SSL/TLS

*Slides borrowed from Vitaly Shmatikov

Optional Reading

- Kaufman. Chapters 15.1-7 and 19.

What Is SSL/TLS?

- Secure Sockets Layer and Transport Layer Security protocols
  - Same protocol design, different crypto algorithms
- De facto standard for Internet security
  - "The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications"
- Deployed in every Web browser; also VoIP, payment systems, distributed systems, etc.

SSL / TLS Guarantees

- End-to-end secure communications in the presence of a network attacker
  - Attacker completely 0wns the network: controls Wi-Fi, DNS, routers, his own websites, can listen to any packet, modify packets in transit, inject his own packets into the network
- Scenario: you are reading your email from an Internet café connected via a r00ted Wi-Fi access point to a dodgy ISP in a hostile authoritarian country

History of the Protocol

- SSL 1.0 – internal Netscape design, early 1994?
  - Lost in the mists of time
- SSL 2.0 – Netscape, Nov 1994
  - Several weaknesses
- SSL 3.0 – Netscape and Paul Kocher, Nov 1996
- TLS 1.0 – Internet standard, Jan 1999
  - Based on SSL 3.0, but not interoperable (uses different cryptographic algorithms)
- TLS 1.1 – Apr 2006
- TLS 1.2 – Aug 2008

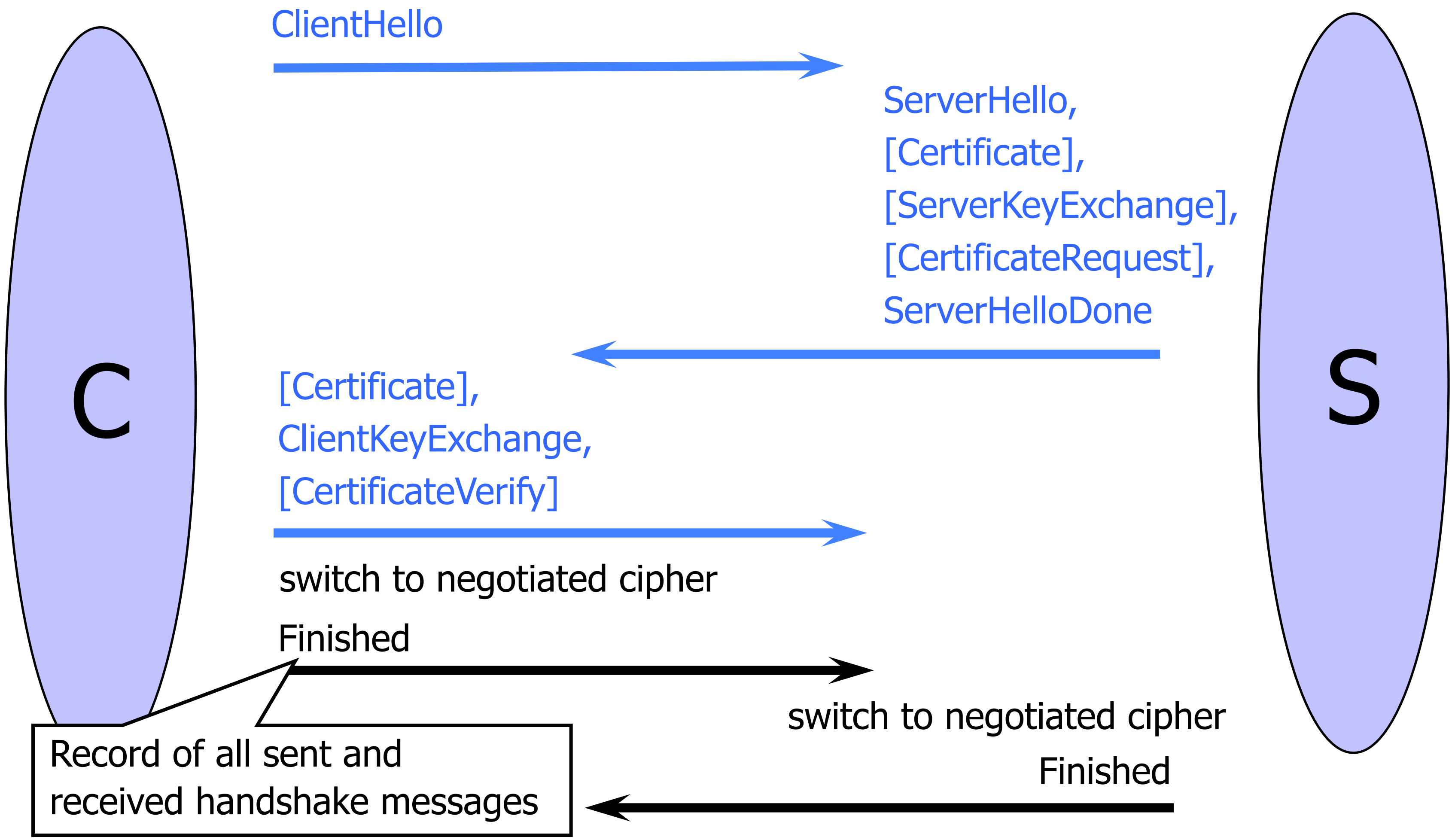
SSL Basics

- SSL consists of two protocols
- Handshake protocol
  - Uses public-key cryptography to establish several shared secret keys between the client and the server
- Record protocol
  - Uses the secret keys established in the handshake protocol to protect confidentiality, integrity, and authenticity of data exchange between the client and the server

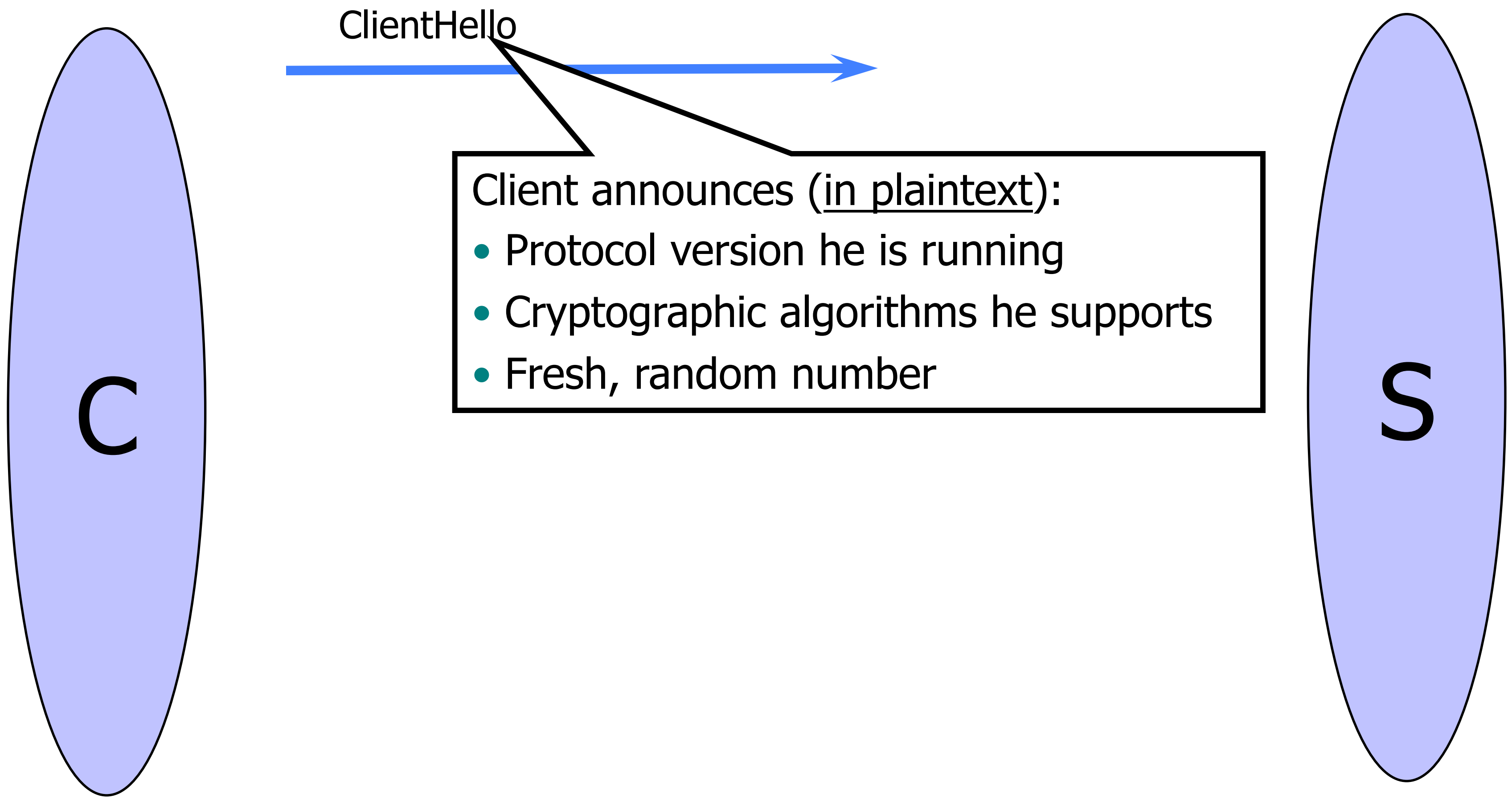
SSL Handshake Protocol

- Runs between a client and a server
  - For example, client = Web browser, server = website
- Negotiate version of the protocol and the set of cryptographic algorithms to be used
  - Interoperability between different implementations
- Authenticate server and client (optional)
  - Use digital certificates to learn each other's public keys and verify each other's identity
  - Often only the server is authenticated
- Use public keys to establish a shared secret

Handshake Protocol Structure



ClientHello



Client announces (in plaintext):

- Protocol version he is running
- Cryptographic algorithms he supports
- Fresh, random number

ClientHello (RFC)

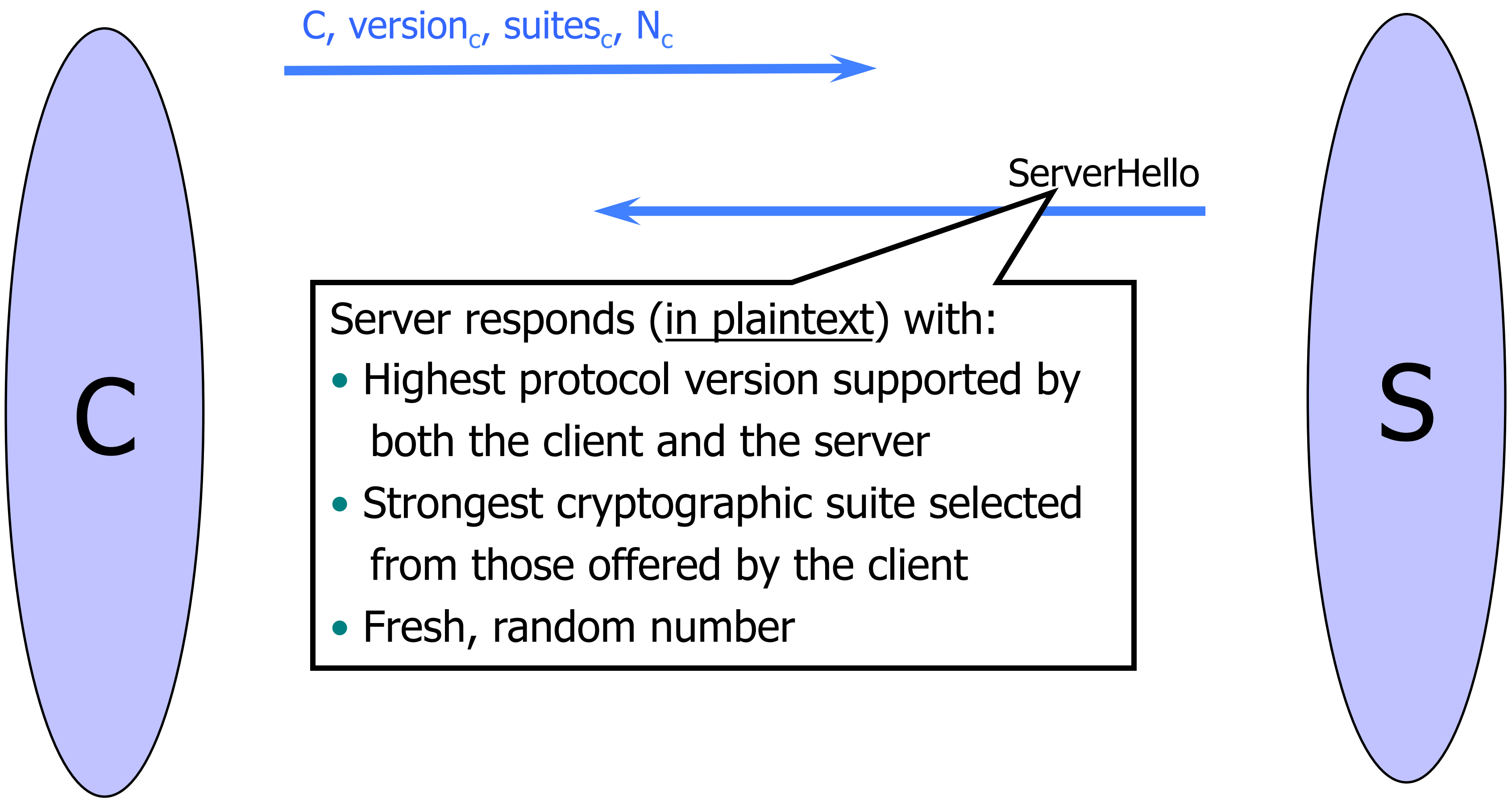
```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites;
    CompressionMethod compression_methods;
} ClientHello
```

Highest version of the protocol supported by the client

Session id (if the client wants to resume an old session)

Set of cryptographic algorithms supported by the client (e.g., RSA or Diffie-Hellman)

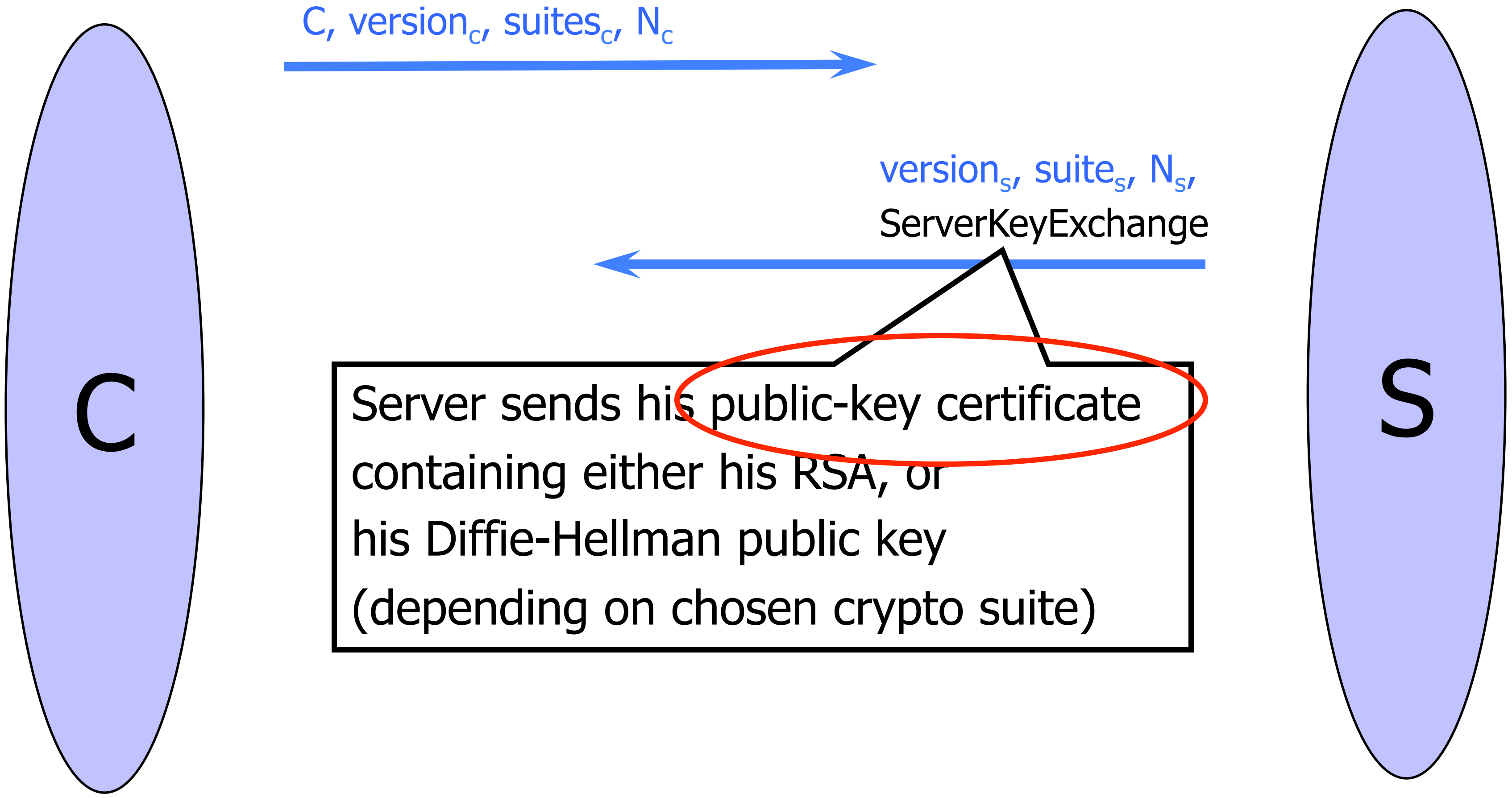
ServerHello



Server responds (in plaintext) with:

