# **Trust Infrastructure of SSL**

#### BİL 448/548 Internet Security Protocols Ali Aydın Selçuk

# SSL/TLS

- The main workhorse of secure Internet communication.
- Everyday, billions of web packets (HTTPS) are encrypted by SSL/TLS.
- Not only web pages: VPN tunneling, electronic banking, cloud services, ... all rely on SSL to secure their communications.

# Success of SSL

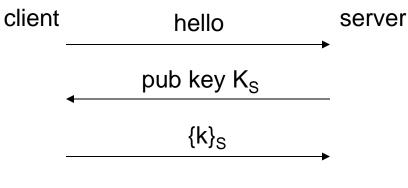
- Brought cryptography to the service of the masses
- Until SSL and spread of Internet, cryptography saw very limited use by common people.
- In the first 20 years of PKC (1976-96), the technology had a very limited penetration.
- This all changed in the second half of the 1990s with SSL.

# Success of SSL

- Trust infrastructure has an autonomous and selfgoverning structure, consisting of
  - browser / OS vendors
  - audit firms and standards bodies
  - certificate authorities
  - SSL servers
- Has been remarkably successful, especially compared to previous efforts such as PEM to secure Internet communications.

# A Simple Key Exchange Protocol

#### ~ SSL key exchange protocol:



k is the session key

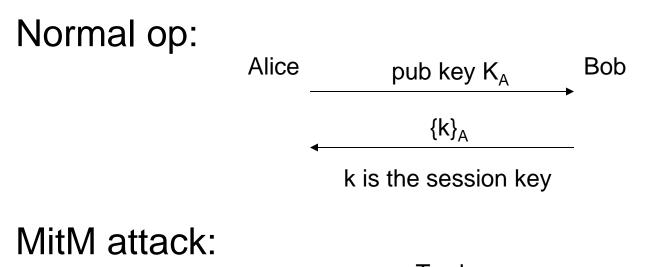
#### Active Attacks & Certificates

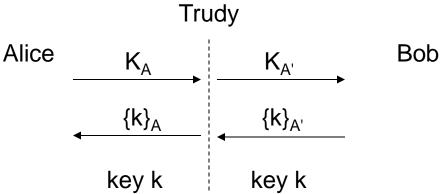
- Simple public key encryption solves the key distribution problem against passive attackers (i.e., an attacker that just eavesdrops).
- Active attackers can send a fake public key & become a "man in the middle" (MitM).

Notation:

- $[M]_X$ : message M signed with the prv. key of X
- $\{M\}_X$ : message M enc. with the pub. key of X

#### MitM Attack





SSL Trust

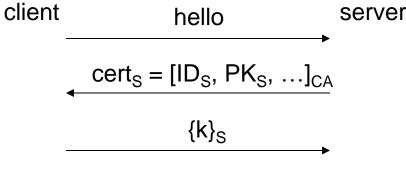
#### Certificates

- These MitM attacks are possible because a receiver cannot distinguish a fake public key from the real one.
- Certificates: IDs and public keys are signed by a trusted authority ("certification authority").

• E.g., 
$$cert_A = [ID_A, PK_A, exp.date, ...]_{CA}$$

# Certified Encrypted Key Exchange

~ SSL key exchange protocol:



k is the session key

# **Certification Authorities**

- CAs' public key should be distributed in a trusted way to all the parties in the system in advance.
- In SSL, root CAs are approved by the browser (or the OS) makers, and distributed with the browser/OS code.
- CAs must satisfy certain criteria for this:
  - <u>https://wiki.mozilla.org/CA:How\_to\_apply</u>
  - <u>http://www.chromium.org/Home/chromium-</u> security/root-ca-policy
  - <u>http://technet.microsoft.com/en-us/library/cc751157.aspx</u>

# **Certification Authorities**

- Browser makers require CA firms to be audited and accredited according to some standards:
  - WebTrust
  - ETSI TS 101/102
  - ISO 21188:2006
- Public key infrastructure of SSL:
  - Oligarchy model: A number of trusted root CAs,
  - which issue certificates to intermediate CAs, or to end users (SSL servers)

Tools > Internet options > Content > Certificates

General	Security	Privacy	Content	Connections	Programs	Advanced
Parenta	al Controls					
Qo	Contro	0.0000000000000000000000000000000000000	ernet conte	ent that can	Parental	Controls
Conten	t Advisor Rating	s help yo	u control 1	the Internet co	ontent that c	an be
Conten	Rating		computer.			an be ttings
Conten	Rating viewe		computer.			
ę	Rating viewed	d on this	computer.		Se	ttings

