

CS 408

Cryptography & Internet Security

Lecture 23:

Secure Communication after Key Setup

SSL

What Happens after Key Setup?

- Assume that Alice and Bob have session keys for encryption and authentication.
- What next? How to protect communication?
 - Differentiate between encryption and authentication
- **Where in the protocol stack to put security?**
- Assume insecure network and powerful attacker (can eavesdrop, inject, modify etc.)

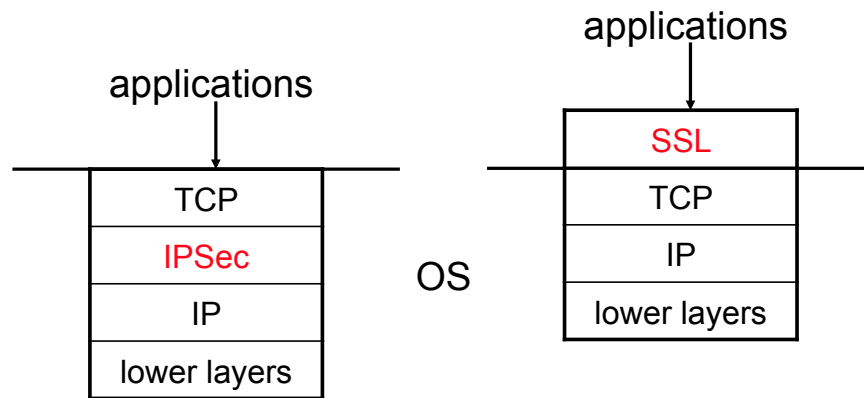
Where to Put Security?

- Application layer?
- Transport layer?
- Network layer?
- Link layer?

Security at the Link Layer?

- When to use?
 - High volume, direct connection between two nodes
 - Vulnerable link due to the nature of the physical layer
- Example:
 - A wireless home network
 - WEP (every LL frame is encrypted and authenticated)
- Not appropriate for devices that do not have a direct connection
 - Intermediate nodes may need routing information (IP address)

Security at the Network or Transport Layer?



- Network layer (IPsec) (“layer 3”)
 - Requires modification of the TCP/IP stack
 - Does not require changes in the applications
- Transport layer (SSL) (“layer 4”)
 - The OS does not need to be modified
 - Requires modification of the applications

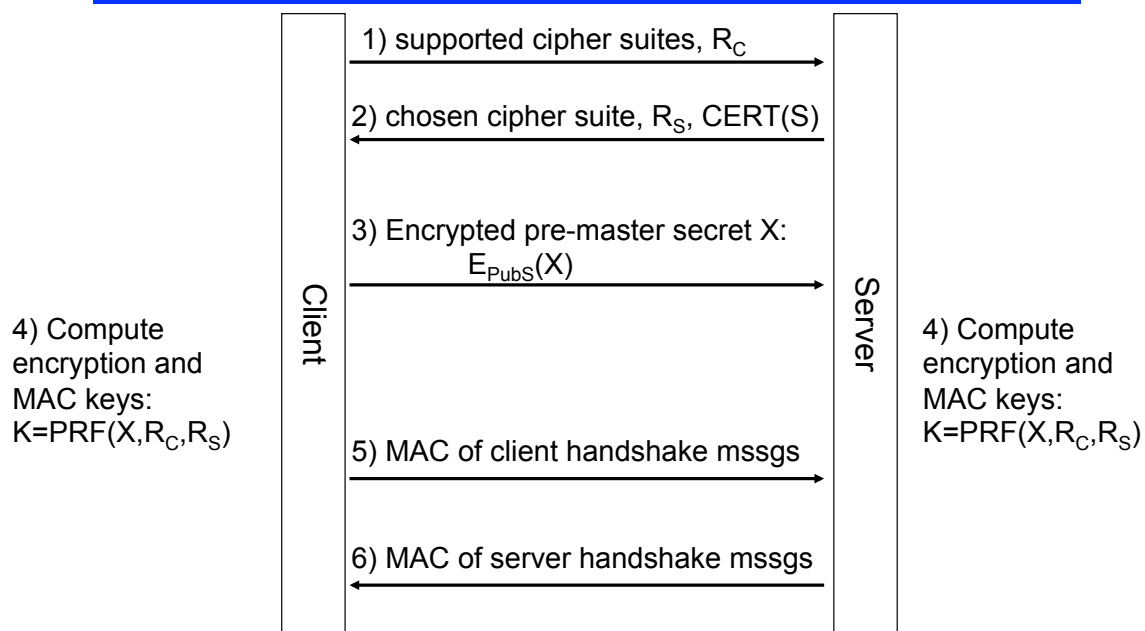
Security at the Application Layer?