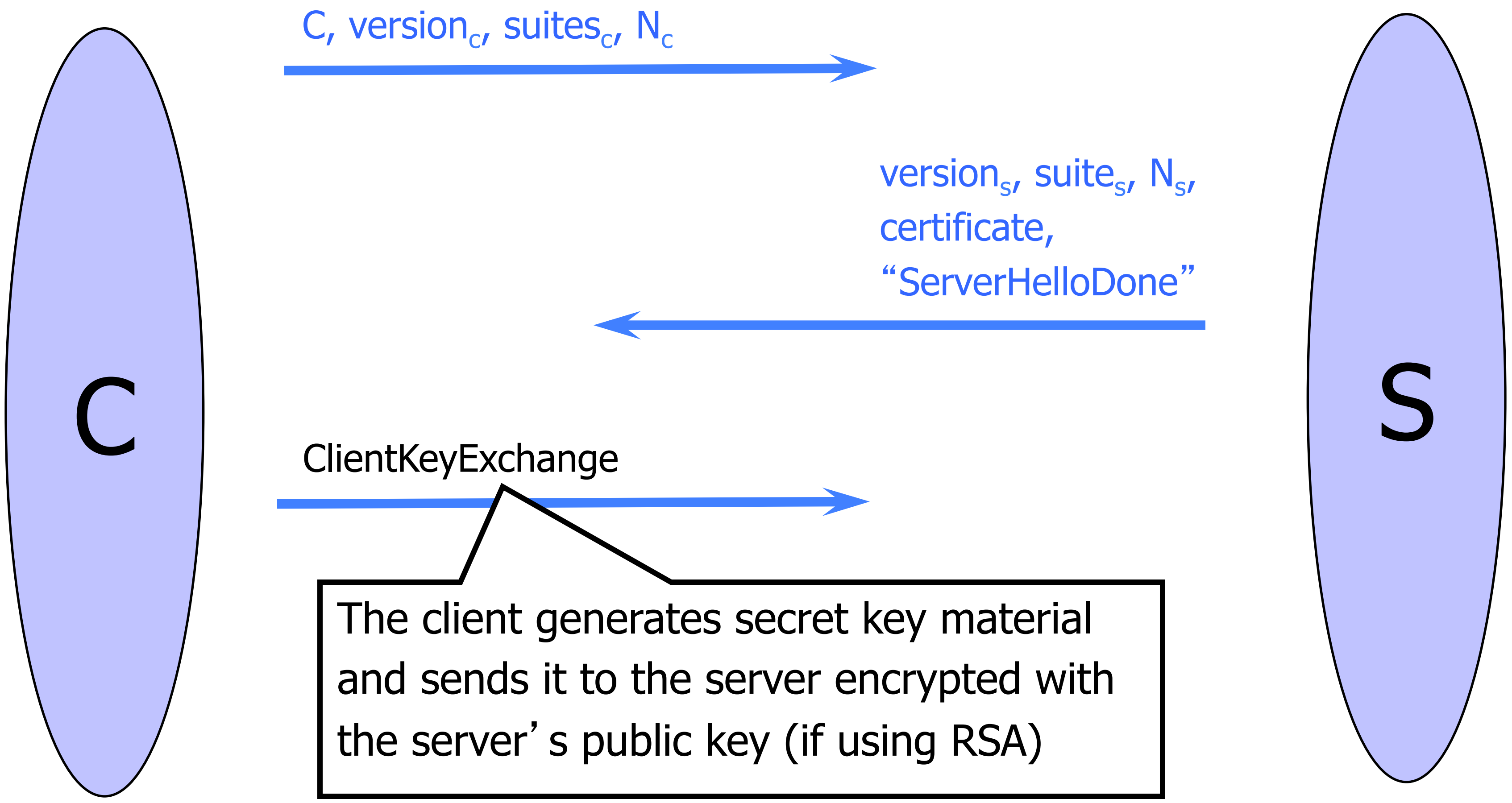
- Highest protocol version supported by both the client and the server
- Strongest cryptographic suite selected from those offered by the client
- Fresh, random number

ServerKeyExchange


C, version$_c$, suites$_c$, N$_c$
version$_s$, suite$_s$, N$_s$,
ServerKeyExchange
C
S

Server sends his public-key certificate containing either his RSA, or his Diffie-Hellman public key (depending on chosen crypto suite)

ClientKeyExchange


C, version$_c$, suites$_c$, N_c
version$_s$, suite$_s$, N_s, certificate, "ServerHelloDone"
C
S
ClientKeyExchange

The client generates secret key material and sends it to the server encrypted with the server's public key (if using RSA)

ClientKeyExchange (RFC)

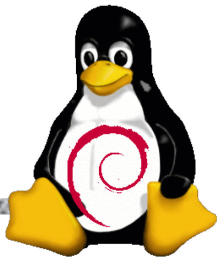
```
struct {
   select (KeyExchangeAlgorithm) {
      case rsa: EncryptedPreMasterSecret;
      case diffie_hellman: ClientDiffieHellmanPublic;
   } exchange_keys
} ClientKeyExchange

struct {
   ProtocolVersion client_version;
   opaque random[46];
} PreMasterSecret
```

Where do random bits come from?

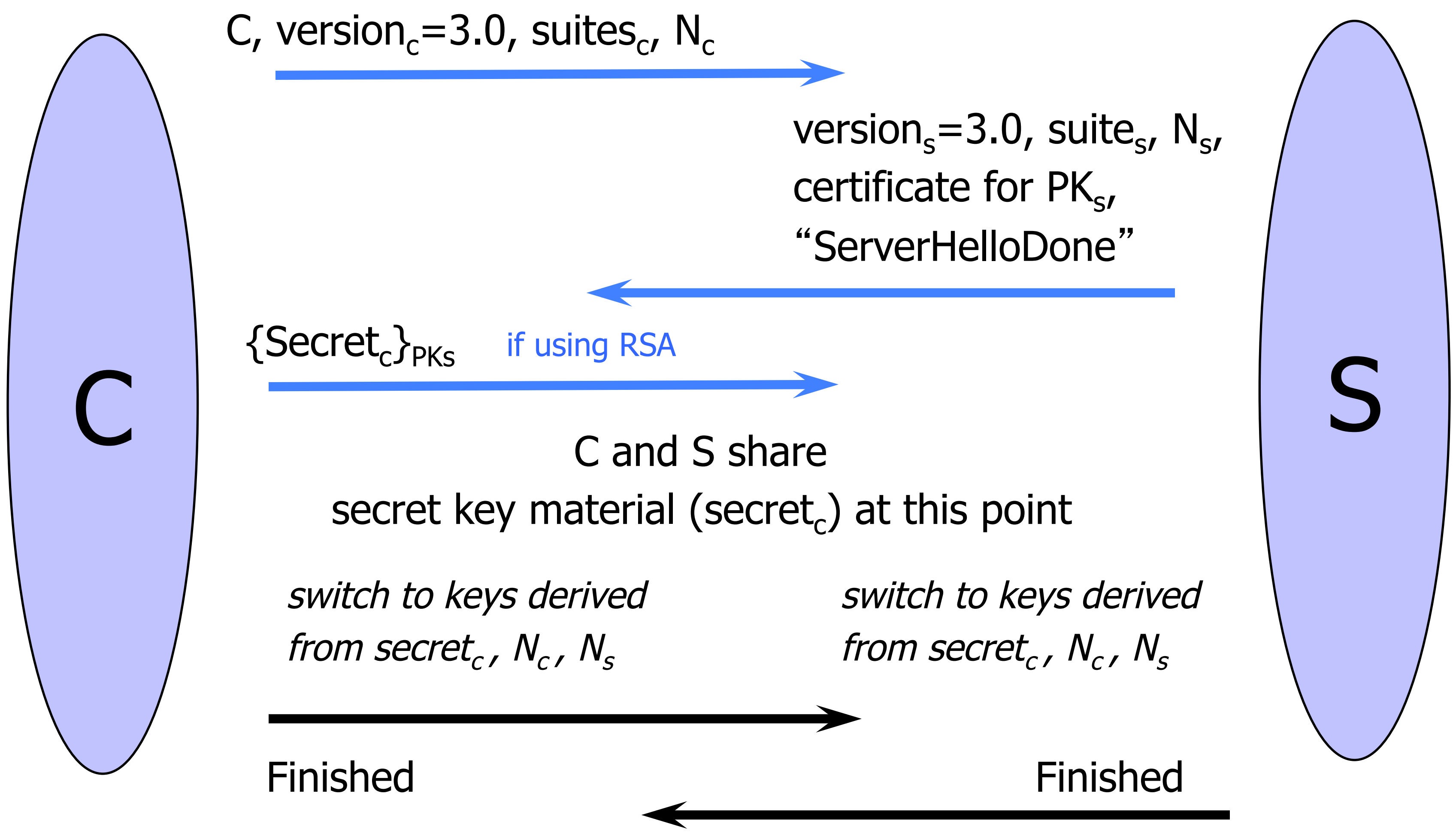
Random bits from which symmetric keys will be derived (by hashing them with nonces)

Debian Linux (2006-08)

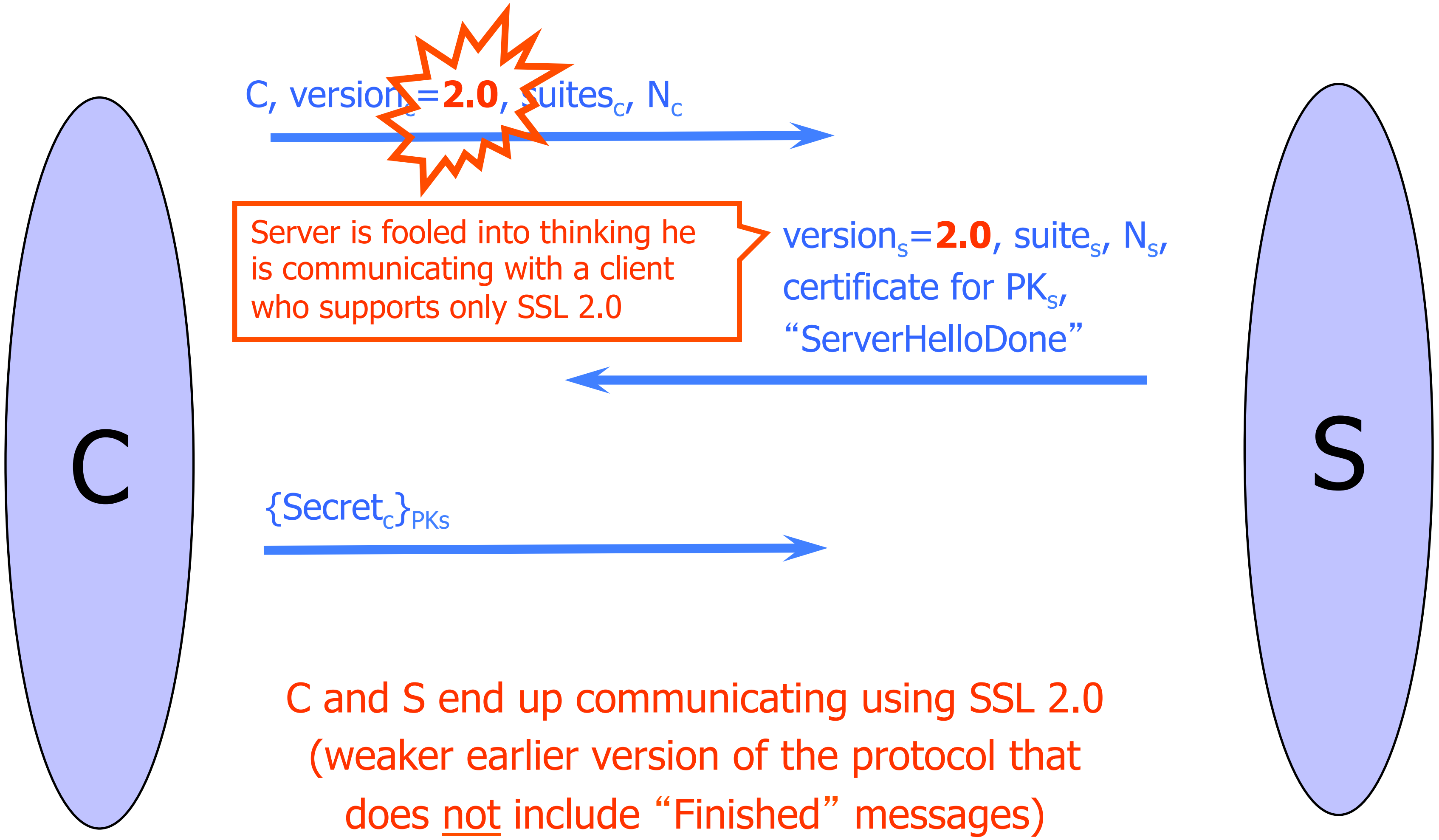


- A line of code commented out from md_rand
  - MD_Update(&m,buf,j); /* purify complains */
- Without this line, the seed for the pseudo-random generator is derived only from process ID
  - Default maximum on Linux = 32768
- Result: <u>all</u> keys generated using Debian-based OpenSSL package in 2006-08 are predictable
  - "Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections"

"Core" SSL 3.0 Handshake


C, version_c=3.0, suites_c, N_c
version_s=3.0, suite_s, N_s,
certificate for PK_s,
"ServerHelloDone"
$\{\text{Secret}_c\}_{PKs}$
if using RSA
C and S share
secret key material (secret_c) at this point
switch to keys derived from secret_c, N_c, N_s
switch to keys derived from secret_c, N_c, N_s
Finished
Finished
C
S

Version Rollback Attack



C, version_c=**2.0**, suites_c, N_c
Server is fooled into thinking he is communicating with a client who supports only SSL 2.0
version_s=**2.0**, suite_s, N_s, certificate for PK_s, "ServerHelloDone"
$\{\text{Secret}_c\}_{PKs}$
C
S

C and S end up communicating using SSL 2.0 (weaker earlier version of the protocol that does not include "Finished" messages)

