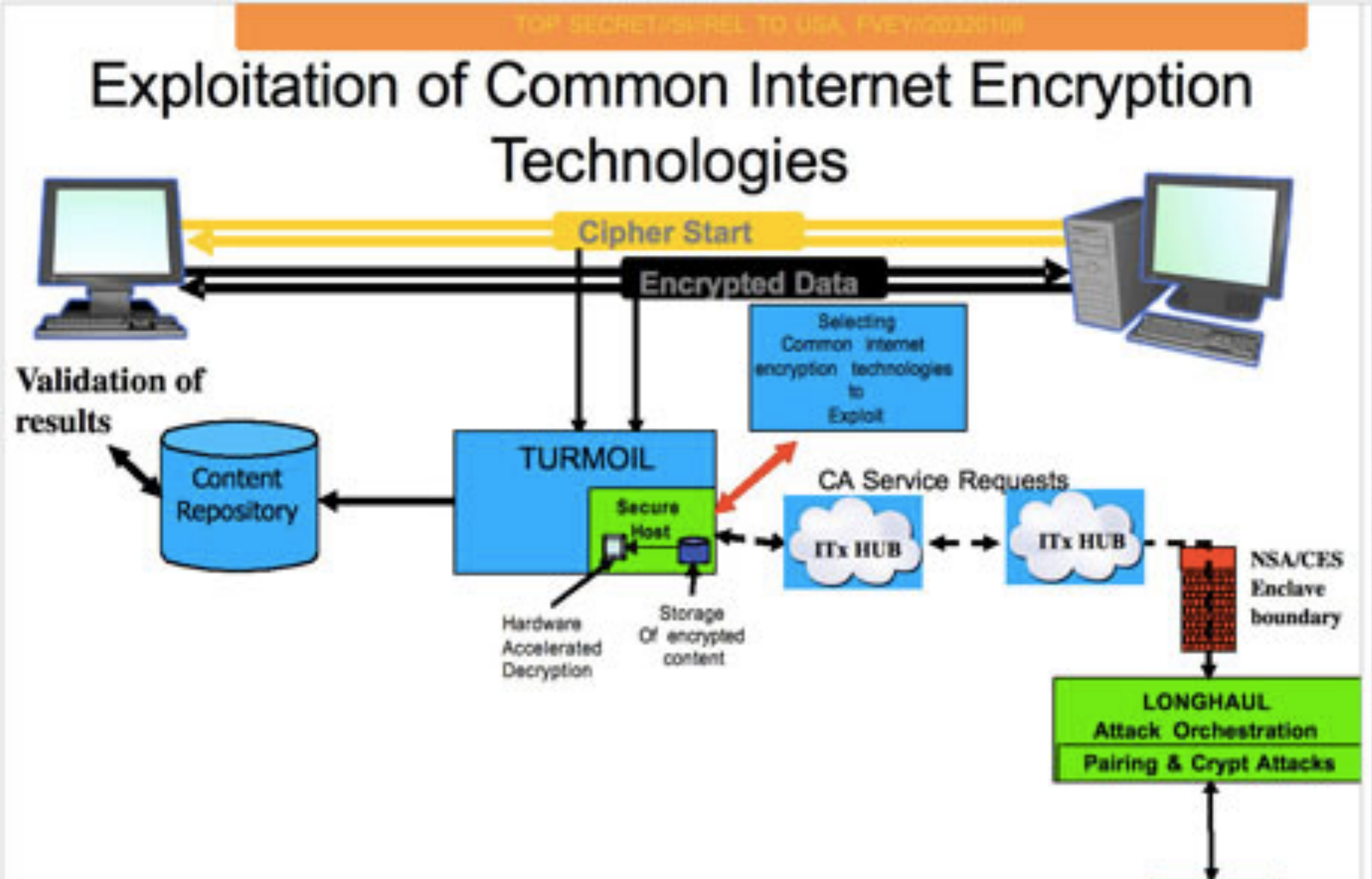
Use EU-CMA signatures to validate the protocol transcript. Then you can achieve the $A \cap B$ security the TLS designers originally set out to achieve.

(TLS 1.3 adds such a message, provisionally.)

Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash, Cryptographic Agility and its Relation to Circular Encryption, in EUROCRYPT 2010