- When to use?
 - When there are very specific security needs required by an application
 - When no end-to-end transport connection exists between two parties
- Example: e-mail
 - Users send emails to other users in different geographic locations, using diverse platforms
 - People may not trust the sys admin
 - PGP (Pretty Good Privacy)

Secure Sockets Layer (SSL)

- Goals for secure communication between a client and a server
 - Provide confidentiality
 - Provide (mutual) authentication
- Communication is divided into two phases
 - Handshake
 - client and server agree on what set of cryptographic algorithms to use
 - authenticates the server
 - establishes keys which will be used for the data transfer
 - Secure data transfer
 - Data is transferred (authenticated and encrypted using the keys established during handshake)

Basic Handshake Protocol

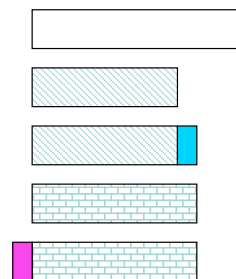


Basic Handshake Protocol

- Client uses https:// instead of http:// (this indicates to server to use port 443 instead of 80)
- X is a random value chosen by the client
- Only the server authenticates itself
 - Client authentication is rarely achieved through SSL
- Messages 5) and 6) protect tampering of the (unprotected) messages 1) and 2)
- The derived key material K includes different keys for encryption and authentication
 - $\text{PRF}(X, R_C, R_S) = (K_{S1}, K_{S2}, K_{C1}, K_{C2})$
 - Server encryption key K_{S1} , server MAC key K_{S2}
 - Client encryption key K_{C1} , client MAC key K_{C2}

SSL Data Transfer

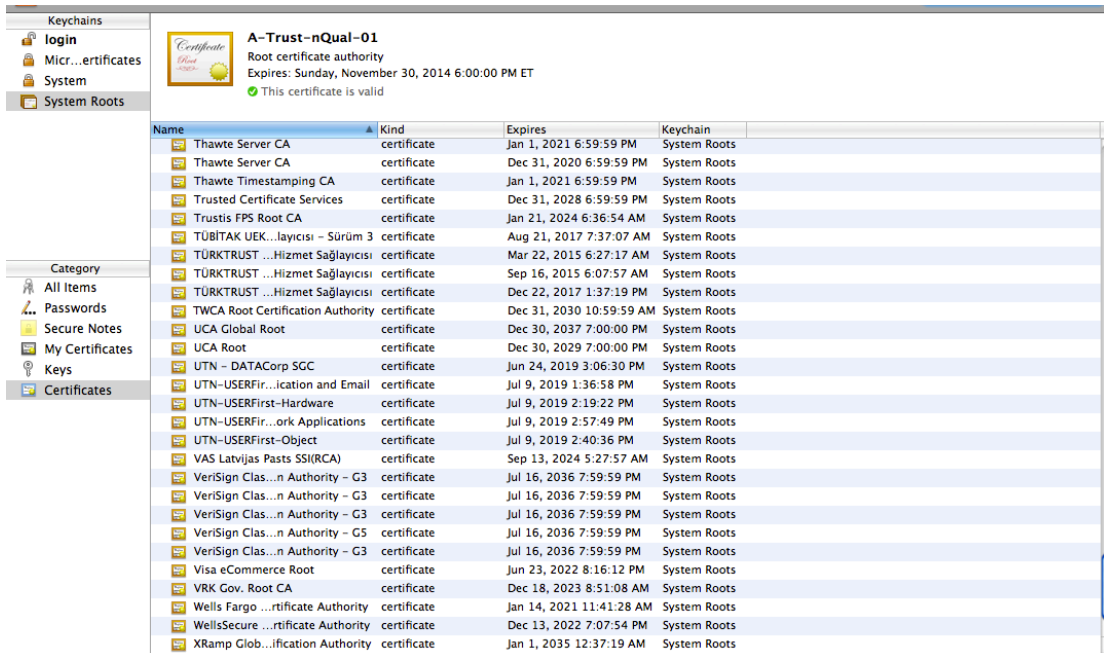
- Data is broken into *records*
- Each record is:
 - Compressed
 - MAC-ed
 - Encrypted
 - Pre-pended with an SSL header