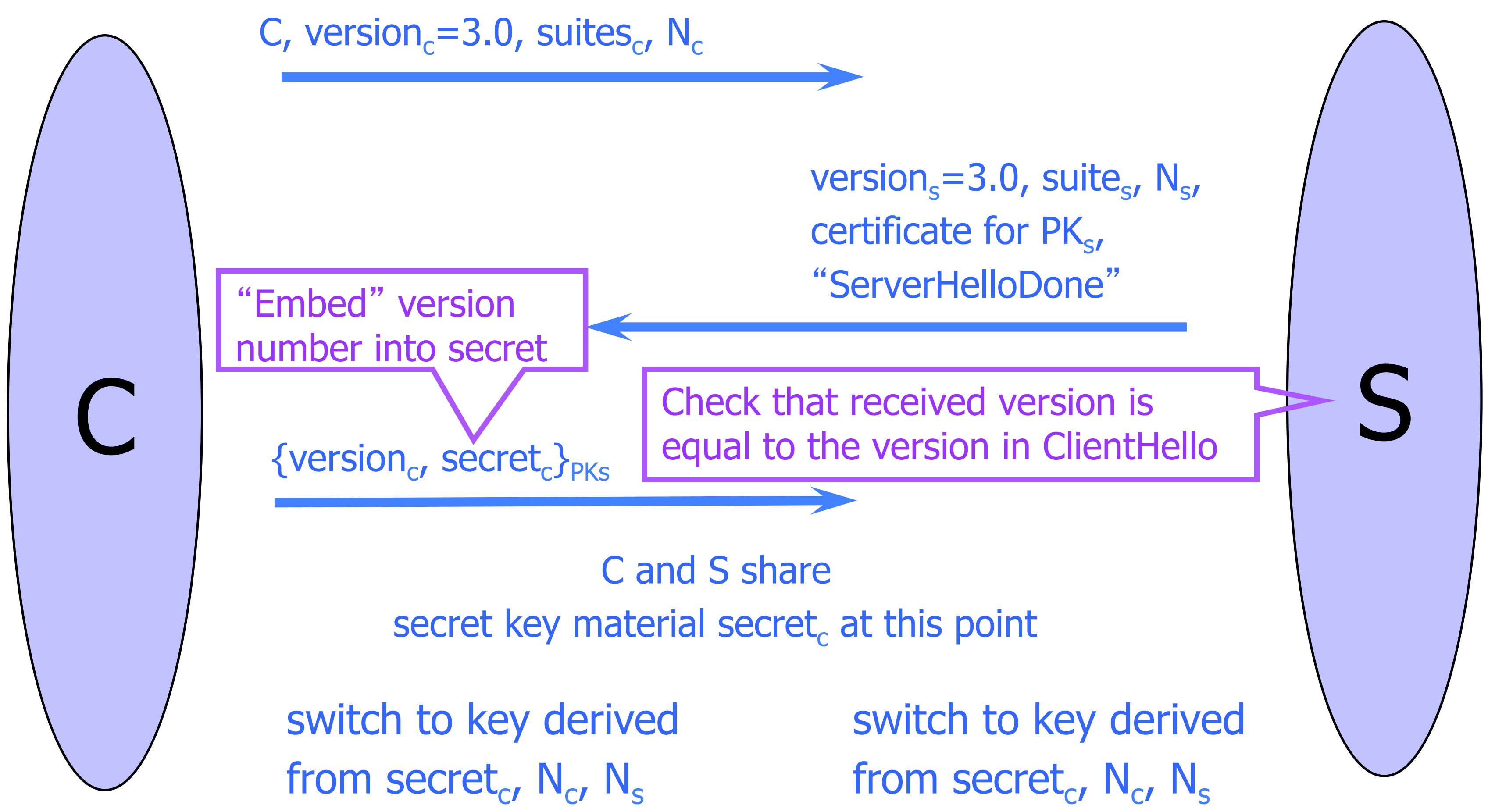
SSL 2.0 Weaknesses (Fixed in 3.0)

- Cipher suite preferences are not authenticated
  - “Cipher suite rollback” attack is possible
- Weak MAC construction, MAC hash uses only 40 bits in export mode
- SSL 2.0 uses padding when computing MAC in block cipher modes, but padding length field is not authenticated
  - Attacker can delete bytes from the end of messages
- No support for certificate chains or non-RSA algorithms

“Chosen-Protocol” Attacks

- Why do people release new versions of security protocols? Because the old version got broken!
- New version must be backward-compatible
  - Not everybody upgrades right away
- Attacker can fool someone into using the old, broken version and exploit known vulnerabilities
  - Similar: fool victim into using weak crypto algorithms
- Defense is hard: must authenticate version early
- Many protocols had “version rollback” attacks
  - SSL, SSH, GSM (cell phones)

Version Check in SSL 3.0


C, version$_c$=3.0, suites$_c$, N$_c$
version$_s$=3.0, suite$_s$, N$_s$,
certificate for PK$_s$,
"ServerHelloDone"
"Embed" version number into secret
Check that received version is equal to the version in ClientHello
{version$_c$, secret$_c$}$_{PKs}$
C
S
C and S share secret key material secret$_c$ at this point
switch to key derived from secret$_c$, N$_c$, N$_s$
switch to key derived from secret$_c$, N$_c$, N$_s$

Exploiting SSL for Denial of Service

https://www.thc.org/thc-ssl-dos/

2 simple commands in bash:

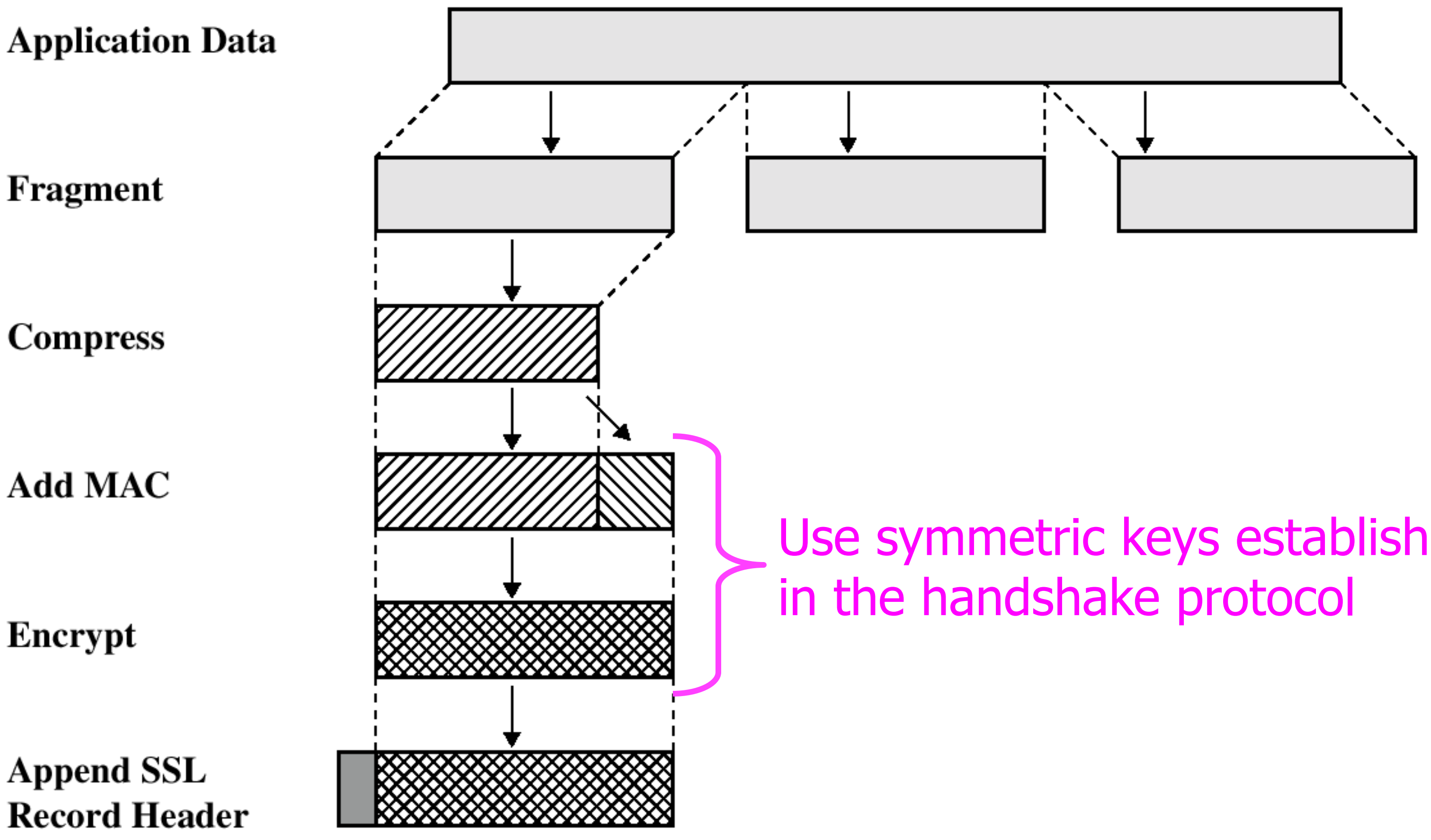
```
-----BASH SCRIPT BEGIN-----
thc-ssl-dosit() { while :; do (while :; do echo R; done) | openssl s_client
-connect 127.0.0.1:443 2>/dev/null; done }
for x in `seq 1 100`; do thc-ssl-dosit & done
-----BASH SCRIPT END-------
```

THC-SSL-DOS is a tool to verify the performance of SSL

Establishing a secure SSL connection requires 15x more processing power on the server than on the client

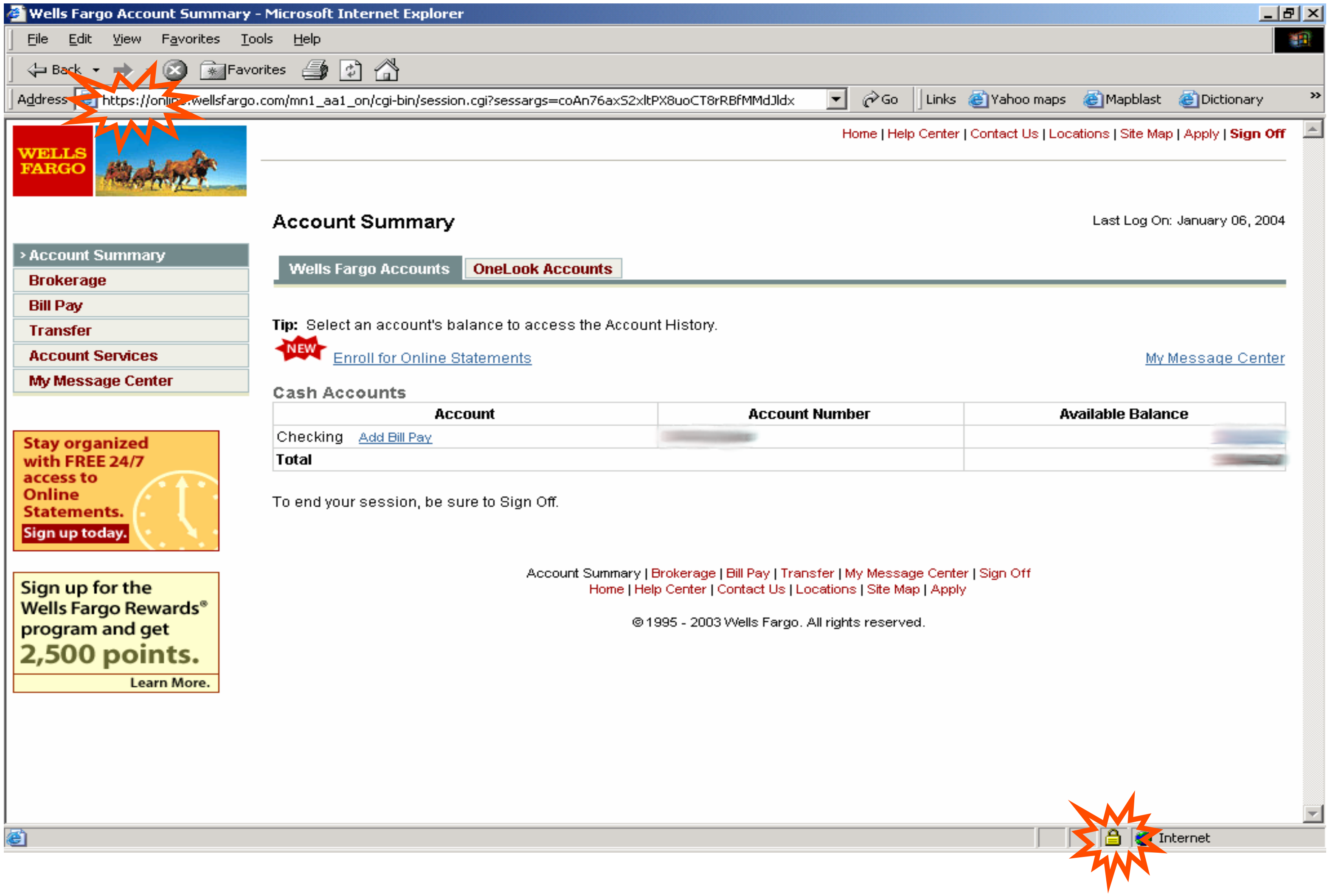
"THC-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet"

SSL/TLS Record Protection



Use symmetric keys established in the handshake protocol

Most Common Use of SSL/TLS


Wells Fargo Account Summary - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Favorites

Address https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76axS2xltPX8uoCT8rRBfMMdJldx Go Links Yahoo maps Mapblast Dictionary

WELLS FARGO

Home | Help Center | Contact Us | Locations | Site Map | Apply | **Sign Off**

Account Summary

Last Log On: January 06, 2004

- › Account Summary
- Brokerage
- Bill Pay
- Transfer
- Account Services
- My Message Center

Wells Fargo Accounts | OneLook Accounts

Tip: Select an account's balance to access the Account History.

NEW Enroll for Online Statements

My Message Center

Cash Accounts

Account	Account Number	Available Balance
Checking Add Bill Pay	[redacted]	[redacted]
Total		[redacted]

To end your session, be sure to Sign Off.

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.

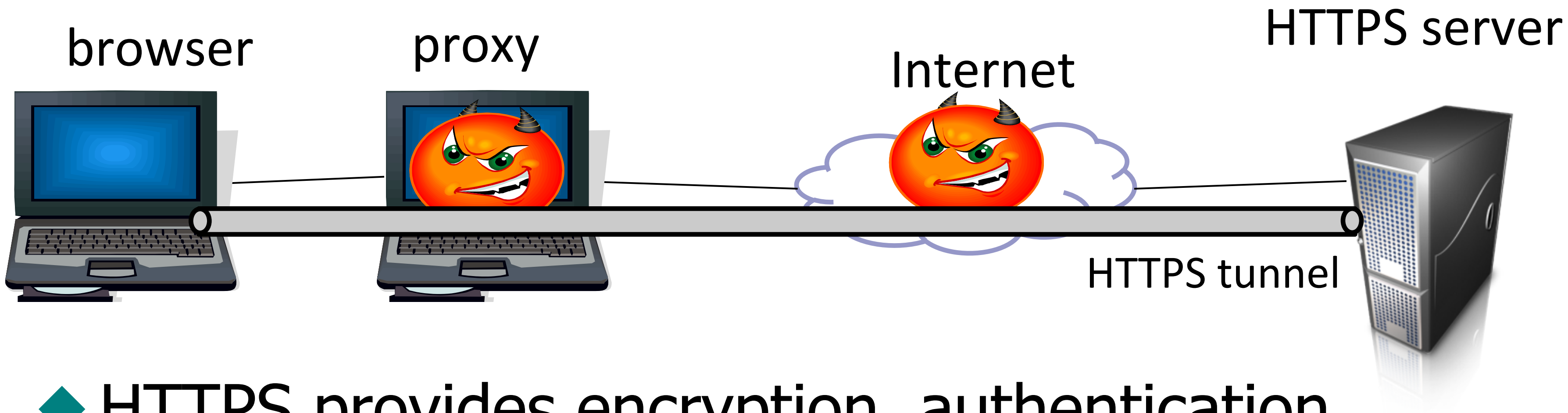
Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off
Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.