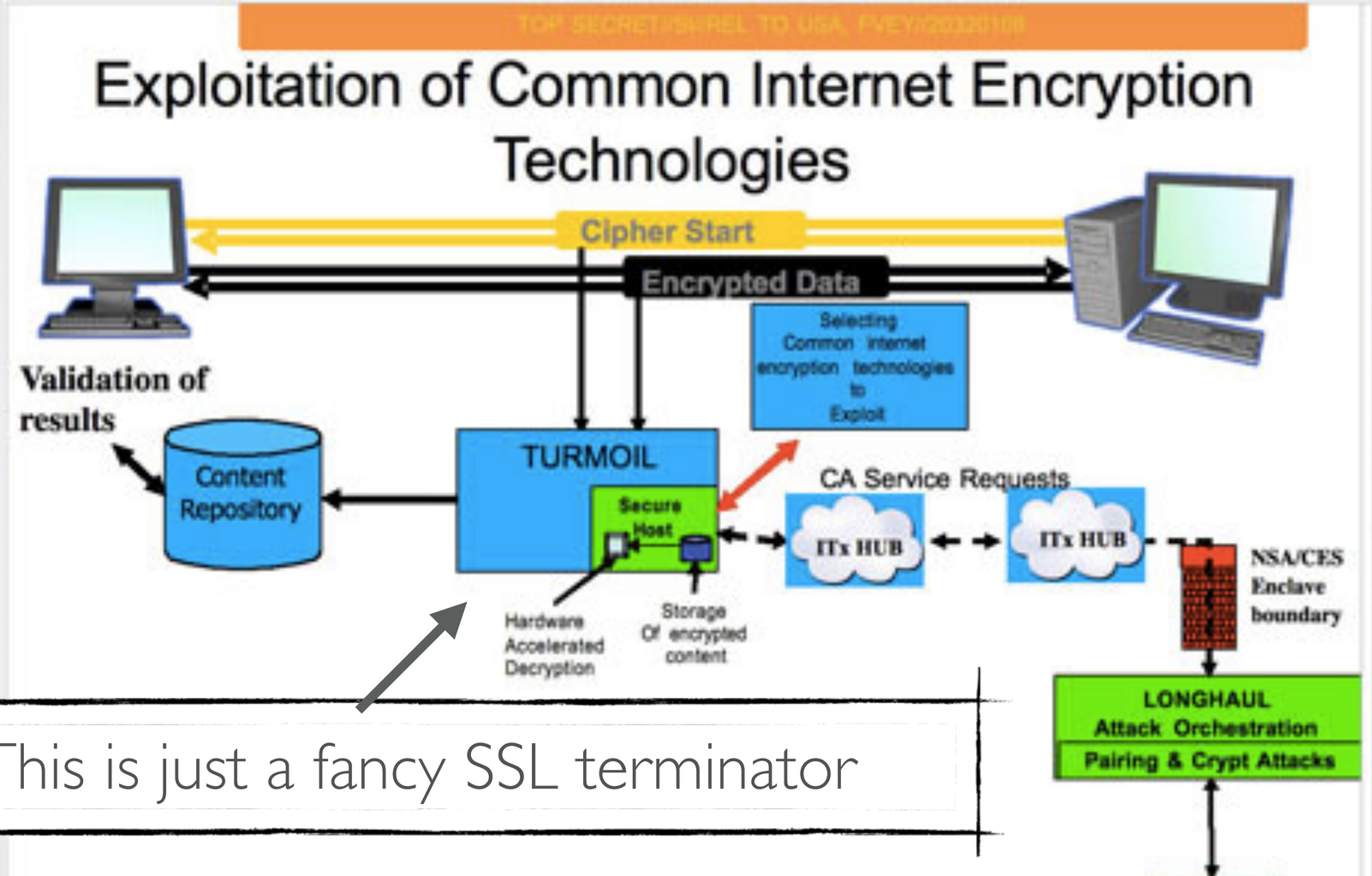
This picture again

- **What's going on here?**



This picture again

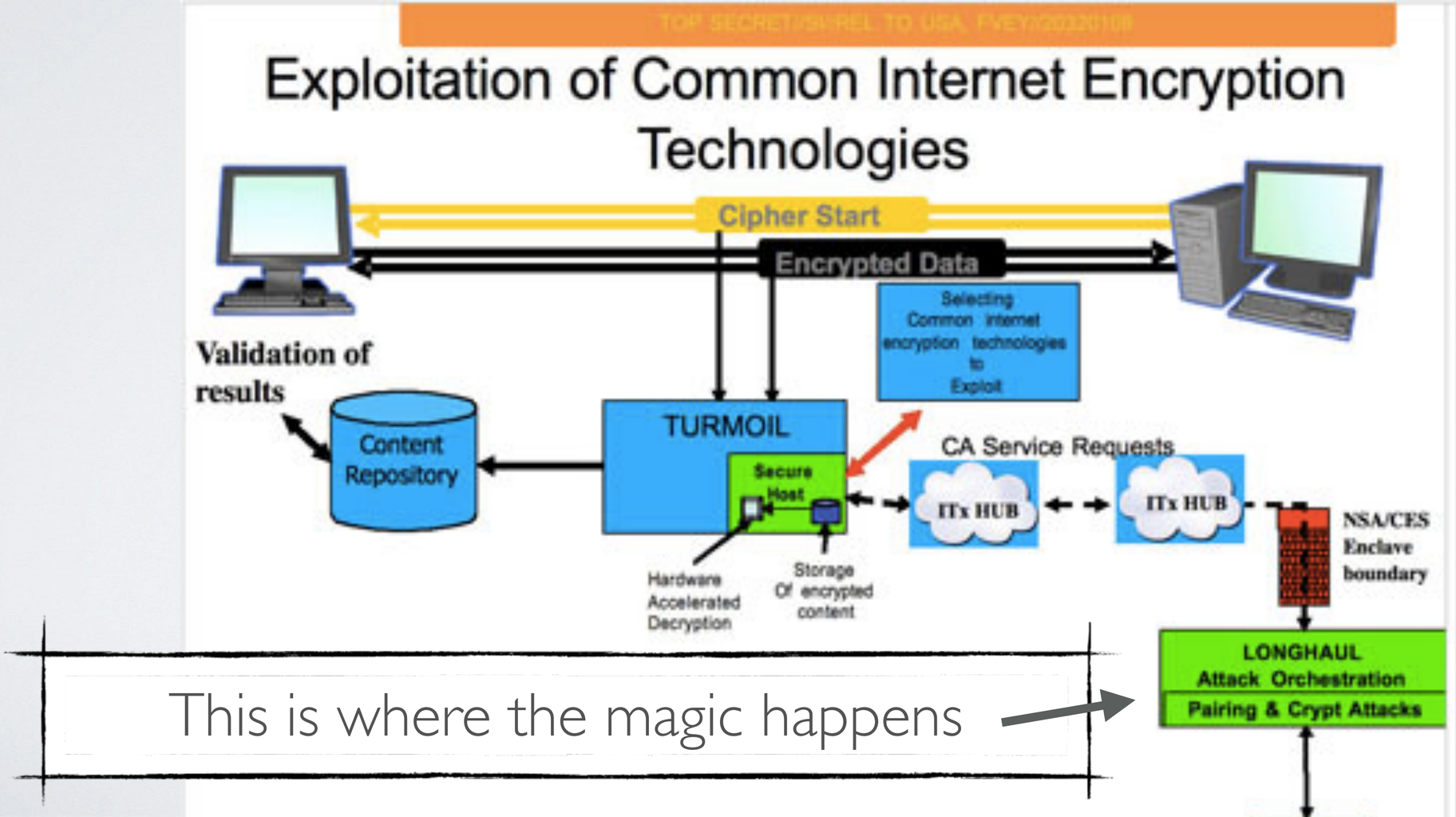
- **What's going on here?**



This is just a fancy SSL terminator

This picture again

- **What's going on here?**



What is LONGHAUL?

(TS//SI/REL) The **LONGHAUL** system provides the **Extended NSA Enterprise** with an end-to-end attack orchestration and key recovery service for Data Network Cipher (DNC) and Data Network Session Cipher (DNSC) traffic. LONGHAUL is extensible to allow for the addition of other Digital Network Intelligence cipher types.