Early Versions of SSL

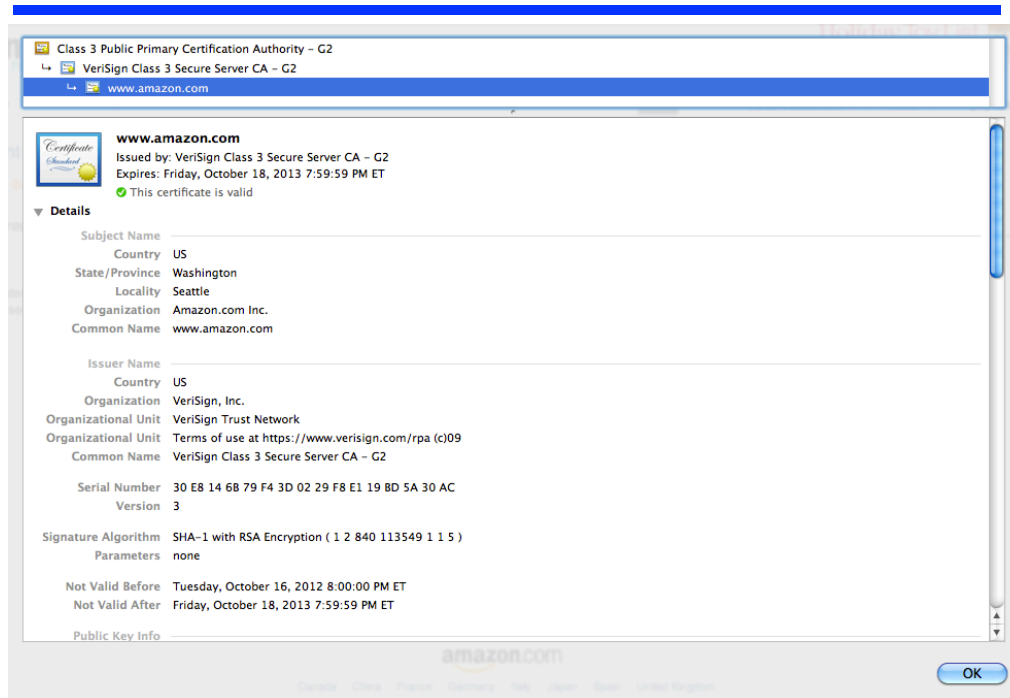
- The presented protocol is SSL v3
- SSL v2 was flawed:
 - MITM attack (messages 5) and 6) were not present; attacker could tamper with messages 1) and 2) and cause a **downgrade** attack to a weak ciphersuite
 - Uses identical keys for both encryption and authentication
- SSL v2 is disabled by default in modern browsers