Internet

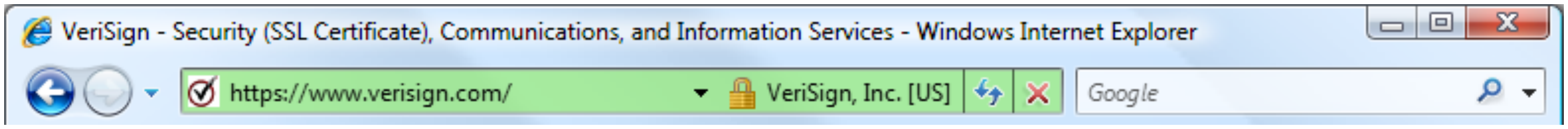
HTTPS and Its Adversary Model

- HTTPS: end-to-end secure protocol for Web
- Designed to be secure against network attackers, including man-in-the-middle (MITM) attacks



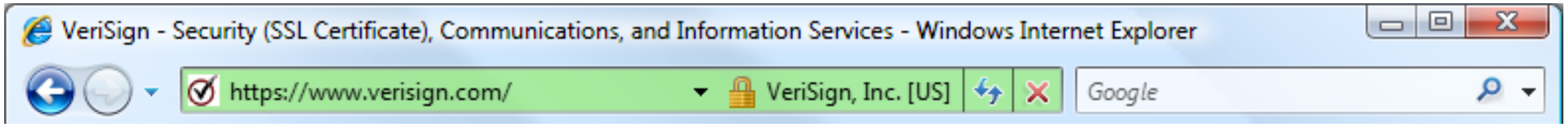
- HTTPS provides encryption, authentication (usually for server only), and integrity checking

The Lock Icon


VeriSign - Security (SSL Certificate), Communications, and Information Services - Windows Internet Explorer
https://www.verisign.com/
VeriSign, Inc. [US]
Google

- Goal: identify secure connection
  - SSL/TLS is being used between client and server to protect against active network attacker
- Lock icon should only be shown when the page is secure against network attacker
  - Semantics subtle and not widely understood by users
  - Problem in user interface design

HTTPS Security Guarantees

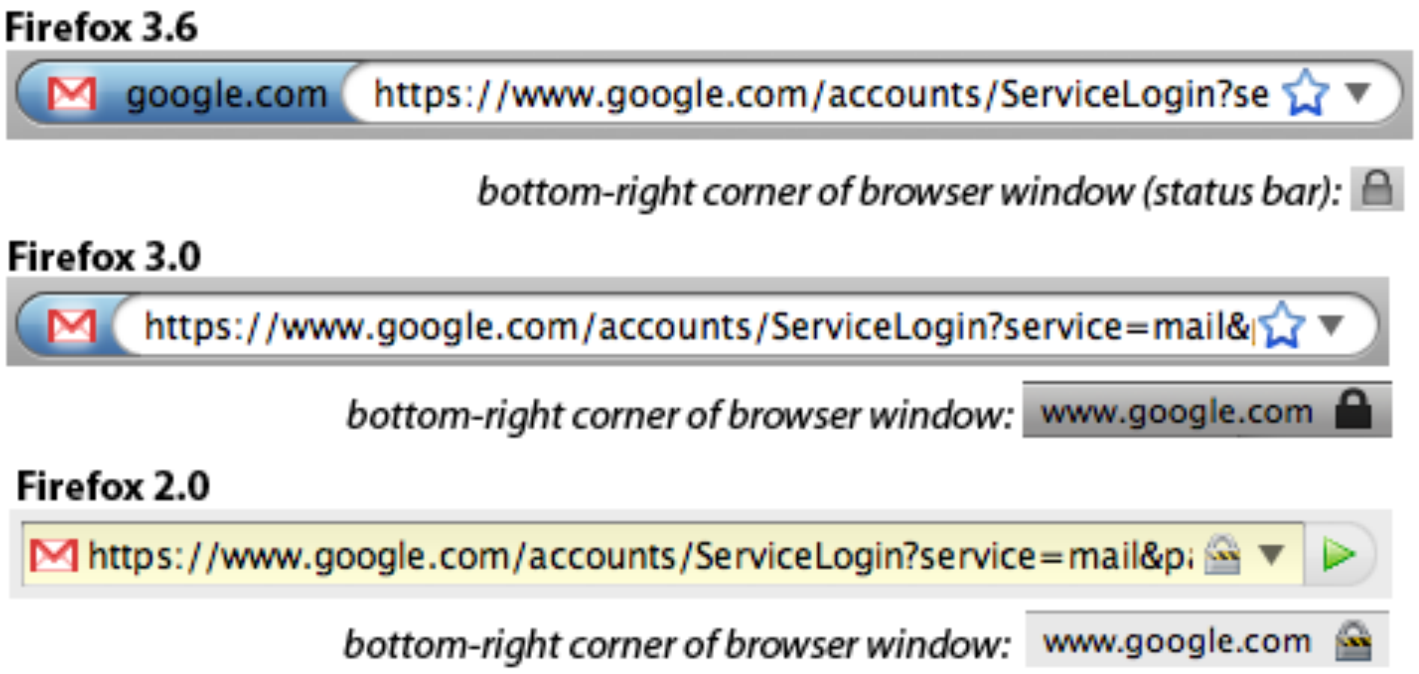

VeriSign - Security (SSL Certificate), Communications, and Information Services - Windows Internet Explorer
https://www.verisign.com/
VeriSign, Inc. [US]
Google

- The origin of the page is what it says in the address bar
  - User must interpret what he sees - remember amazonaccounts.com?
- Contents of the page have not been viewed or modified by a network attacker

Evolution of the Lock in Firefox

[Schultze]

How about Firefox 4?


Firefox 3.6

google.com https://www.google.com/accounts/ServiceLogin?se

bottom-right corner of browser window (status bar):

Firefox 3.0

https://www.google.com/accounts/ServiceLogin?service=mail&

bottom-right corner of browser window: www.google.com

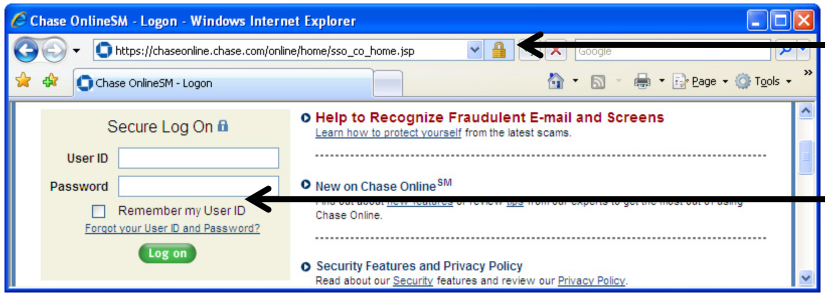
Firefox 2.0

https://www.google.com/accounts/ServiceLogin?service=mail&p

bottom-right corner of browser window: www.google.com

Combining HTTPS and HTTP

- Page served over HTTPS but contains HTTP
  - IE 7: no lock, “mixed content” warning
  - Firefox: “!” over lock, no warning by default
  - Safari: does not detect mixed content



https://chaseonline.chase.com/online/home/sso_co_home.jsp

Secure Log On

User ID

Password

Remember my User ID

Forgot your User ID and Password?

Help to Recognize Fraudulent E-mail and Screens

Learn how to protect yourself from the latest scams.

New on Chase Online^{SM}

Find out about new features or review tips from our experts to get the most out of using Chase Online.

Security Features and Privacy Policy

Read about our Security features and review our Privacy Policy.

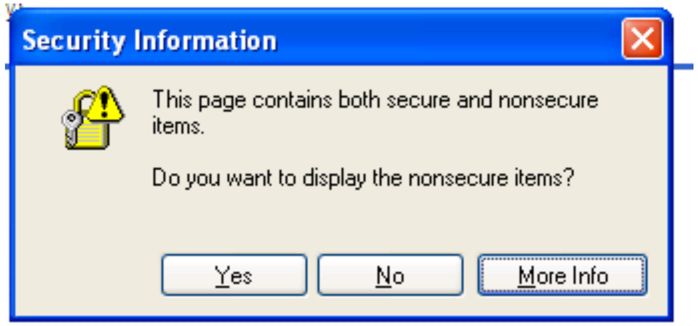
Lock icon

Flash file served over HTTP

Can script embedding page!

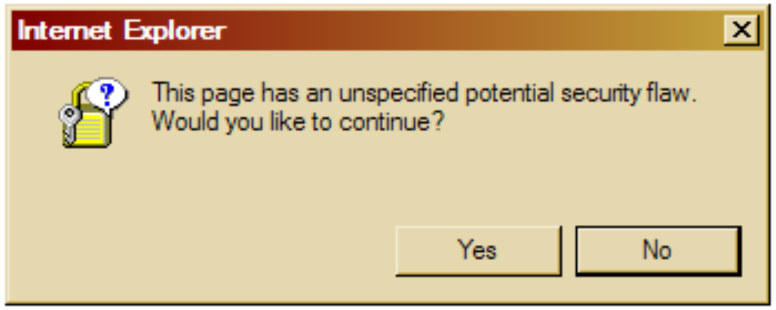
  - Flash does not trigger warning in IE7 and FF
- Network attacker can now inject scripts, hijack session

Mixed Content: UI Challenges

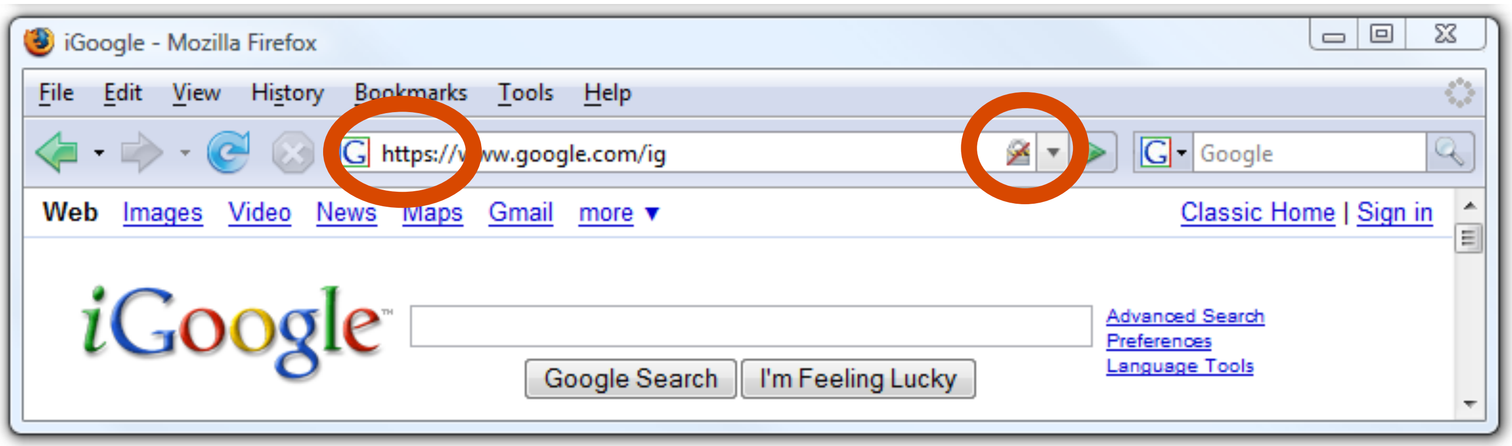

Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?


Internet Explorer

This page has an unspecified potential security flaw. Would you like to continue?



Mixed Content and Network Attacks

- Banks: after login, all content served over HTTPS
- Developer error: somewhere on bank site write

```
<script src=http://www.site.com/script.js> </script>
```

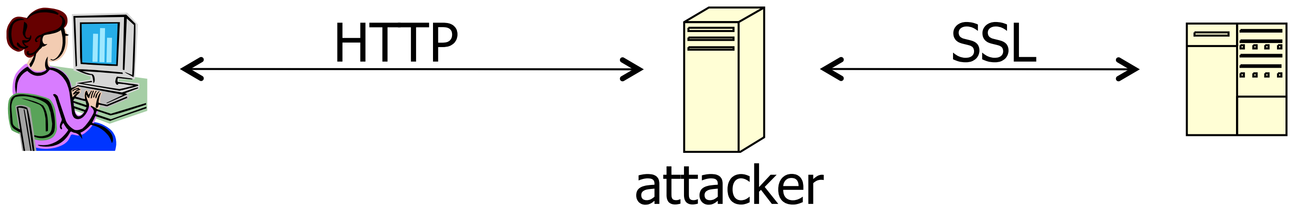
  - Active network attacker can now hijack any session (how?)
- Better way to include content:

```
<script src=//www.site.com/script.js> </script>
```

  - Served over the same protocol as embedding page

HTTP → HTTPS and Back

- Typical pattern: HTTPS upgrade
  - Come to site over HTTP, redirect to HTTPS for login
  - Browse site over HTTP, redirect to HTTPS for checkout
- sslstrip: network attacker downgrades connection

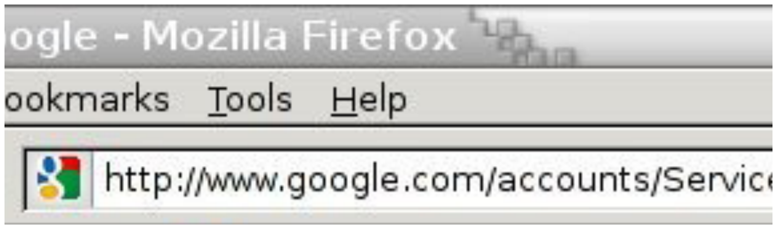


  - Rewrite <a href=https://…> to <a href=http://…>
  - Redirect Location: https://... to Location: http://...
  - Rewrite <form action=https://… > to <form action=http://…>

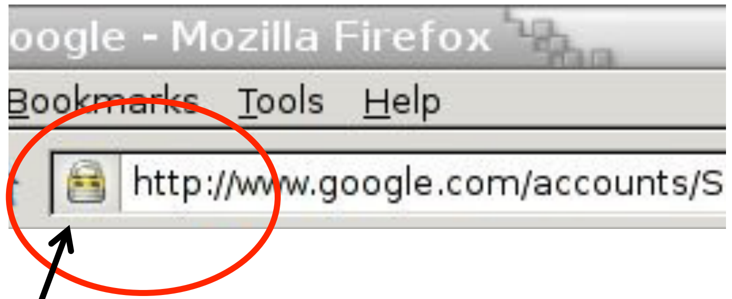
Can the server detect this attack?

Will You Notice?

[Moxie Marlinspike]