Hypothesis 1: LONGHAUL is a database of stolen RSA secret keys

- This works well, but it's boring
- Easy to solve: switch to PFS cipher suites (DHE/ECDHE)

RSA Exploitation Steps

- Is it the key exchange RSA? (server hello)
  - If so, is the modulus match a known private key? (server certificate)
    - If so, is there 2-sided collect?
      - If so, do we have:
        - Client Hello
        - Server Hello
        - Client Key Exchange

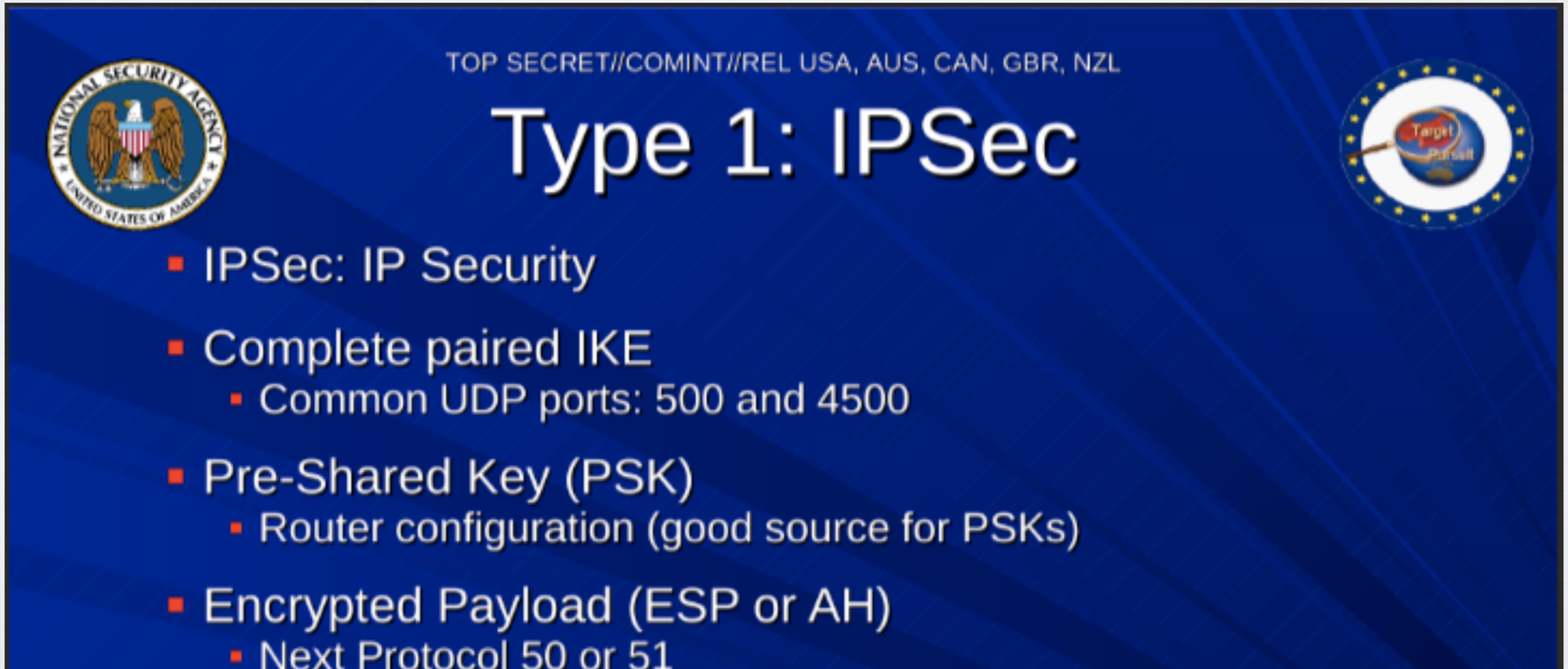
DECRYPTION!

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

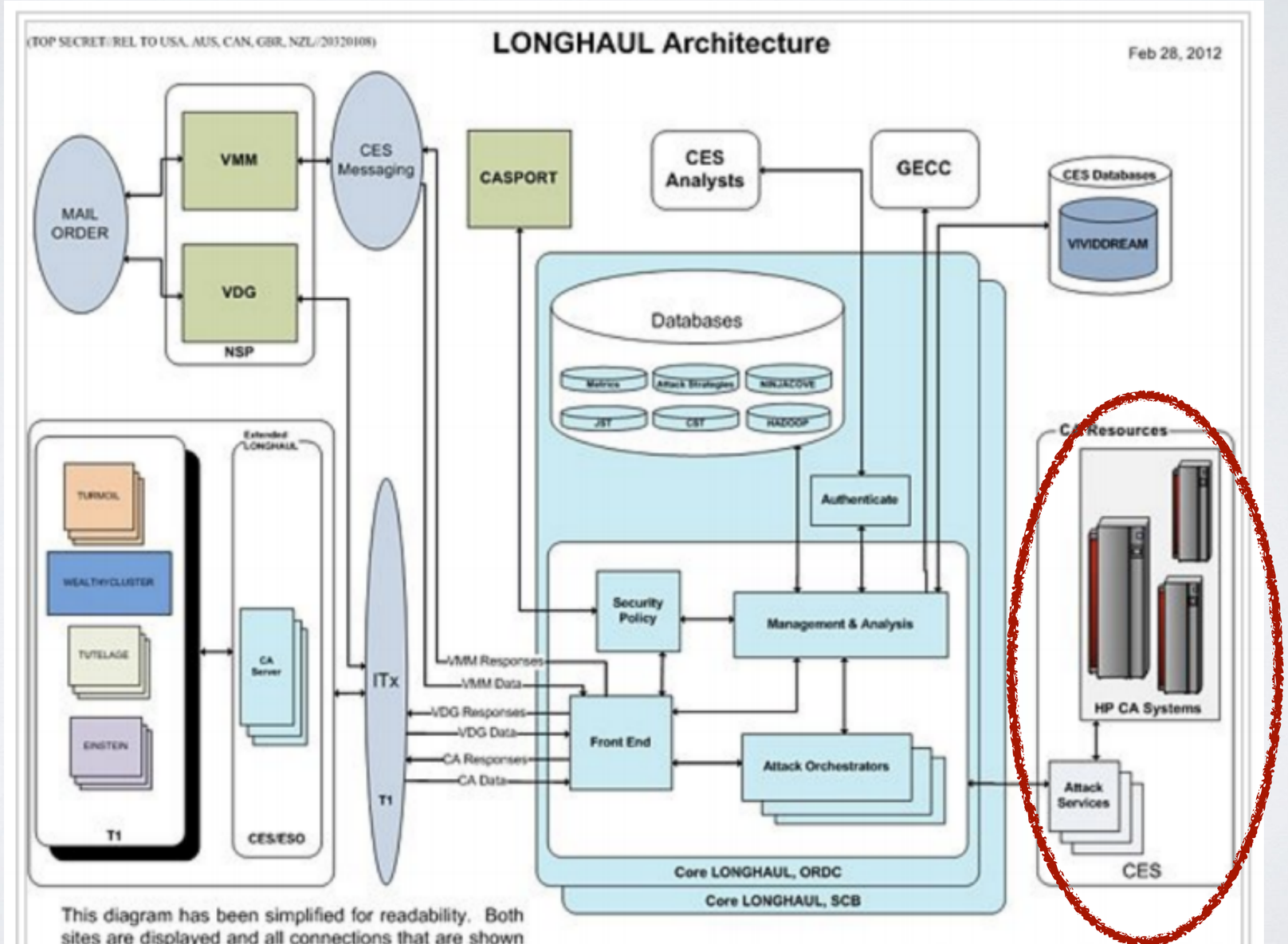
Happy Dance!!

