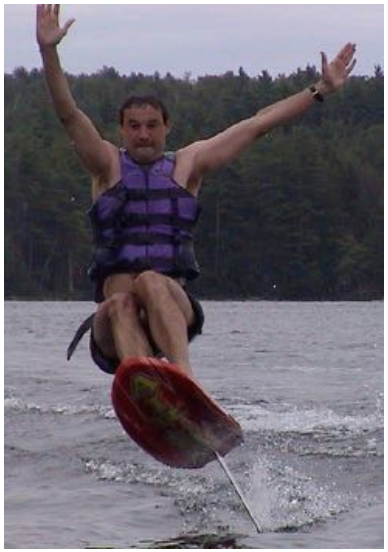
EECS 388
Introduction to Computer Security

HTTPS

October 3, 2017

Professor Fu

My Background


+

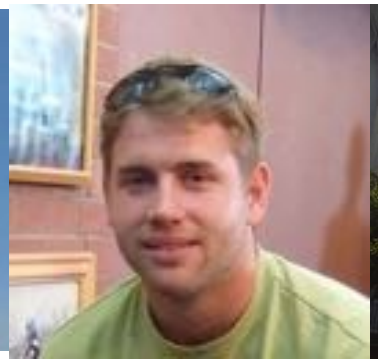
@

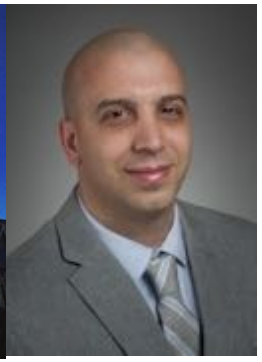
MIT CSAIL

⇒



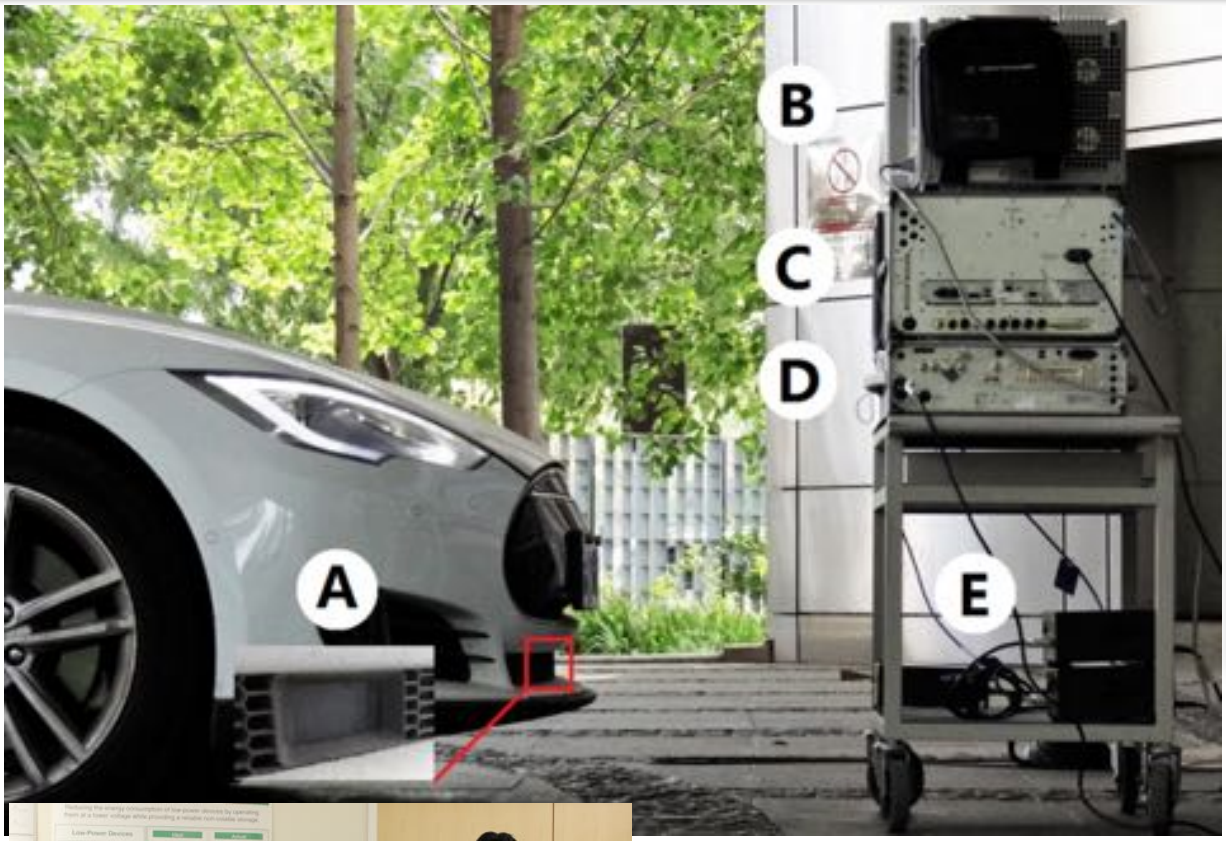






SPQR.eecs.umich.edu

SPQR Lab: Embedded Security



ANDY GREENBERG SECURITY 08.04.16 08:00 AM

HACKERS FOOL TESLA S'S AUTOPILOT TO HIDE AND SPOOF OBSTACLES

GILAI SHEN/BLOOMBERG/GETTY IMAGES