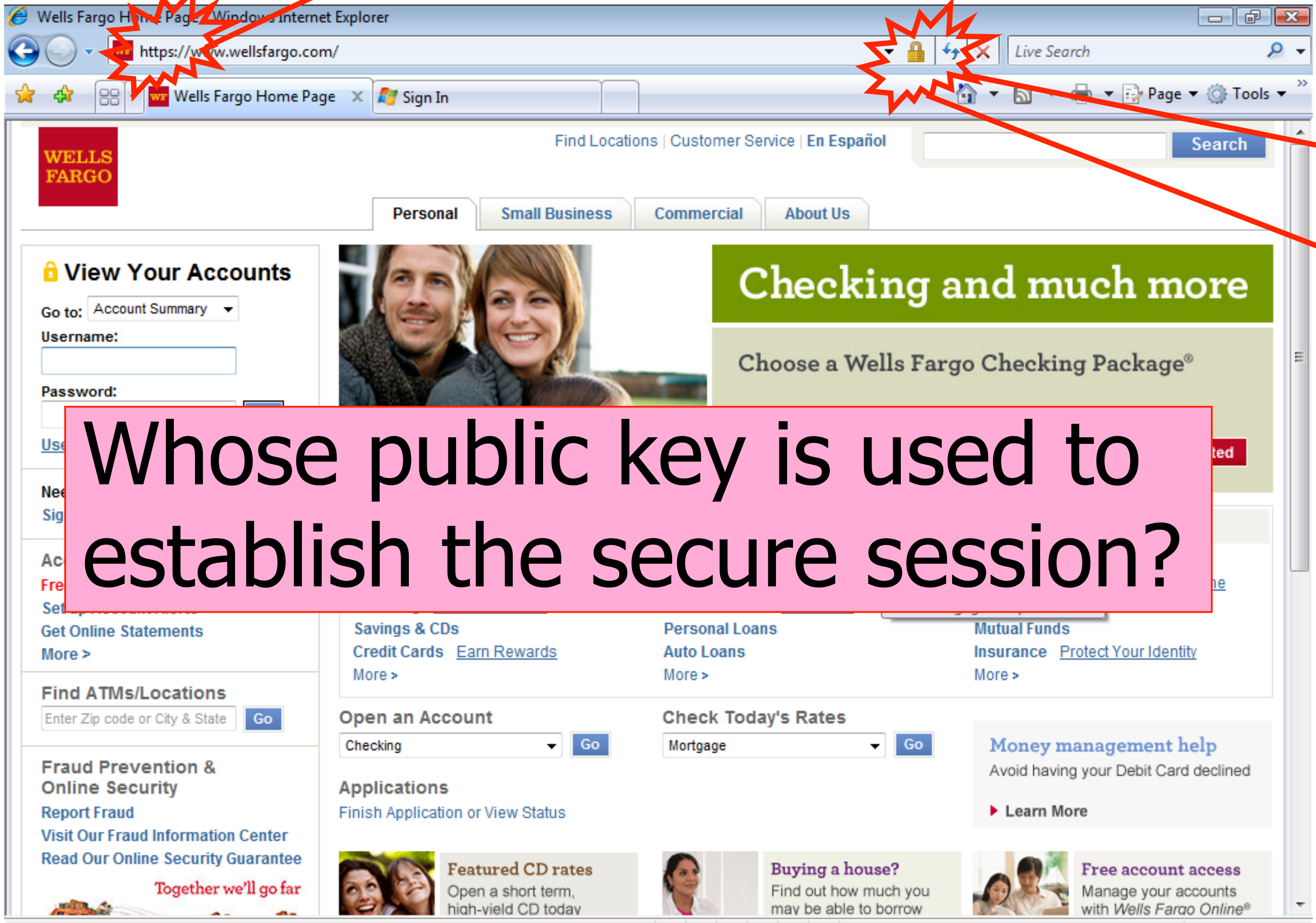
⇒



Clever favicon inserted by network attacker

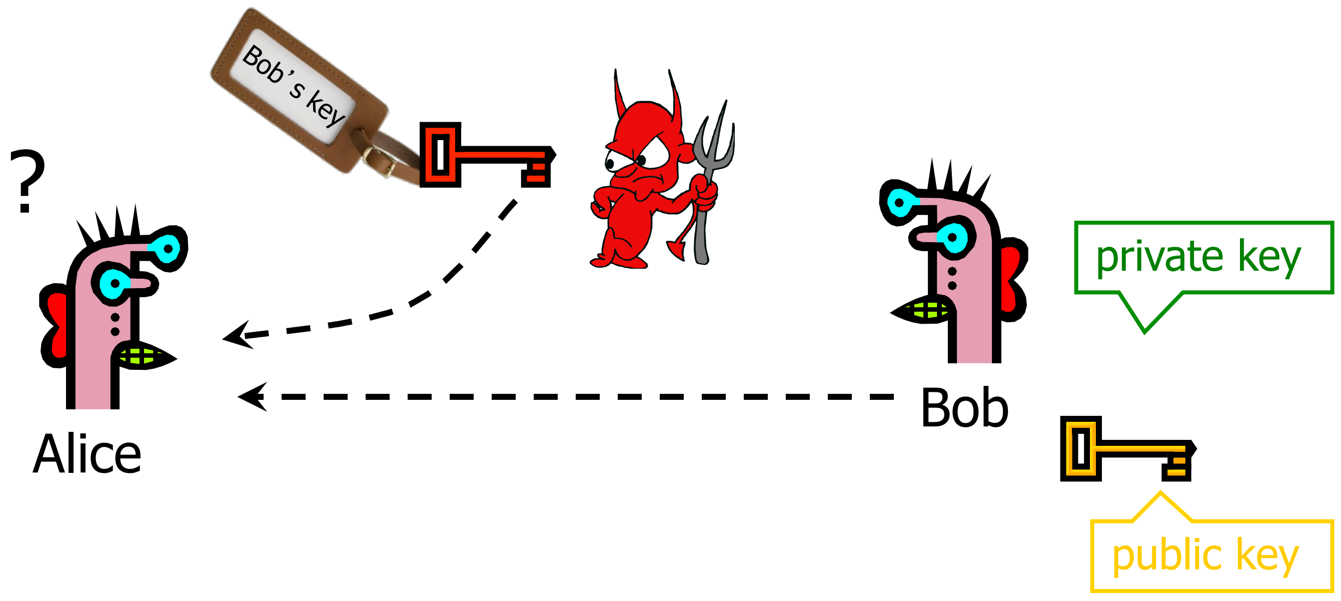
Motivation

https://


Wells Fargo Home Page - Windows Internet Explorer
https://www.wellsfargo.com/
Live Search
Wells Fargo Home Page
Sign In
Page
Tools
WELLS FARGO
Find Locations | Customer Service | En Español
Search
Personal
Small Business
Commercial
About Us
View Your Accounts
Go to: Account Summary
Username:
Password:
Checking and much more
Choose a Wells Fargo Checking Package®
Get Online Statements
More >
Find ATMs/Locations
Enter Zip code or City & State
Go
Fraud Prevention & Online Security
Report Fraud
Visit Our Fraud Information Center
Read Our Online Security Guarantee
Together we'll go far
Savings & CDs
Credit Cards Earn Rewards
Personal Loans
Auto Loans
Mutual Funds
Insurance Protect Your Identity
Open an Account
Checking
Check Today's Rates
Mortgage
Applications
Finish Application or View Status
Money management help
Avoid having your Debit Card declined
Learn More
Featured CD rates
Open a short term, high-yield CD today
Buying a house?
Find out how much you may be able to borrow
Free account access
Manage your accounts with Wells Fargo Online®

Whose public key is used to establish the secure session?

Authenticity of Public Keys

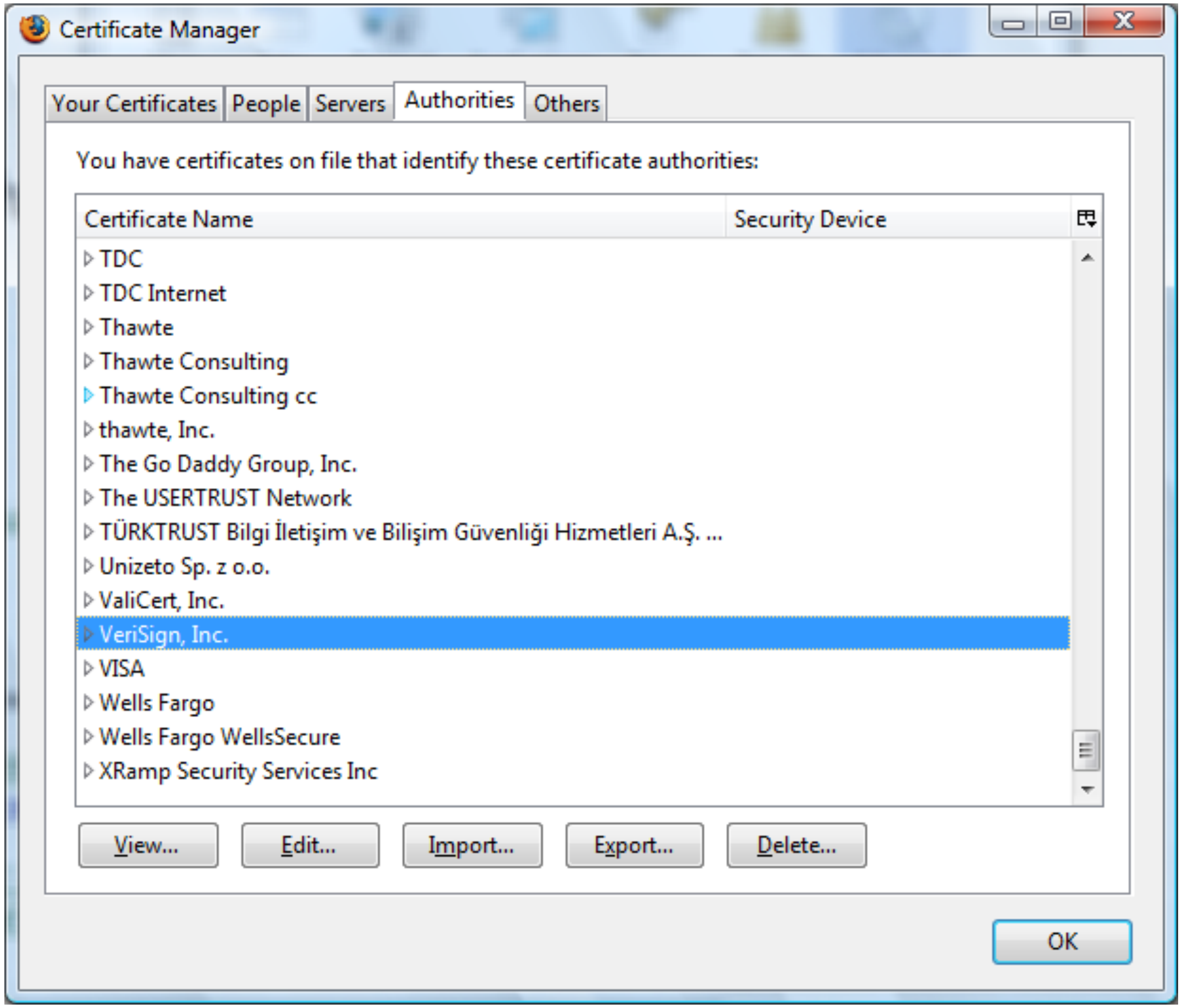


Problem: How does Alice know that the public key she received is really Bob's public key?

Distribution of Public Keys

- Public announcement or public directory
  - Risks: forgery and tampering
- Public-key certificate
  - Signed statement specifying the key and identity
    - sig_{Alice}(“Bob”, PK_B)
- Common approach: certificate authority (CA)
  - An agency responsible for certifying public keys
  - Browsers are pre-configured with 100+ of trusted CAs
  - A public key for any website in the world will be accepted by the browser if certified by one of these CAs

Trusted Certificate Authorities



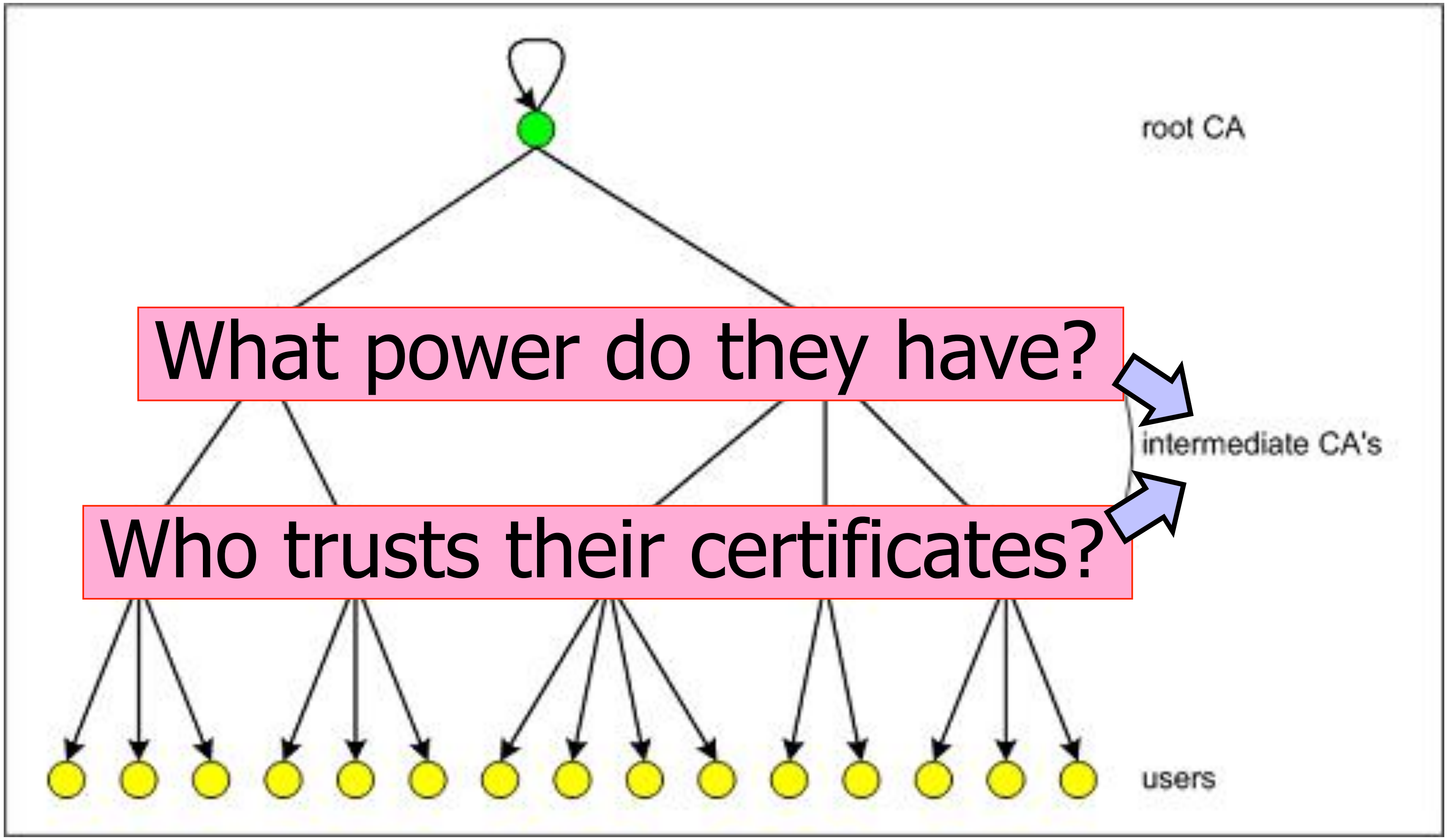
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
TDC	
TDC Internet	
Thawte	
Thawte Consulting	
Thawte Consulting cc	
thawte, Inc.	
The Go Daddy Group, Inc.	
The USERTRUST Network	
TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ...	
Unizeto Sp. z o.o.	
ValiCert, Inc.	
VeriSign, Inc.	
VISA	
Wells Fargo	
Wells Fargo WellsSecure	
XRamp Security Services Inc	

CA Hierarchy

- Browsers, operating systems, etc. have trusted root certificate authorities
  - Firefox 3 includes certificates of 135 trusted root CAs
- A Root CA signs certificates for intermediate CAs, they sign certificates for lower-level CAs, etc.
  - Certificate “chain of trust”
    - $\text{sig}_{\text{Verisign}}$(“UT Austin”, PK_{UT}), sig_{UT}(“Vitaly S.”, $\text{PK}_{\text{Vitaly}}$)
- CA is responsible for verifying the identities of certificate requestors, domain ownership

Certificate Hierarchy

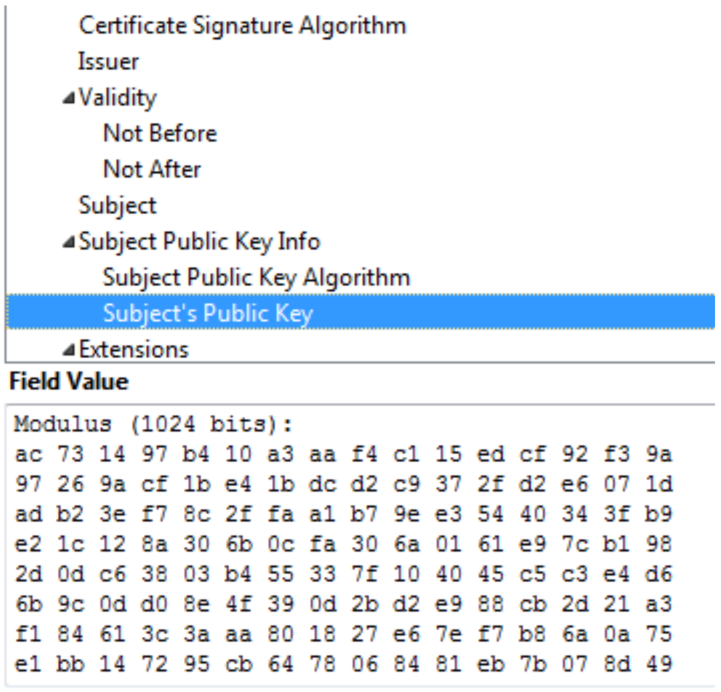


What power do they have?

Who trusts their certificates?