Problem

- LONGHAUL also purports to decrypt IPSec/IKE
  - IKE does not use RSA
  - It uses Diffie-Hellman for each connection.



What is LONGHAUL?



The breakthrough was enormous, says the former official, and soon afterward the agency pulled the shade down tight on the project, even within the intelligence community and Congress. “Only the chairman and vice chairman and the two staff directors of each intelligence committee were told about it,” he says. The reason? “They were thinking that this computing breakthrough was going to give them the ability to crack current public encryption.”

What is LONGHAUL?

(TS//SI/REL) The **LONGHAUL** system provides the **Extended NSA Enterprise** with an end-to-end attack orchestration and key recovery service for Data Network Cipher (DNC) and Data Network Session Cipher (DNSC) traffic. LONGHAUL is extensible to allow for the addition of other Digital Network Intelligence cipher types.

Hypothesis 2: The NSA is breaking1024-bit DHE

- This sounds completely insane
- Maybe it's not

Breaking DHE at scale

- Breaking DHE == solving the Discrete Logarithm problem
  - In theory, this is too expensive for keys >=768 bits
  - However there is a wrinkle…

Breaking DHE at scale

- A large percentage of Apache/Java/ISS servers use *fixed, hardcoded parameters for DHE*
  - IPSec/IKE is even worse: nearly 50% of servers will choose Oakley groups 1 and 2 (768/1024) - generated in 1998
  - NFS is heavily optimized for pre-computation using only the primes
  - **With specific pre-computation ($10s-100s of Million/1 year?)**
    an attacker might be able to break 30-50% of DHE connections with academic levels of computing
  - Approximately 30 core days for final descent

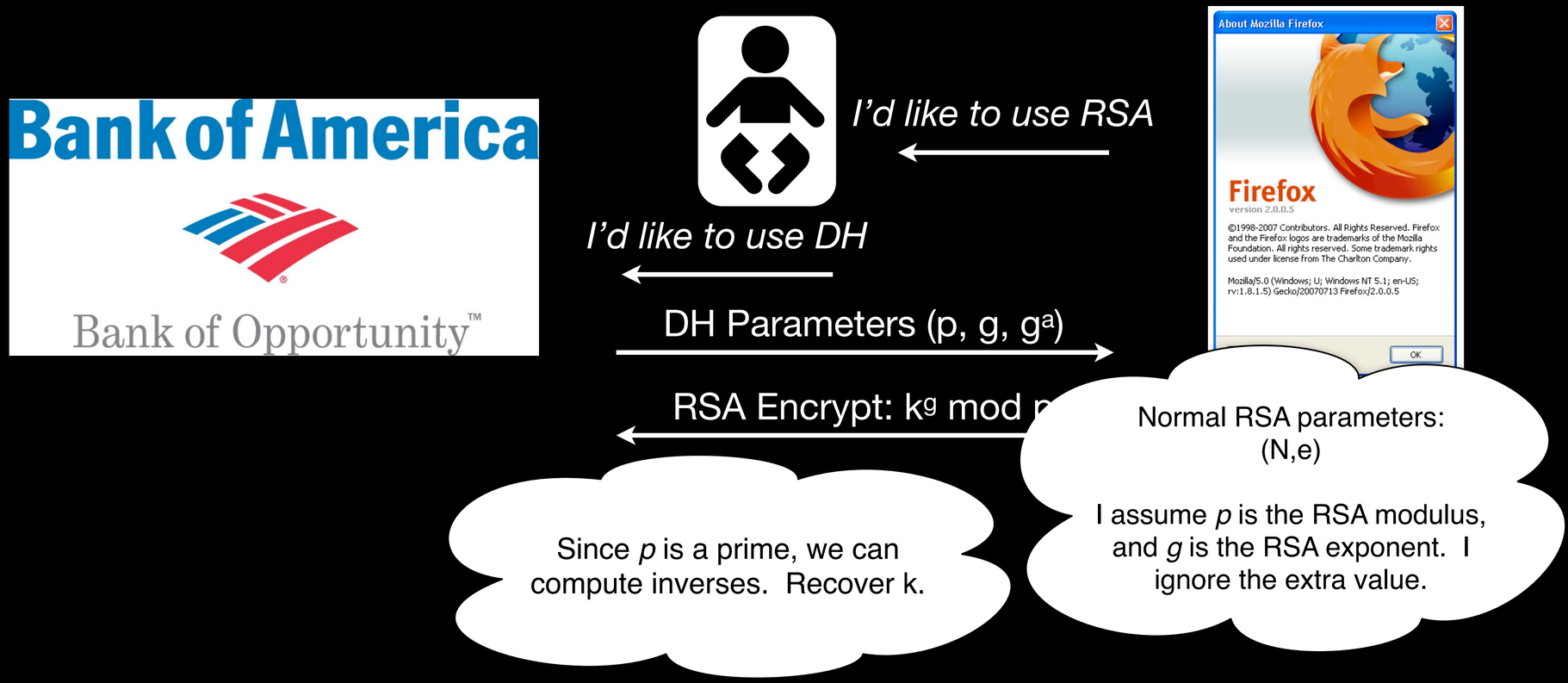
How do we fix *this*?

- Eliminate 1024-bit DH
  - This is challenging in TLS, since many machines (Java 7) crash on longer parameter lengths
  - D. Gillmor, new extension to negotiate FF-DHE
- Eliminate DHE altogether
  - Move to ECDHE, which is currently not 100% supported
  - Downgrade to RSA (!)
- Eliminate common primes

Why aren’t we fixing this?

Why aren’t we fixing this?