Certificates in SSL – root certificates



Name	Kind	Expires	Keychain
Thawte Server CA	certificate	Jan 1, 2021 6:59:59 PM	System Roots
Thawte Server CA	certificate	Dec 31, 2020 6:59:59 PM	System Roots
Thawte Timestamping CA	certificate	Jan 1, 2021 6:59:59 PM	System Roots
Trusted Certificate Services	certificate	Dec 31, 2028 6:59:59 PM	System Roots
Trustis FPS Root CA	certificate	Jan 21, 2024 6:36:54 AM	System Roots
TÜBITAK UEK...layıcısı - Sürüm 3	certificate	Aug 21, 2017 7:37:07 AM	System Roots
TÜRKTRUST ...Hizmet Sağlayıcısı	certificate	Mar 22, 2015 6:27:17 AM	System Roots
TÜRKTRUST ...Hizmet Sağlayıcısı	certificate	Sep 16, 2015 6:07:57 AM	System Roots
TÜRKTRUST ...Hizmet Sağlayıcısı	certificate	Dec 22, 2017 1:37:19 PM	System Roots
UCA Global Root	certificate	Dec 31, 2030 10:59:59 AM	System Roots
UCA Root	certificate	Dec 30, 2037 7:00:00 PM	System Roots
UTN - DATACorp SGC	certificate	Dec 30, 2029 7:00:00 PM	System Roots
UTN - USERFir...ication and Email	certificate	Jun 24, 2019 3:06:30 PM	System Roots
UTN - USERFir...ork Applications	certificate	Jul 9, 2019 1:36:58 PM	System Roots
UTN - USERFir...ork Applications	certificate	Jul 9, 2019 2:19:22 PM	System Roots
UTN - USERFir...ork Applications	certificate	Jul 9, 2019 2:57:49 PM	System Roots
UTN - USERFir...ork Applications	certificate	Jul 9, 2019 2:40:36 PM	System Roots
VAS Latvias Pastis SSI(RCA)	certificate	Sep 13, 2024 5:27:57 AM	System Roots
VeriSign Clas...n Authority - G3	certificate	Jul 16, 2036 7:59:59 PM	System Roots
VeriSign Clas...n Authority - G3	certificate	Jul 16, 2036 7:59:59 PM	System Roots
VeriSign Clas...n Authority - G3	certificate	Jul 16, 2036 7:59:59 PM	System Roots
VeriSign Clas...n Authority - G5	certificate	Jul 16, 2036 7:59:59 PM	System Roots
VeriSign Clas...n Authority - G3	certificate	Jul 16, 2036 7:59:59 PM	System Roots
Visa eCommerce Root	certificate	Jun 23, 2022 8:16:12 PM	System Roots
VRK Gov. Root CA	certificate	Dec 18, 2023 8:51:08 AM	System Roots
Wells Fargo ...rtificate Authority	certificate	Jan 14, 2021 11:41:28 AM	System Roots
WellsSecure ...rtificate Authority	certificate	Dec 13, 2022 7:07:54 PM	System Roots
XRamp Glob...ification Authority	certificate	Jan 1, 2035 12:37:19 AM	System Roots