Example of a Certificate

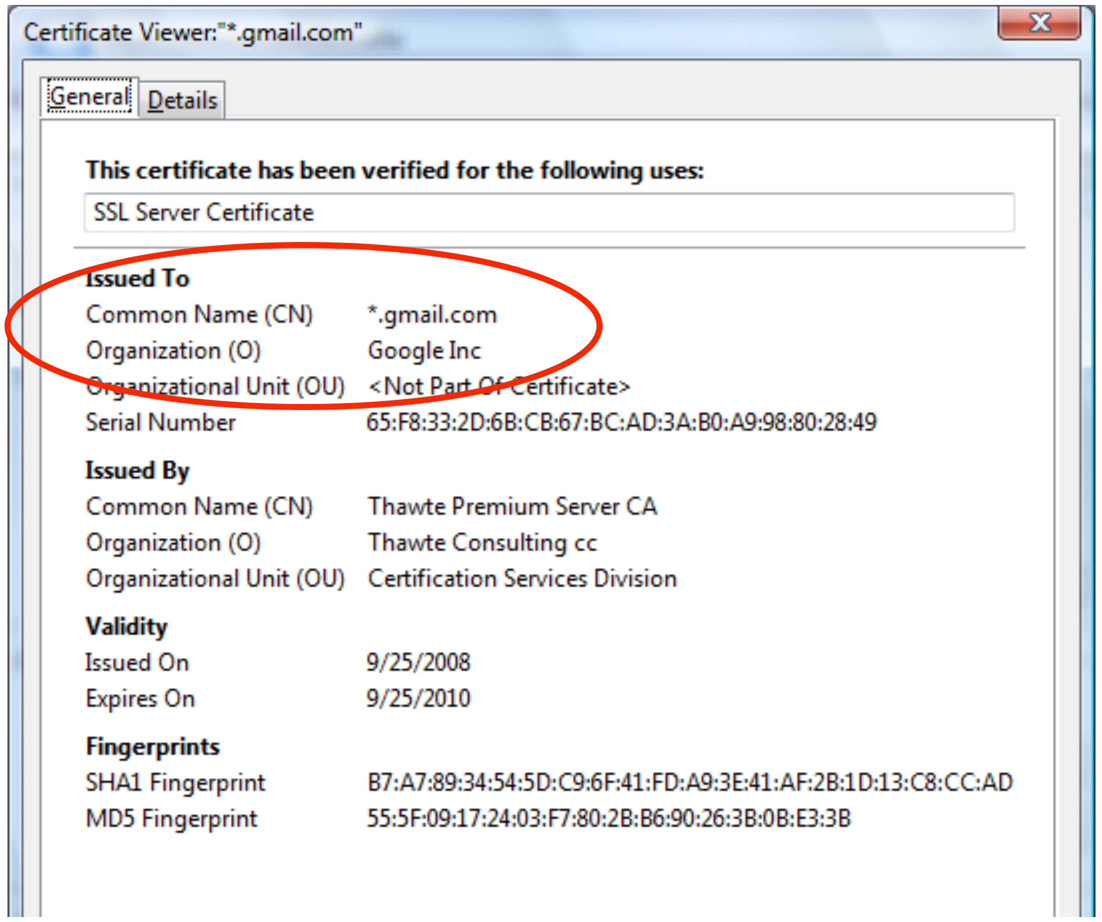
Important fields



Certificate Signature Algorithm
Issuer
◢Validity
Not Before
Not After
Subject
◢Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
◢Extensions

Field Value

```
Modulus (1024 bits):
ac 73 14 97 b4 10 a3 aa f4 c1 15 ed cf 92 f3 9a
97 26 9a cf 1b e4 1b dc d2 c9 37 2f d2 e6 07 1d
ad b2 3e f7 8c 2f fa a1 b7 9e e3 54 40 34 3f b9
e2 1c 12 8a 30 6b 0c fa 30 6a 01 61 e9 7c b1 98
2d 0d c6 38 03 b4 55 33 7f 10 40 45 c5 c3 e4 d6
6b 9c 0d d0 8e 4f 39 0d 2b d2 e9 88 cb 2d 21 a3
f1 84 61 3c 3a aa 80 18 27 e6 7e f7 b8 6a 0a 75
e1 bb 14 72 95 cb 64 78 06 84 81 eb 7b 07 8d 49
```



Certificate Viewer:"*.gmail.com"

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	*.gmail.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	65:F8:33:2D:6B:CB:67:BC:AD:3A:B0:A9:98:80:28:49

Issued By

Common Name (CN)	Thawte Premium Server CA
Organization (O)	Thawte Consulting cc
Organizational Unit (OU)	Certification Services Division

Validity

Issued On	9/25/2008
Expires On	9/25/2010

Fingerprints

SHA1 Fingerprint	B7:A7:89:34:54:5D:C9:6F:41:FD:A9:3E:41:AF:2B:1D:13:C8:CC:AD
MD5 Fingerprint	55:5F:09:17:24:03:F7:80:2B:B6:90:26:3B:0B:E3:3B

Common Name

- Explicit name: www.foo.com
- Wildcard: *.foo.com or www*.foo.com
- Matching rules
  - Firefox 3: * matches anything
  - Internet Explorer 7: * must occur in the leftmost component, does not match '.'
    - *.foo.com matches a.foo.com, but not a.b.foo.com

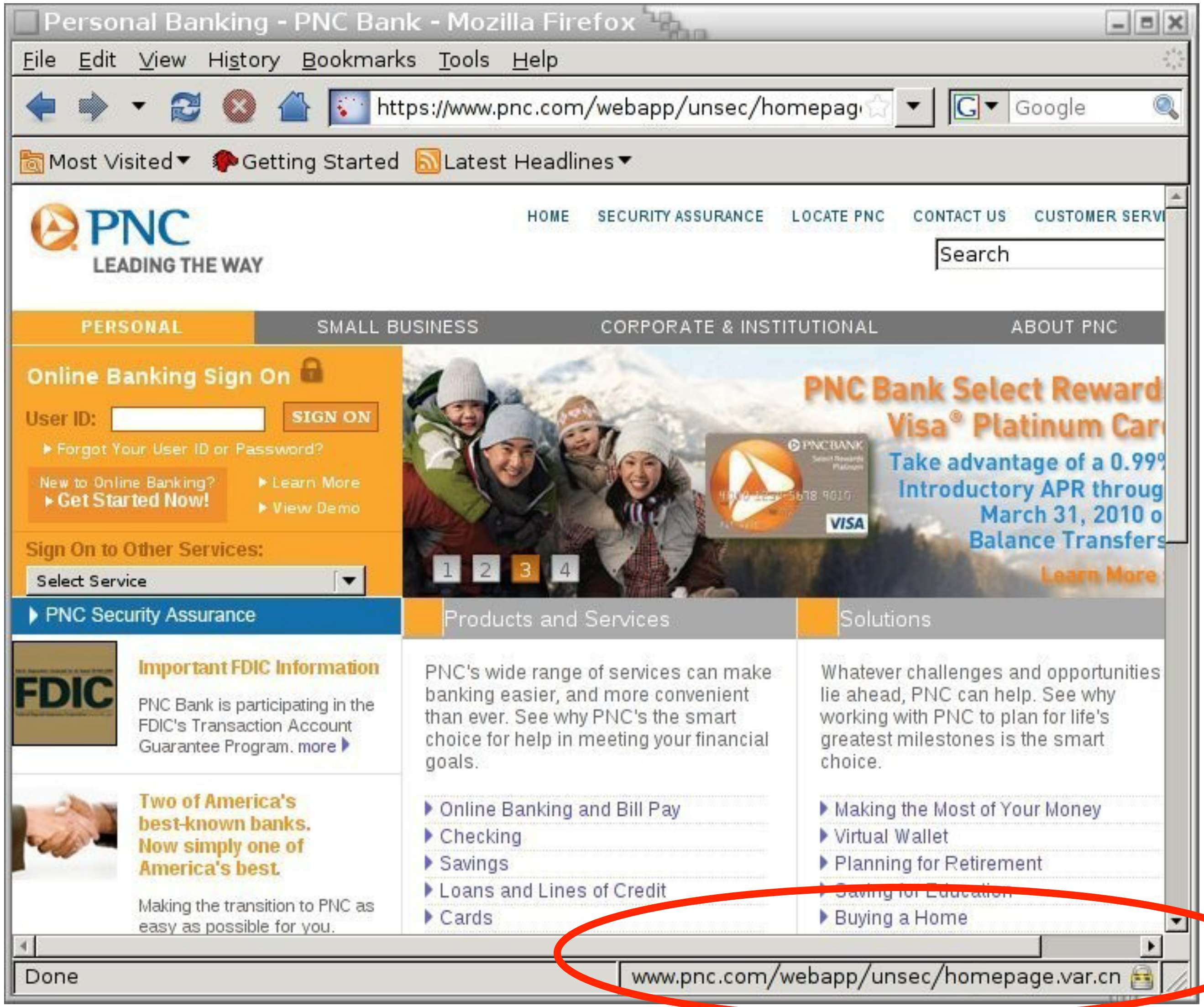
International Domain Names

- Rendered using international character set
- Chinese character set contains characters that look like / ? = .
  - What could go wrong?
- Can buy a certificate for *.foo.cn, create any number of domain names that look like

  www.bank.com/accounts/login.php?q=me.foo.cn
  - What does the user see?
  - *.foo.cn certificate works for all of them!

Example

[Moxie Marlinspike]



Important FDIC Information

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more

Two of America's best-known banks. Now simply one of America's best.

Making the transition to PNC as easy as possible for you.

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- Online Banking and Bill Pay
- Checking
- Savings
- Loans and Lines of Credit
- Cards

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

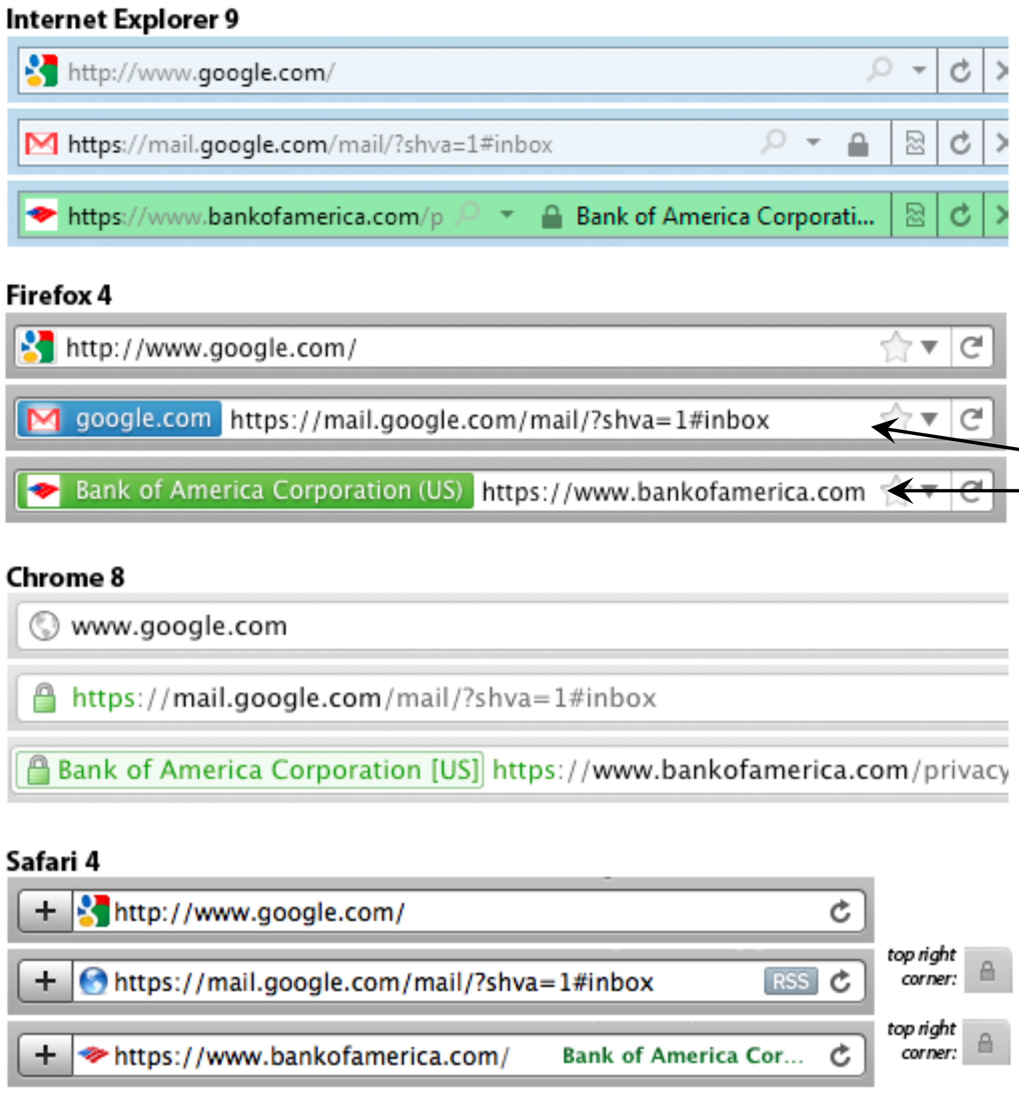
- Making the Most of Your Money
- Virtual Wallet
- Planning for Retirement
- Saving for Education
- Buying a Home

Done

www.pnc.com/webapp/unsec/homepage.var.cn

Meaning of Color

[Schultze]



Internet Explorer 9

http://www.google.com/

https://mail.google.com/mail/?shva=1#inbox

https://www.bankofamerica.com/p Bank of America Corporati...

Firefox 4

http://www.google.com/

google.com https://mail.google.com/mail/?shva=1#inbox

Bank of America Corporation (US) https://www.bankofamerica.com

Chrome 8

www.google.com

https://mail.google.com/mail/?shva=1#inbox

Bank of America Corporation [US] https://www.bankofamerica.com/privacy

Safari 4

http://www.google.com/

https://mail.google.com/mail/?shva=1#inbox RSS

https://www.bankofamerica.com/ Bank of America Cor...

What is the difference?

Domain Validation (DV) certificate

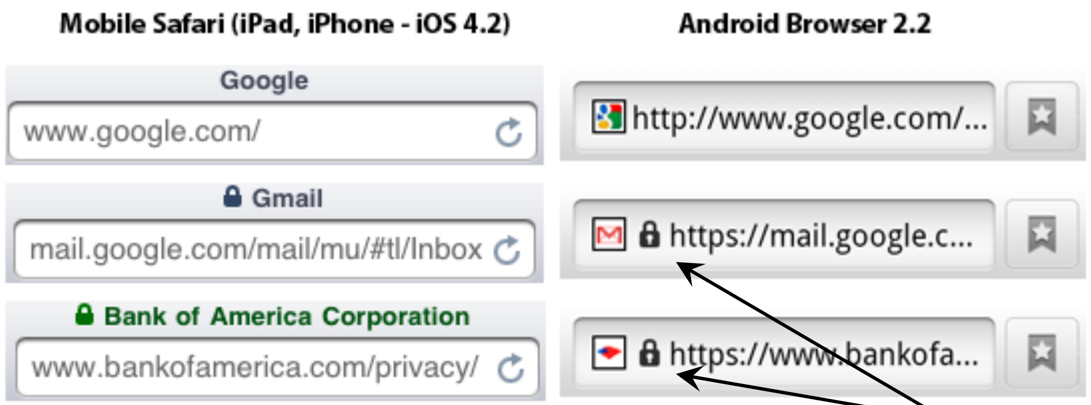
vs.

Extended Validation (EV) certificate

Means what?

Mobile Browsing

[Schultze]


Mobile Safari (iPad, iPhone - iOS 4.2)
Android Browser 2.2
Google
www.google.com/
Gmail
mail.google.com/mail/mu/#tl/Inbox
Bank of America Corporation
www.bankofamerica.com/privacy/
http://www.google.com/...
https://mail.google.c...
https://www.bankofa...