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

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

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 [illegible] related to the contents of

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

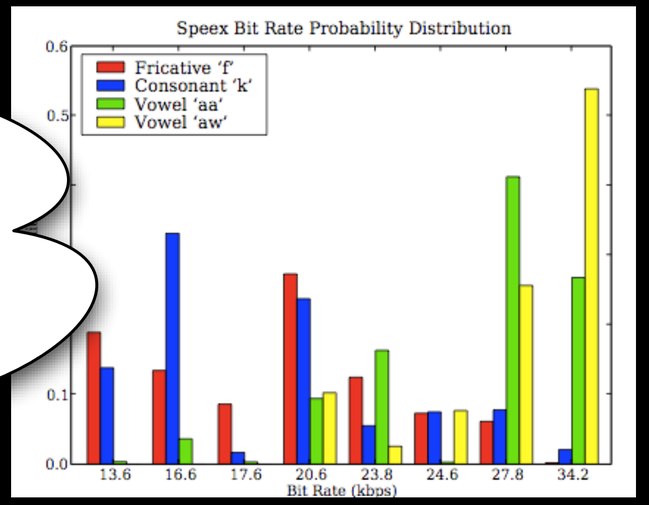


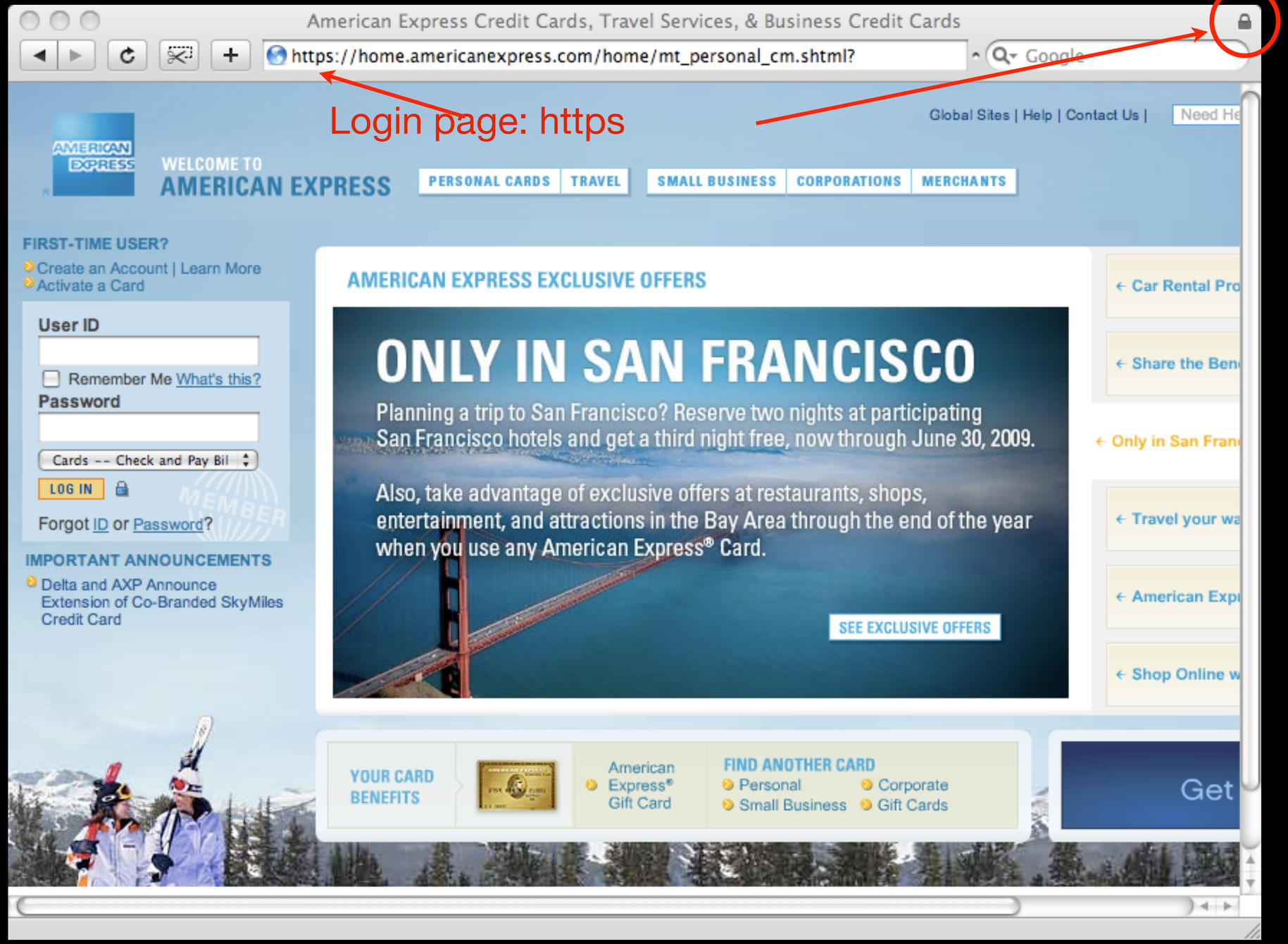
Image from Wright, Ballard, Coull, Monrose, Masson: Spot me if you Can, Uncovering spoken phrases in VoIP conversations