Certificates in SSL – website certificates

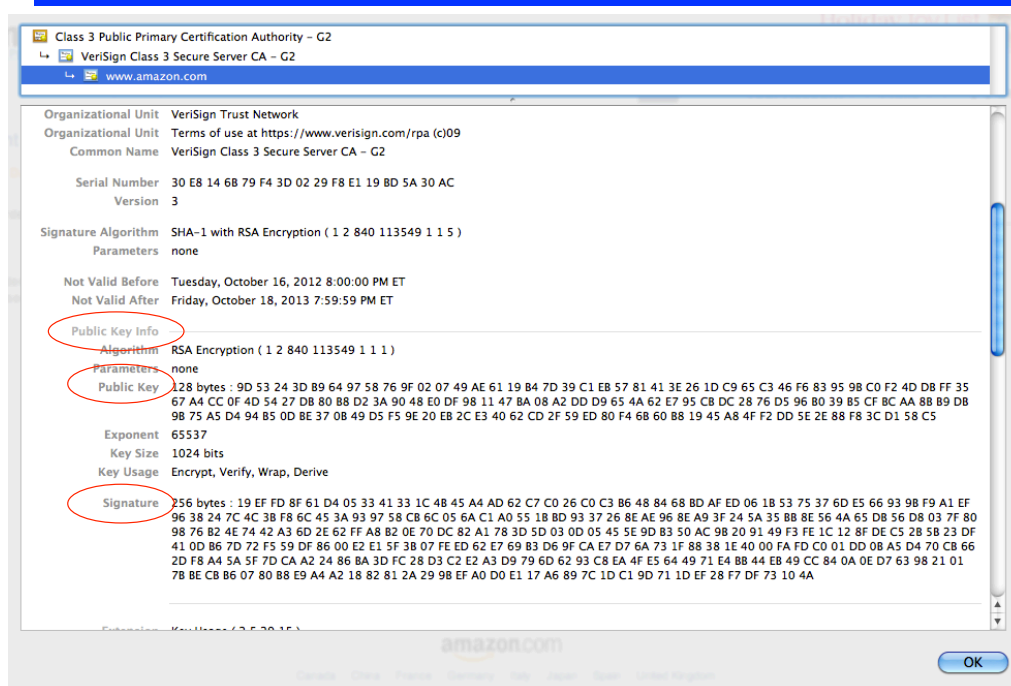


CS 408

Lecture 23 / Spring 2015

13

Certificates in SSL – website certificates

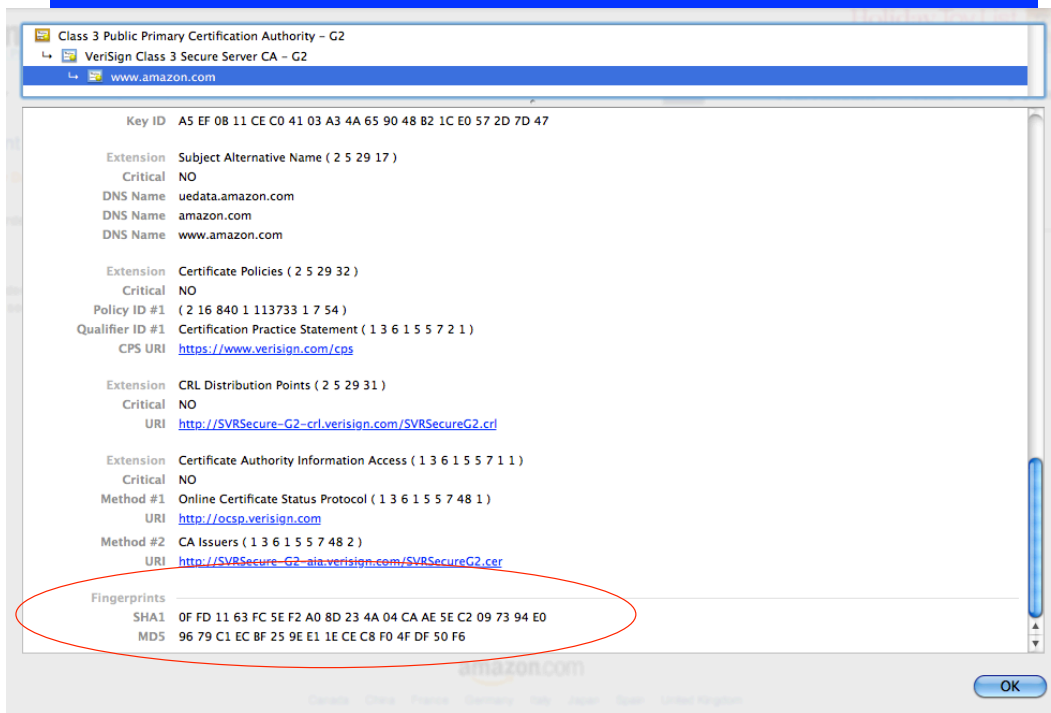


CS 408

Lecture 23 / Spring 2015

14

Certificates in SSL – website certificates



CS 408

Lecture 23 / Spring 2015

15

How to Get an SSL Certificate for a Domain?