Same lock for DV and EV

Windows Phone 7: same behavior

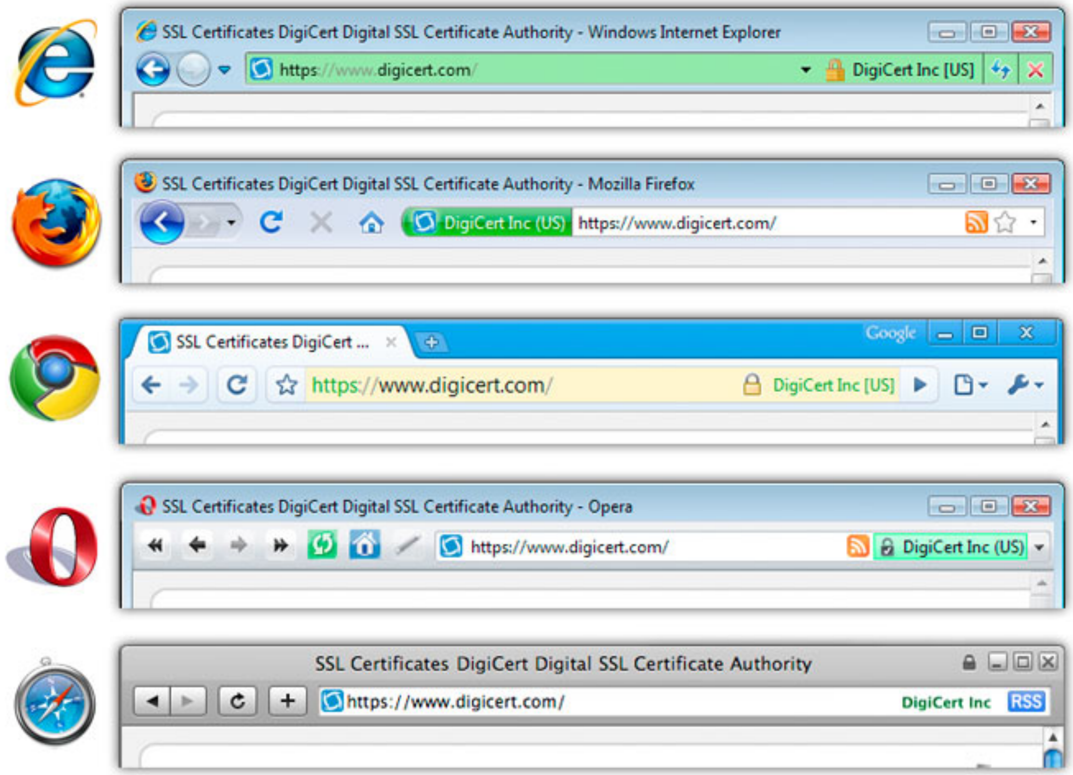
... but only when URL bar present

... landscape mode: no URL bar

http://www.freedom-to-tinker.com/blog/sjs/web-browser-security-user-interfaces-hard-get-right-and-increasingly-inconsistent

Extended Validation (EV) Certificates

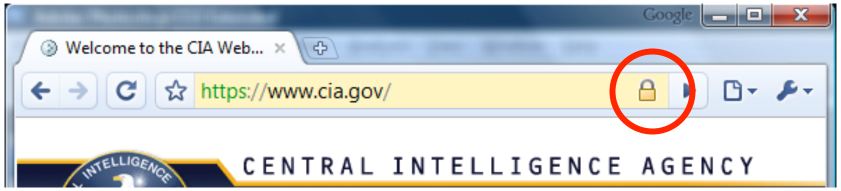
- Certificate request must be approved by a human lawyer at the certificate authority


SSL Certificates DigiCert Digital SSL Certificate Authority - Windows Internet Explorer
https://www.digicert.com/
DigiCert Inc [US]
SSL Certificates DigiCert Digital SSL Certificate Authority - Mozilla Firefox
DigiCert Inc (US)
https://www.digicert.com/
SSL Certificates DigiCert ...
Google
https://www.digicert.com/
DigiCert Inc [US]
SSL Certificates DigiCert Digital SSL Certificate Authority - Opera
https://www.digicert.com/
DigiCert Inc (US)
SSL Certificates DigiCert Digital SSL Certificate Authority
https://www.digicert.com/
DigiCert Inc
RSS

Questions about EV Certificates

- What does EV certificate mean?
- What is the difference between an HTTPS connection that uses a regular certificate and an HTTPS connection that uses an EV certificate?
- If an attacker has somehow obtained a non-EV certificate for bank.com, can he inject a script into https://bank.com content?
  - What is the origin of the script? Can it access or modify content that arrived from actual bank.com via HTTPS?
- What would the browser show – blue or green?

When Should The Lock Be Shown?



- All elements on the page fetched using HTTPS

For all elements:

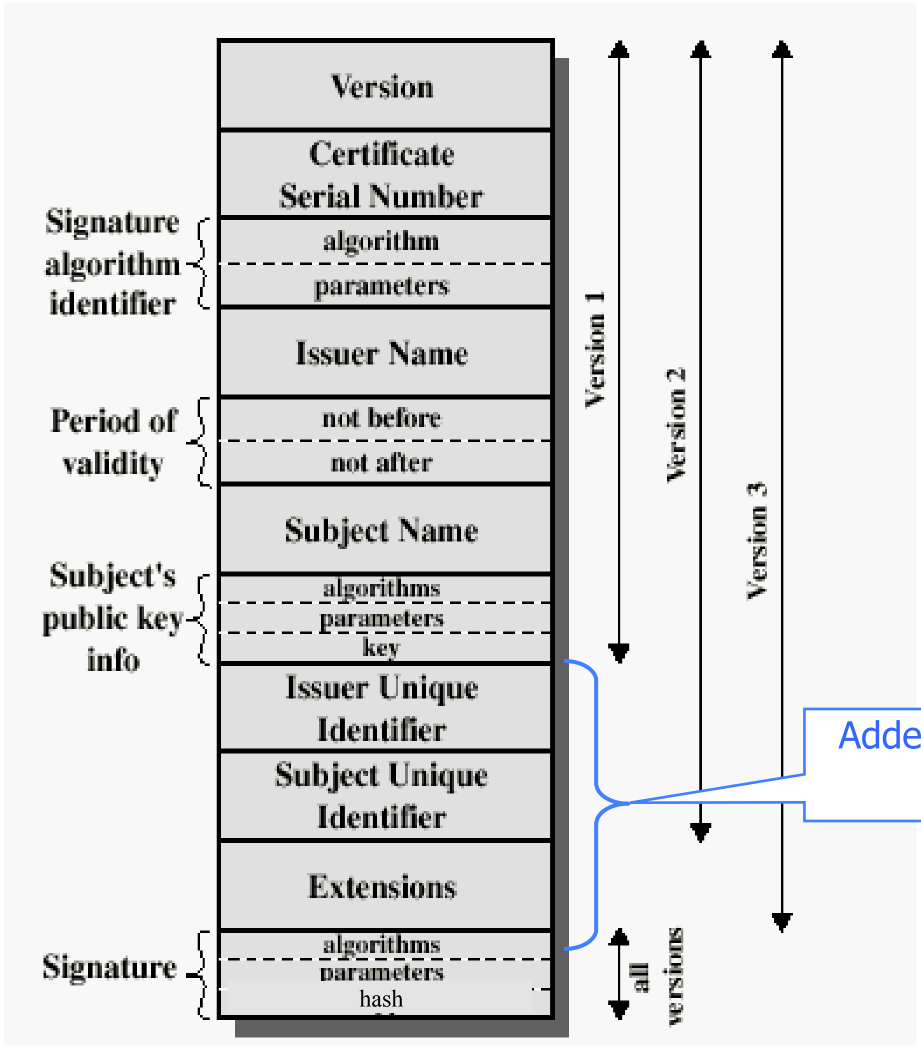
- HTTPS certificate is issued by a certificate authority (CA) trusted by the browser
- HTTPS certificate is valid – means what?
- Common Name in the certificate matches domain name in the URL

X.509 Authentication Service

- Internet standard (1988-2000)
- Specifies certificate format
  - X.509 certificates are used in IPsec and SSL/TLS
- Specifies certificate directory service
  - For retrieving other users' CA-certified public keys
- Specifies a set of authentication protocols
  - For proving identity using public-key signatures
- Can use with any digital signature scheme and hash function, but must hash before signing

Remember MD5?

X.509 Certificate



Added in X.509 versions 2 and 3 to address usability and security problems

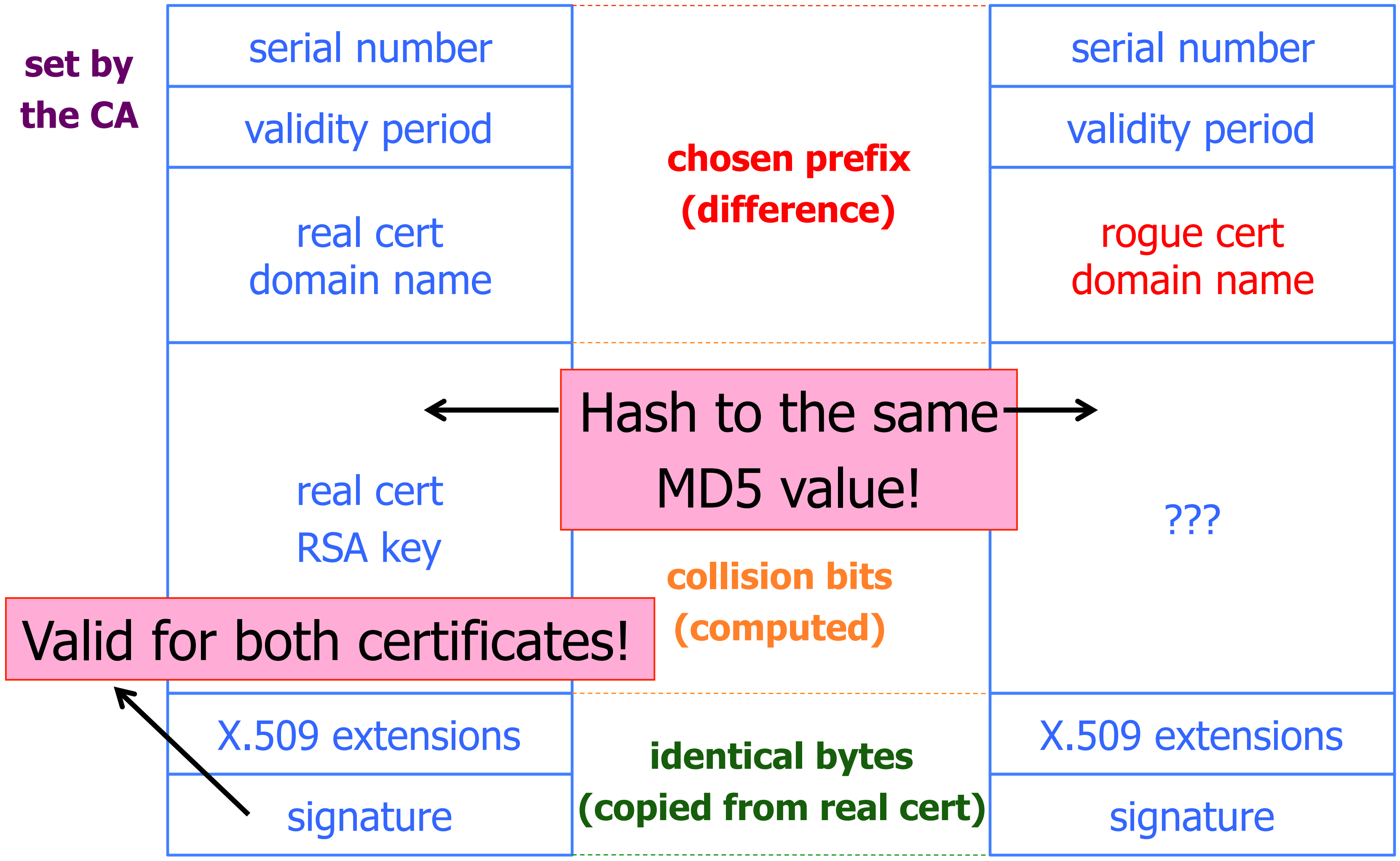
Back in 2008

[Sotirov et al. “Rogue Certificates”]

- Many CAs still used MD5
  - RapidSSL, FreeSSL, TrustCenter, RSA Data Security, Thawte, verisign.co.jp
- Sotirov et al. collected 30,000 website certificates
- 9,000 of them were signed using MD5 hash
- 97% of those were issued by RapidSSL

Colliding Certificates

[Sotirov et al. "Rogue Certificates"]



Generating Collisions

[Sotirov et al. “Rogue Certificates”]

1-2 days on a cluster of 200 PlayStation 3’s

Equivalent to 8000 desktop CPU cores or $20,000 on Amazon EC2

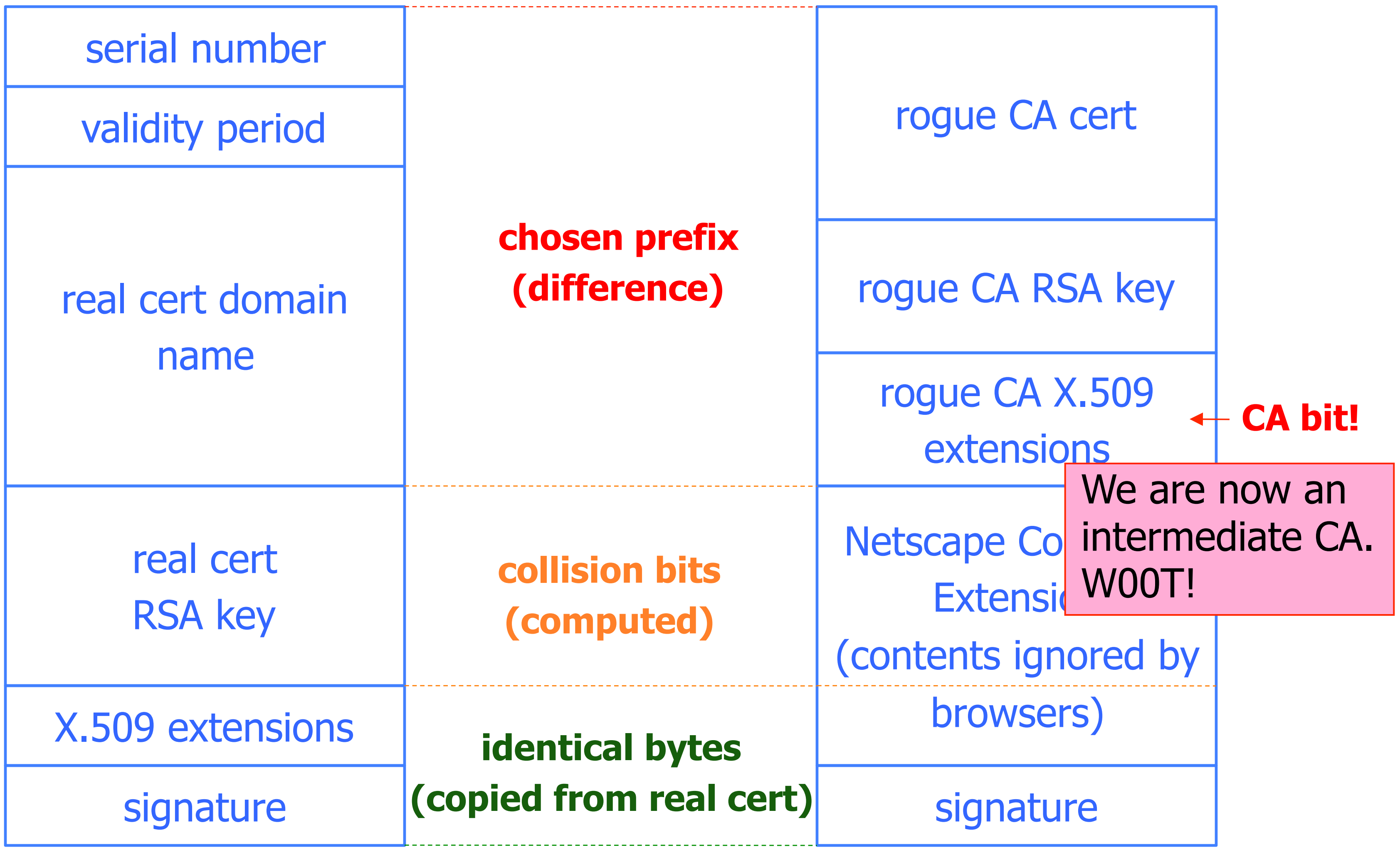
Generating Colliding Certificates

[Sotirov et al. "Rogue Certificates"]

- RapidSSL uses a fully automated system
  - $69 for a certificate, issued in 6 seconds
  - Sequential serial numbers
- Technique for generating colliding certificates
  - Get a certificate with serial number S
  - Predict time T when RapidSSL's counter goes to S+1000
  - Generate the collision part of the certificate
  - Shortly before time T buy enough (non-colliding) certificates to increment the counter to S+999
  - Send colliding request at time T and get serial number S+1000

Creating a Fake Intermediate CA

[Sotirov et al. “Rogue Certificates”]

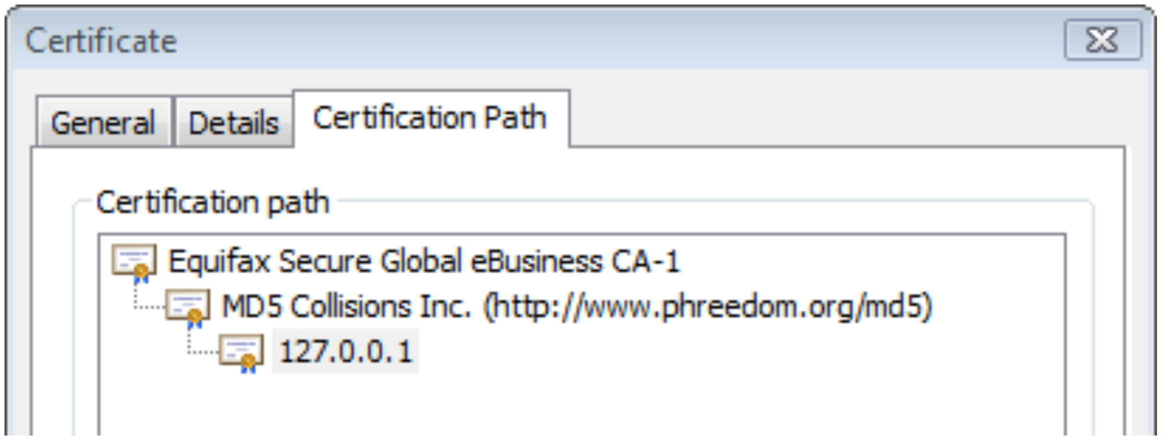


serial number
validity period
real cert domain name
real cert RSA key
X.509 extensions
signature
chosen prefix (difference)
collision bits (computed)
identical bytes (copied from real cert)
rogue CA cert
rogue CA RSA key
rogue CA X.509 extensions
CA bit!
Netscape Co
Extensi
(contents ignored by browsers)
signature
We are now an intermediate CA. W00T!