SSL Stripping & Pinning

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

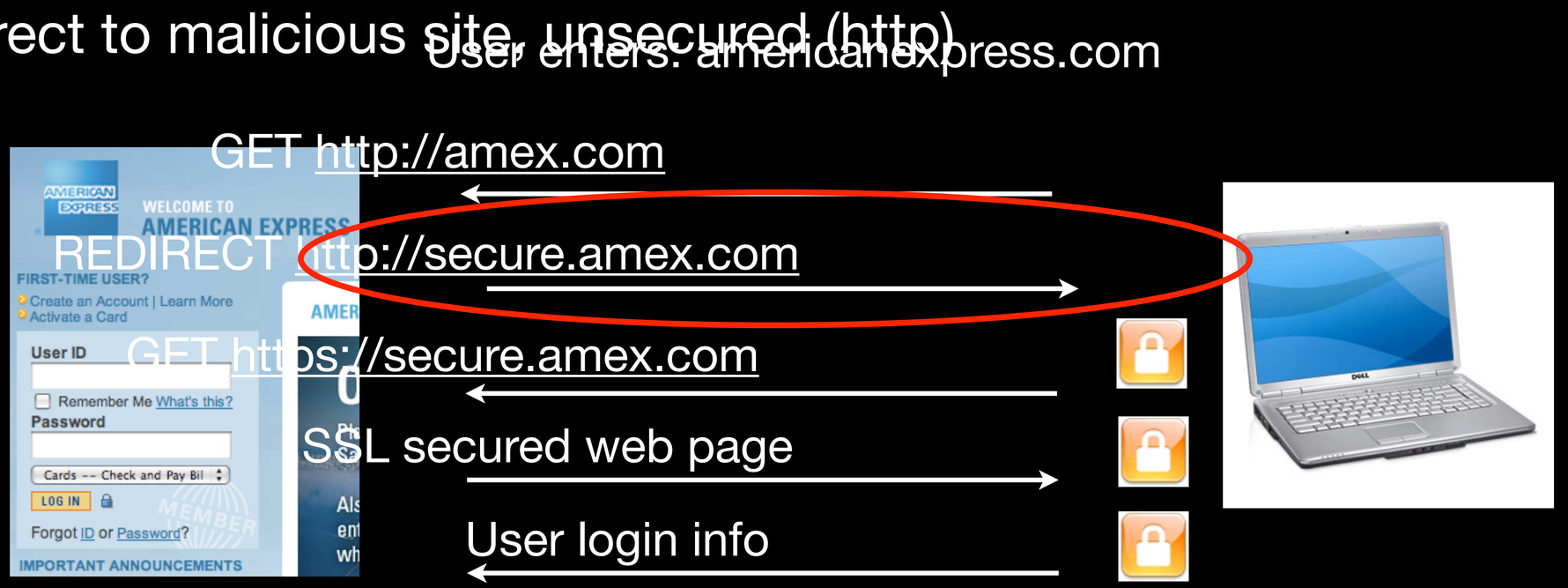
HTTP->HTTPS

- 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
Cards -- Check and Pay Bil
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
Car Rental Pro
Share the Ben
Only in San Fran
Travel your wa
American Expr
Shop Online w
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: 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

GET http://americanexpress.com

Unsecured http web page

User login info

Wachovia – Personal Finance and Business Financial Services

http://wachovia.com/

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

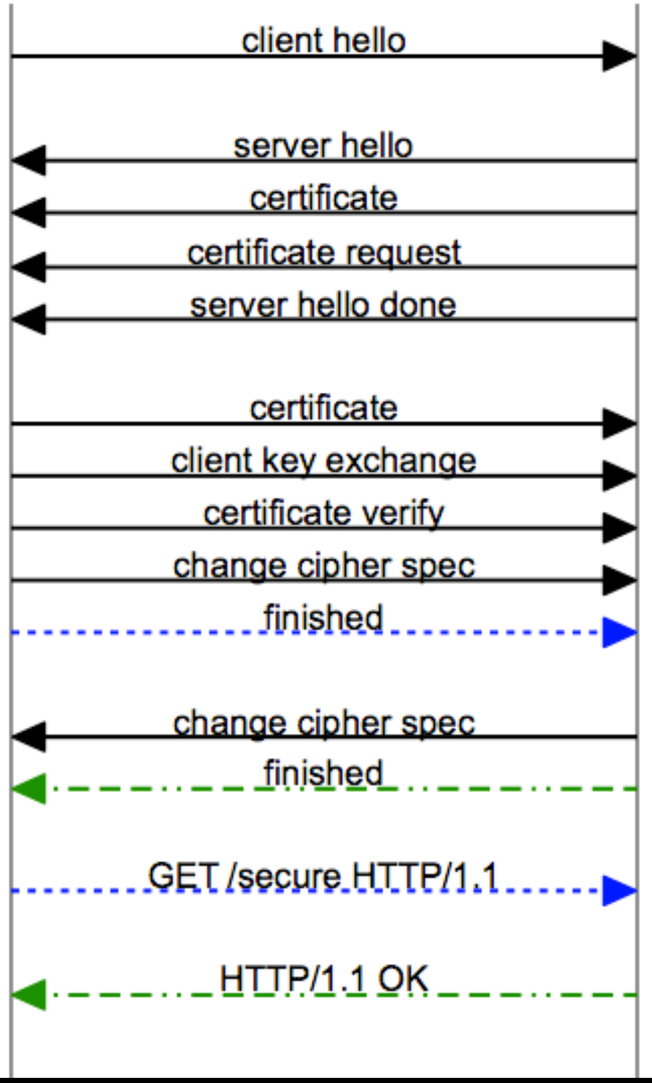
Injecting Prefixes

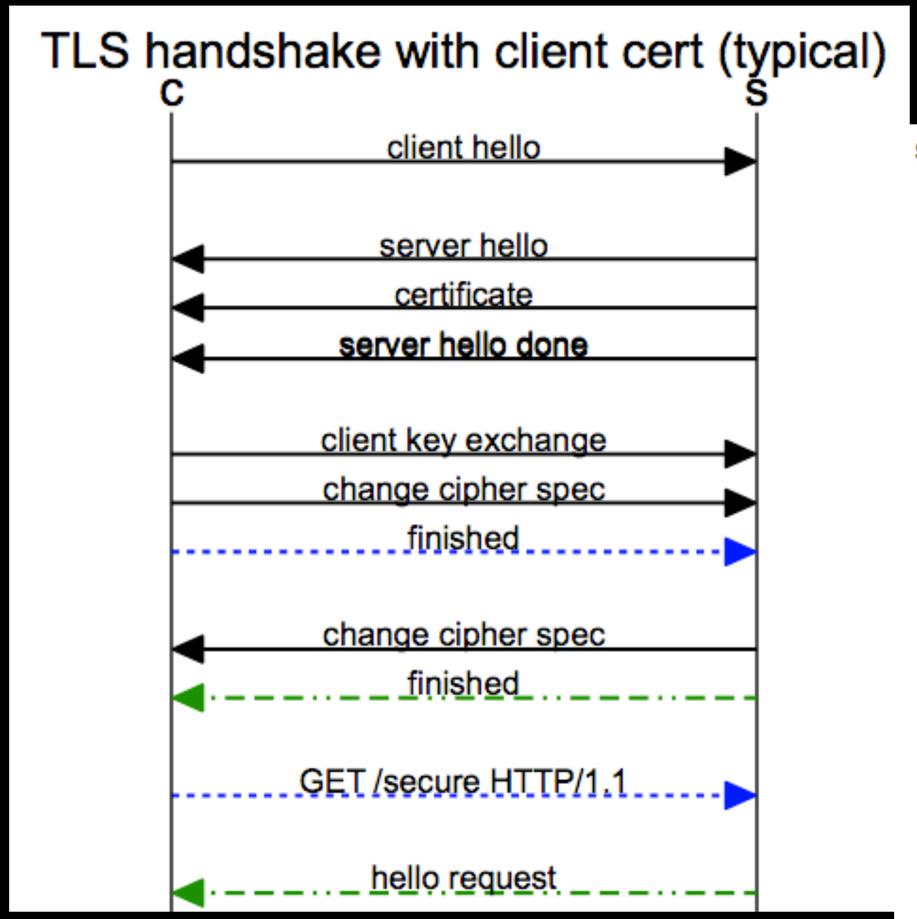
- Ray, Dispensa, 11/2009:
  - Many web servers require client-side auth, but only for certain resources