- Pay money
 - Verisign (\$350)
 - Thawte (\$150)
- Prove that your request comes from the legal holder of the domain
 - Letter from company
 - Notarized document
- CA may check
 - Existence of business
 - Ownership of the domain name
 - Employment status

CS 408

Lecture 23 / Spring 2015

16

SSL Pitfalls

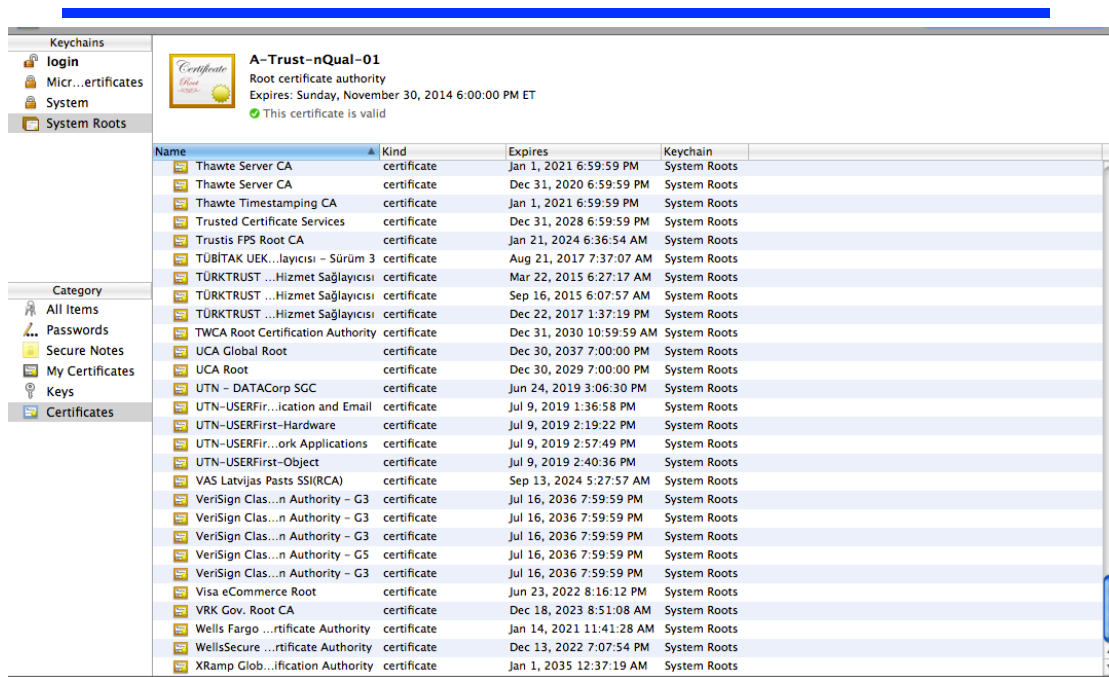
- Presence of SSL is indicated by a lock at the bottom of the browser window
- What does this mean?
 - Browser is engaging in a secure session with *some* server
 - Burden is on the user to check information about the certificate
 - There is no guarantee that the server that serves the certificate is the entity in the certificate
 - Users usually ignore browser warnings

SSL Pitfalls

- The PayPal.com scam
 - Phishing attempt in 2000
 - Using I (uppercase i) instead of l (lowercase l)
 - Attacker registered paypal.com domain and obtained a certificate for it
 - User is tricked into revealing PayPal account credentials
- SSL is not a magical solution for Web security
 - Provides a secure pipe between user-server, but the user is responsible to verify identity of the server

SSL Pitfalls

- Users don't check certificates
 - Users ignore warnings about invalid or expired certificates
 - Many users don't even know what certificates mean!
- Certificates can be easily obtained
- Browsers contain too many CAs
- Performance
 - Some sites turn it off during peak times



Certificate Authorities: are they trustworthy?

- In general, yes, for all practical purposes
- However, they are not immune to attacks
 - In August 2011 a Dutch CA (DigiNotar) was hacked and fraudulent digital certificates had been issued for *.google.com, *.microsoft.com, *.windowsupdate.com, www.update.microsoft.com, etc.
 - Man-in-the-middle attack becomes possible
 - Attacker sits in between client and server and can listen (and potentially tamper with) the communication
 - How was this addressed?
 - Web browsers needed to update their CA list (remove DigiNotar as a trusted CA)
 - Users can also manually remove a trusted CA from the browser