Result: Perfect Man-in-the-Middle

[Sotirov et al. "Rogue Certificates"]

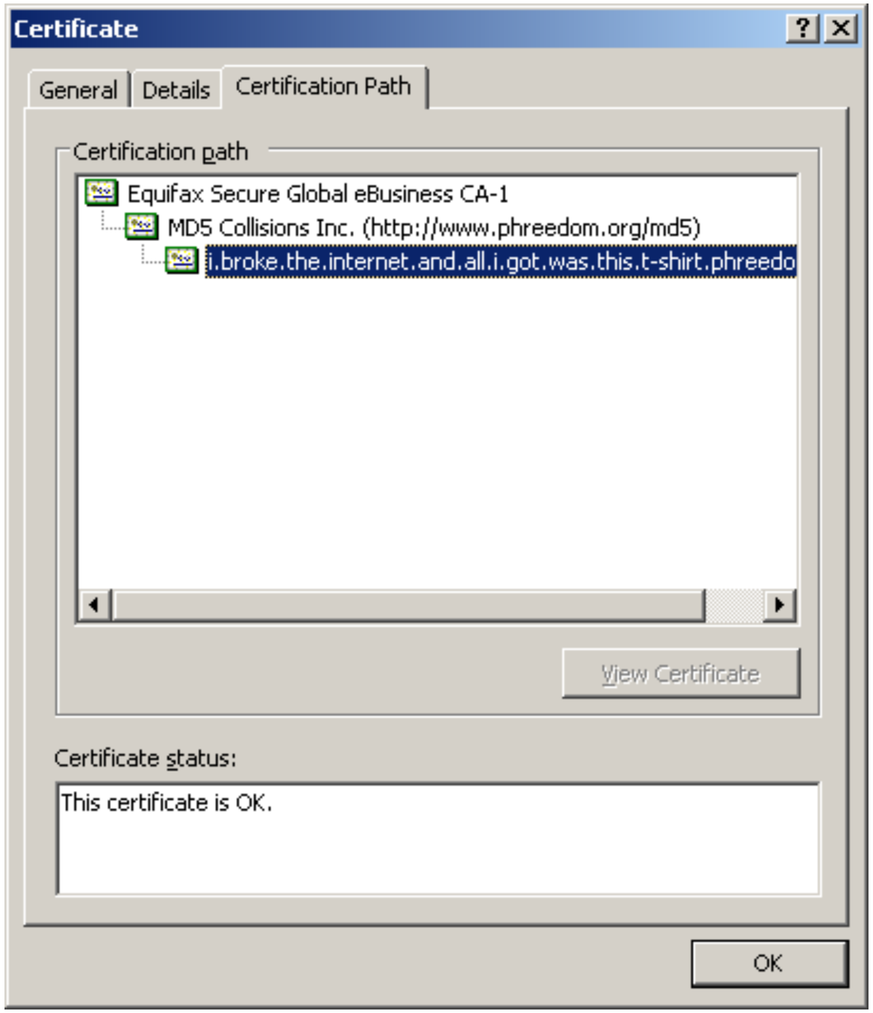
- This is a "skeleton key" certificate: it can issue fully trusted certificates for <u>any</u> site (why?)



Equifax Secure Global eBusiness CA-1
MD5 Collisions Inc. (http://www.phreedom.org/md5)
127.0.0.1

- To take advantage, need a network attack
  - Insecure wireless, DNS poisoning, proxy auto-discovery, hacked routers, etc.

A Rogue Certificate



Certification path

Equifax Secure Global eBusiness CA-1

MD5 Collisions Inc. (http://www.phreedom.org/md5)

i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedo

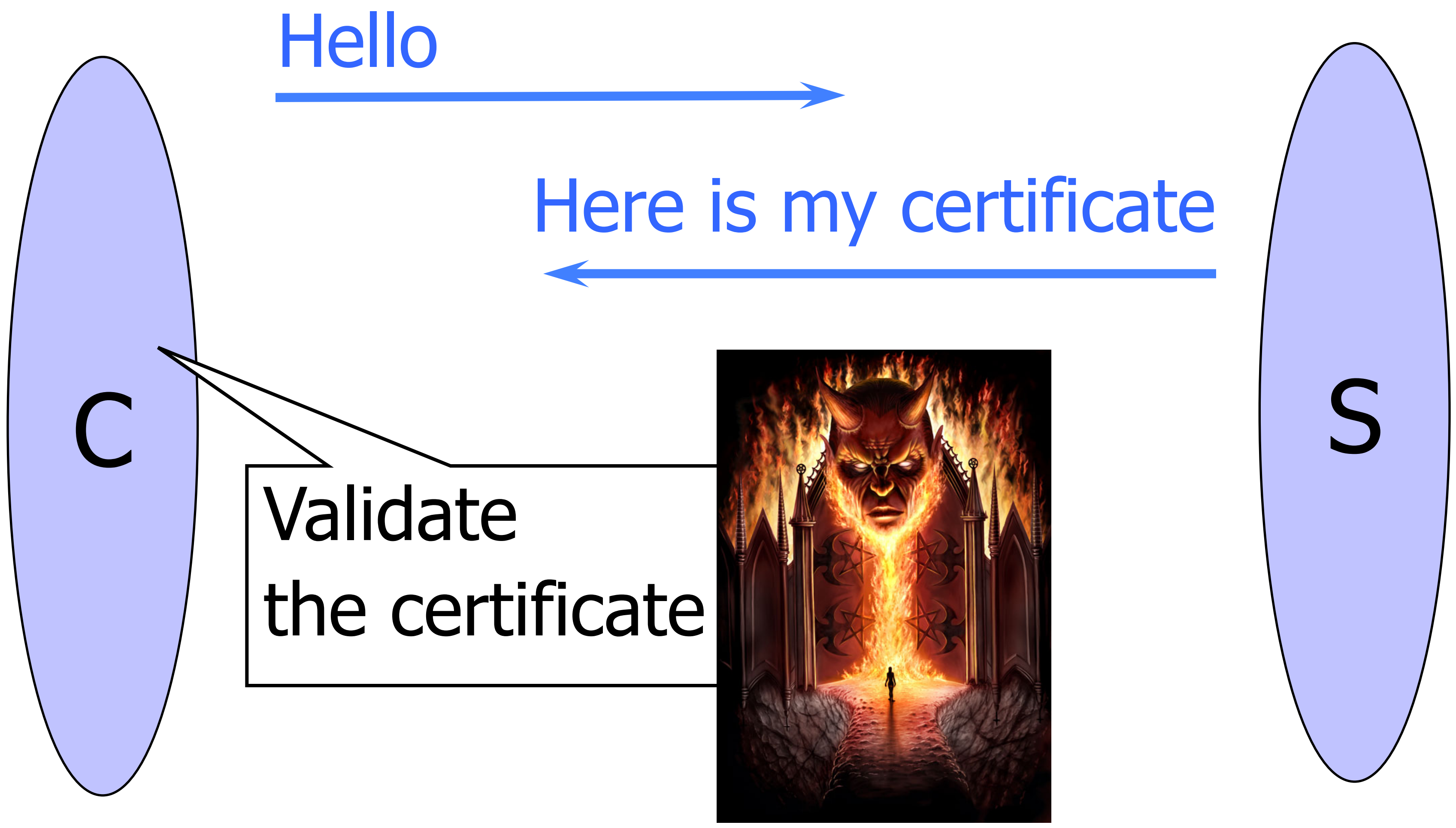
Certificate status:

This certificate is OK.

Remember Flame?

- Cyber-espionage virus (2010-2012)
- Signed with a fake intermediate CA certificate that appears to be issued by Microsoft and thus accepted by any Windows Update service
  - Fake intermediate CA certificate was created using an MD5 chosen-prefix collision against an obscure Microsoft Terminal Server Licensing Service certificate that was enabled for code signing and still used MD5
- MD5 collision technique possibly pre-dates Sotirov et al.' s work
  - Evidence of state-level cryptanalysis?

SSL/TLS Handshake



SSL/TLS Handshake

CHASE

Android app

Hello $\longrightarrow$

I am Chase.com
Here is my certificate $\longleftarrow$

Issued by GoDaddy to
AllYourSSLAreBelongTo.us

Ok!

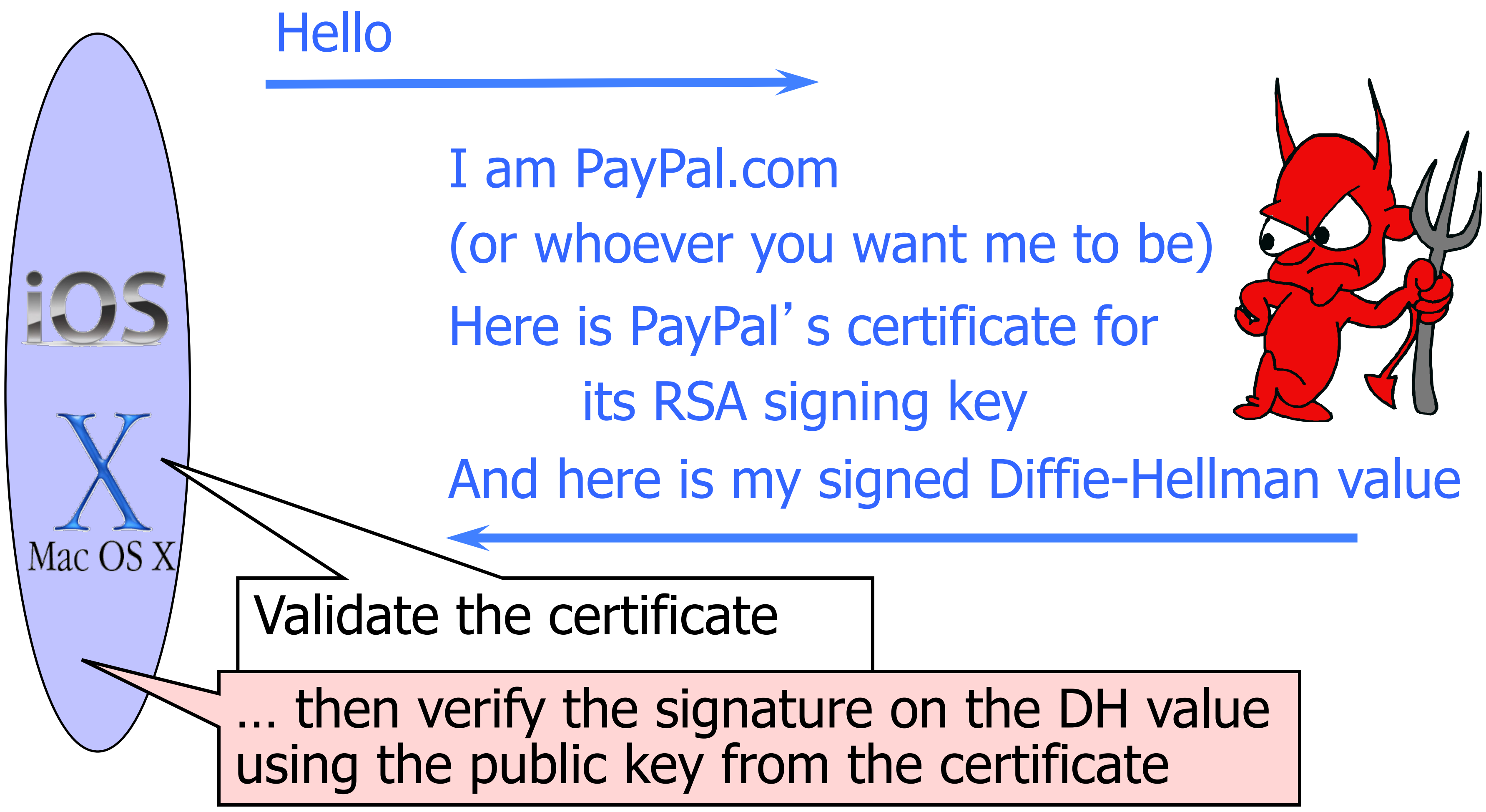
Failing to Check Hostname

"Researchers at the University of Texas at Austin and Stanford University have discovered that poorly designed APIs used in SSL implementations are to blame for vulnerabilities in many critical non-browser software packages. Serious security vulnerabilities were found in programs such as Amazon's EC2 Java library, Amazon's and PayPal's merchant SDKs, Trillian and AIM instant messaging software, popular integrated shopping cart software packages, Chase mobile banking software, and several Android applications and libraries. SSL connections from these programs and many others are vulnerable to a man in the middle attack…"

- Threatpost (Oct 2012)

Major payment processing gateways, client software for cloud computing, integrated e-commerce software, etc.

What Happens After Validation?



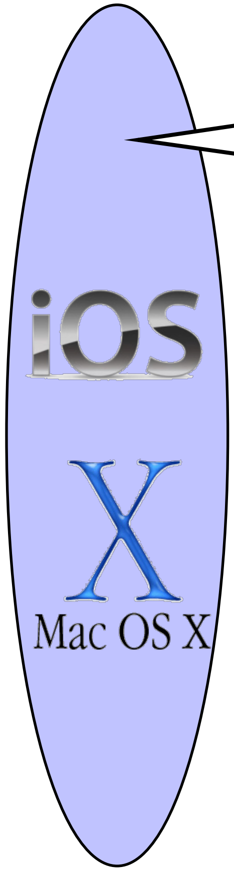
I am PayPal.com
(or whoever you want me to be)
Here is PayPal's certificate for its RSA signing key
And here is my signed Diffie-Hellman value

Validate the certificate

… then verify the signature on the DH value using the public key from the certificate

Goto Fail

Here is PayPal's certificate
And here is my signed Diffie-Hellman value



... verify the signature on the DH value using the public key from the certificate

```
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;   ???
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail; …
err = sslRawVerify(...);   Signature is verified here
…
fail: … return err …
```

Complete Fail Against MITM

- Discovered in February 2014
- All OS X and iOS software vulnerable to man-in-the-middle attacks
  - Broken TLS implementation provides <u>no</u> protection against the very attack it was supposed to prevent
- What does this tell you about quality control for security-critical software?

Certificate Revocation

- Revocation is <u>very</u> important
- Many valid reasons to revoke a certificate
    - Private key corresponding to the certified public key has been compromised
    - User stopped paying his certification fee to the CA and the CA no longer wishes to certify him
    - CA’s certificate has been compromised!
- Expiration is a form of revocation, too
    - Many deployed systems don’t bother with revocation
    - Re-issuance of certificates is a big revenue source for certificate authorities

Certificate Revocation Mechanisms

- Online revocation service
  - When a certificate is presented, recipient goes to a special online service to verify whether it is still valid
- Certificate revocation list (CRL)
  - CA periodically issues a signed list of revoked certificates
  - Can issue a “delta CRL” containing only updates

Q: Does revocation protect against forged certificates?