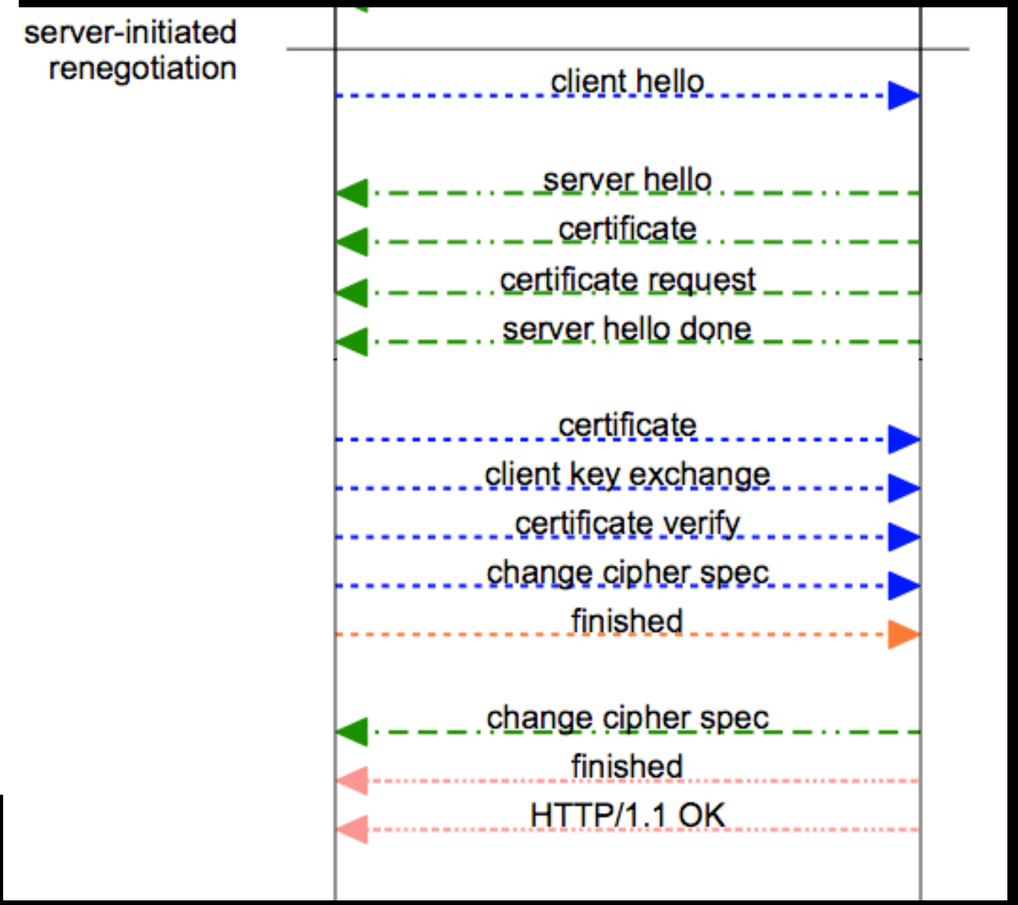
```
GET /highsecurity/index.html HTTP/1.1
Host: example.com
Connection: keep-alive
```

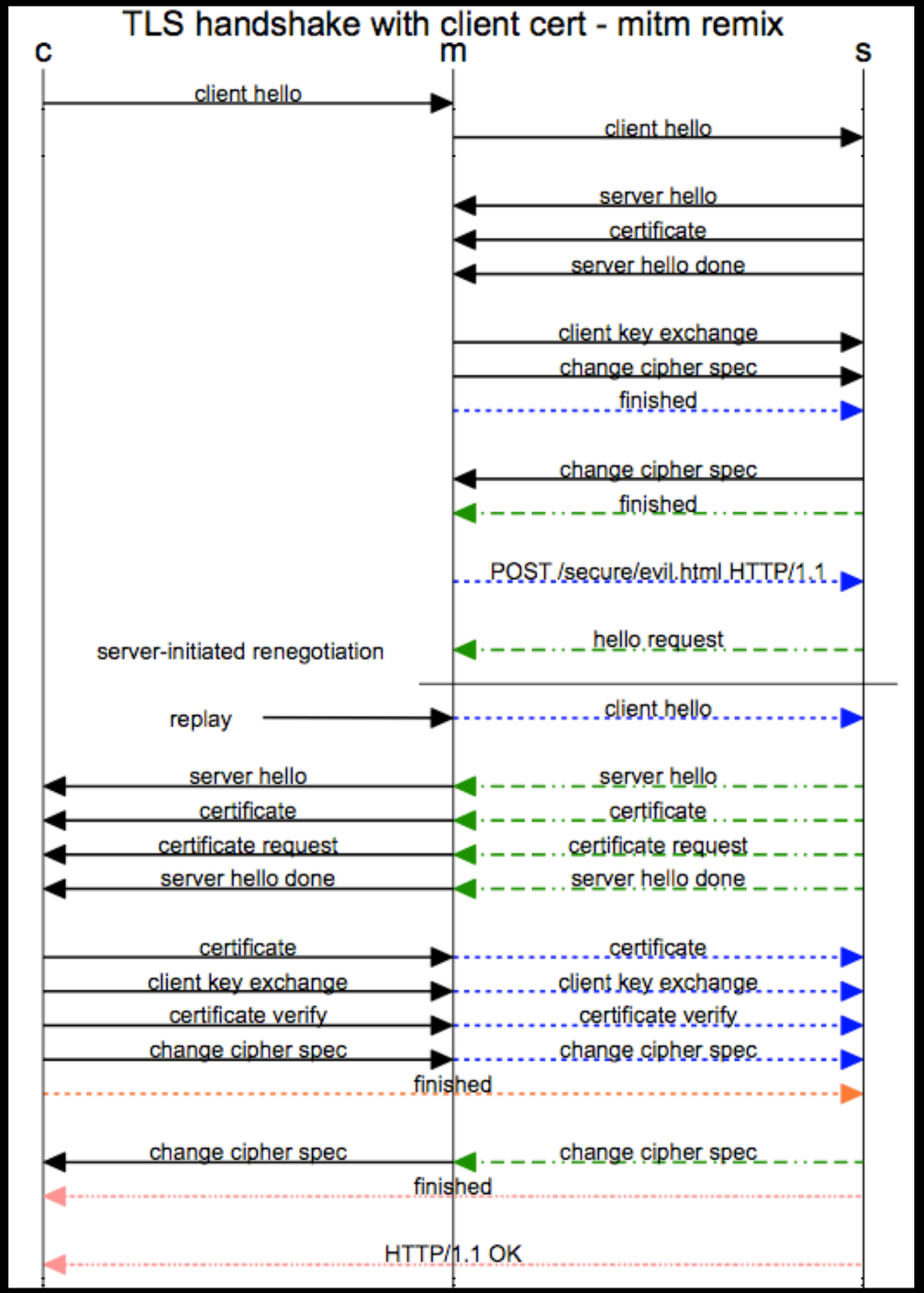
  - This may require an on-the-fly TLS re-negotiation