#### • Trusted root CAs:

enness berbeset	All>			
Frusted Root Certification	on Authorities Trustee	d Publishers	Untrusted Publishers	
Issued To	Issued By	Expirati	Friendly Name	*
Microsoft Root C NO LIABILITY A StartCom Certifi Thawte Premiu Thawte Timesta UBITAK UEKAE	Microsoft Root Aut Microsoft Root Cer NO LIABILITY ACC StartCom Certifica Thawte Premium Thawte Timestam TÜBİTAK UEKAE K UTN-USERFirst-Ob	10/05/2 08/01/2 17/09/2 01/01/2 01/01/2 21/08/2	Microsoft Roo VeriSign Time StartCom Cer thawte Thawte Time KamuSM	III
VeriSign Class 3	VeriSign Class 3 P VeriSign Commer	17/07/2	VeriSign	-
Import Expo	rt		ſ	Advanced

• E.g., VeriSign root certificate:

Seneral	eral Details Certification Path					
Show	ww <ali></ali>					
Field		Value		*		
Va	lid from lid to bject	08 November 2006 02:00 17 July 2036 01:59:59 VeriSign Class 3 Public Pr				
📕 Public key		RSA (2048 Bits) 30 5f a1 5d a0 5b 30 59		Ш		
Elegatype Elegation Subject Key Identifier Elegation Subject Key Identifier Elegation Subject Key Usage		7f d3 65 a7 c2 dd ec bb f Subject Type=CA, Path L Certificate Signing, Off-lin				

#### • Untrusted / revoked certificates:

ntended purpose:	<all></all>					
Trusted Root Certific	ation Authoritie	s Trusted	Publishers	Untrusted Publis	hers	
Issued To	Issued By		Expirati	Friendly Name		*
DigiNotar Root	CA Entrust.net	Secure	14/08/2	Untrusted		-
DigiNotar Root	C DigiNotar R	oot CA	03/07/2	Untrusted		
🛱 DigiNotar Servic	Entrust.net	Secure	26/08/2	Untrusted		
🛱 Digisign Server	I Entrust.net	Certific	16/07/2	Untrusted		
Digisign Server	I GTE Cyber	Trust Gl	17/07/2	Untrusted		Ħ
🗔 global trustee	UTN-USERI	First-Ha	15/03/2	Fraudulent		
🗔 login.live.com	UTN-USERI	First-Ha	15/03/2	Fraudulent		
login.skype.com	UTN-USERI	First-Ha	15/03/2	Fraudulent		
login.yahoo.con	n UTN-USERI	First-Ha	15/03/2	Fraudulent		
login.vahoo.con	n UTN-USERI	First-Ha	15/03/2	Fraudulent		
Import	xport	Remove	]		Adva	anced

## **Certificates & Validation**

- Valid SSL/TLS certificates are issued to web servers by root or intermediate CAs.
  - E.g., Google's certificate: GeoTrust (root) →
    Google Internet Authority → accounts.google.com
- Client (browser) authenticates this chain of certificates beginning from the root CA.

http://en.wikipedia.org/wiki/Certification\_path\_validation \_algorithm

# **Example Client Certificate**

• E.g., gmail.com (or, accounts.google.com)

⇒ C	Attps://accou	nts.google.com/Se	erviceLogin?service=mail8
ow to B	accounts.google. Identity verified	com	×
	Permissions	Connection	
		of this website has b Google Internet Authon Information	25
	- 33 집중 집안 이번 이상 읽고 7 위험	tion to ogle.com is encrypte encryption.	ed
	The connect	ion uses TLS 1.1.	Download on th

# **Example Client Certificate**

• E.g., gmail.com (or, accounts.google.com)

General	Details	Certification Path	
Certifi	cation pa	ath	
	eoTrust		
	Google	e Internet Authority counts.google.com	

# **Example Client Certificate**

• Example Client Certificate

eneral	Details Certification	Path			
Show	Show <a>All&gt;</a>				
Field		Value			
Issuer		Google Internet Authority,			
Valid from		24 April 2013 17:06:00			
Valid to		30 December 2013 17:06	-		
📕 Subject		accounts.google.com, Go	III		
Public key		RSA (1024 Bits)			
En	hanced Key Usage	Server Authentication (1			
🐻 Subject Key Identifier		83 37 16 75 f6 d7 e1 d1 f			
a Au	thority Key Identifier	KeyID=bf c0 30 eb f5 43			
<u> </u>			1846		

# **SSL/TLS in Practice**

#### SSL/TLS:

- A reasonably secure protocol
- with a reasonable trust model
- and commercially viable operation

#### What may go wrong?

- "Man in the browser" attacks
- Cert. validation software may get it wrong
- Compromised CAs, fake certificates
- and more...