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)

Lucks, Schuler, Tews, Weinmann, Wenzel: Attacks on the DECT authentication mechanisms

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!

Lucks, Schuler, Tews, Weinmann, Wenzel: Attacks on the DECT authentication mechanisms

DECT

- Step 2: Authentication
  - Two [illegible] commended one:

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

RS, RAND_F ←

SRES →

In common mode, only the handset is authenticated!

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

SRES == XRES?

Lucks, Schuler, Tews, Weinmann, Wenzel: Attacks on the DECT authentication mechanisms

DECT Attack

- Step 2: Authentication
  - Two commended one:

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

RS, RAND_F

SRES

Switch to Encrypted Mode?

Nope.

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

SRES == XRES?

Lucks, Schuler, Tews, Weinmann, Wenzel: Attacks on the DECT authentication mechanisms

DECT, other

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

Lucks, Schuler, Tews, Weinmann, Wenzel: Attacks on the DECT authentication mechanisms

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

Image of "DVD Jon" Johansen from http://nanocr.eu/picture.php, used under a Creative Commons license. XBox product photos by Microsoft.

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)

$r_A, Cert_A$

$r_B, Cert_B$

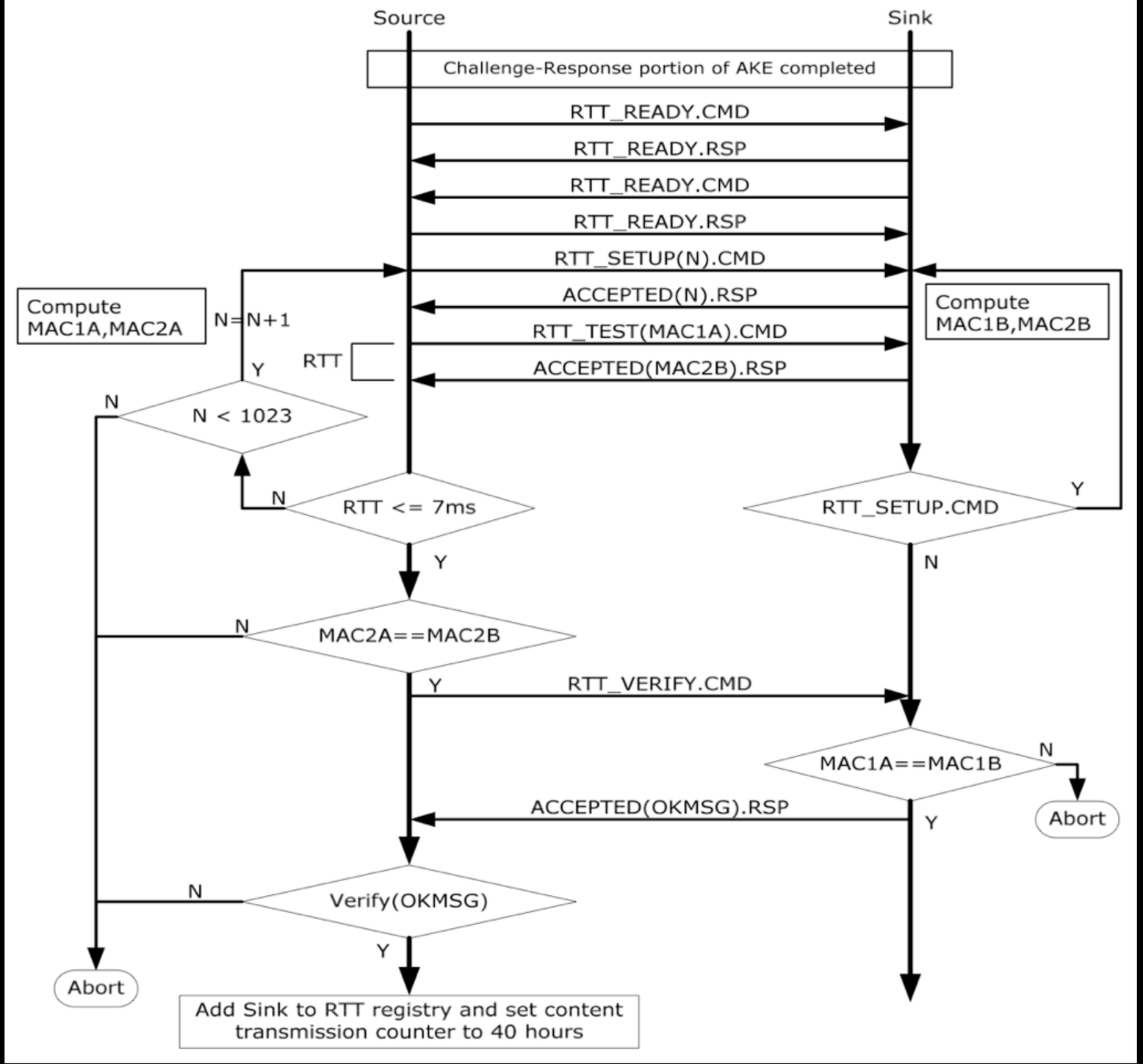
$g^a, Text_A, Sign_{sk_A}(r_A, g^a, Text_A)$

$g^b, Text_B, Sign_{sk_B}(r_B, g^b, Text_B)$

Compute shared key

Verify Shared Key (Localization)

Talk!


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
N
MAC1A==MAC1B
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

[change cipher spec to Auth]

[finalize: MAC]

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Ciphersuite Rollback

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Ciphersuite Rollback

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

[change c… …pec to Auth]

[finalize: Encrypted MAC]

Server thinks encryption is disabled, but gets an encrypted MAC

Wagner, Schneier: Analysis of the SSL 3.0 Protocol