It's Possible to Hack a Phone With Sound Waves, Researchers Show

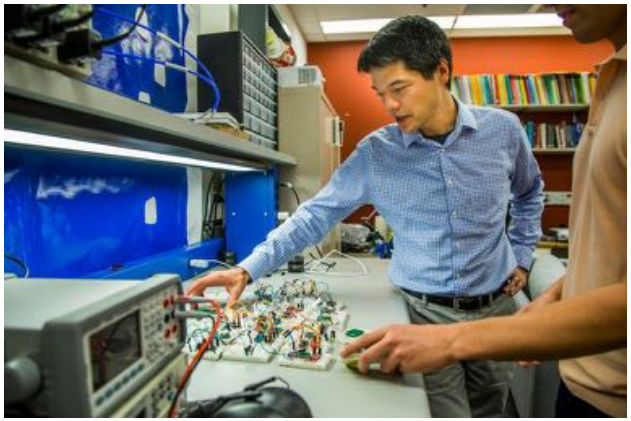
By JOHN MARKOFF MARCH 14, 2017

The New York Times

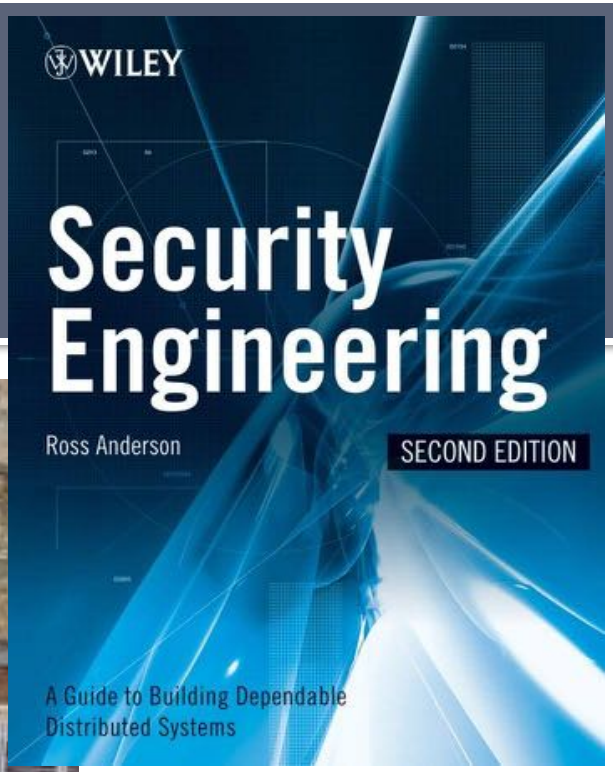
Of Fact, Fiction and Cheney's Defibrillator

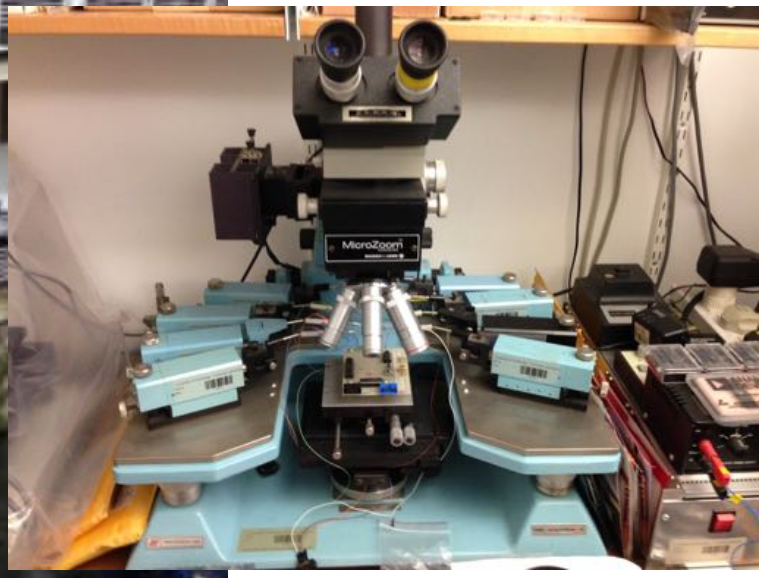
By GINA KOLATA
Published: October 27, 2013

In a chilling episode of "Homeland" last year, a terrorist killed the vice president with a fiendishly clever weapon: a remote-control device that attacked the computerized defibrillator implanted in his chest.

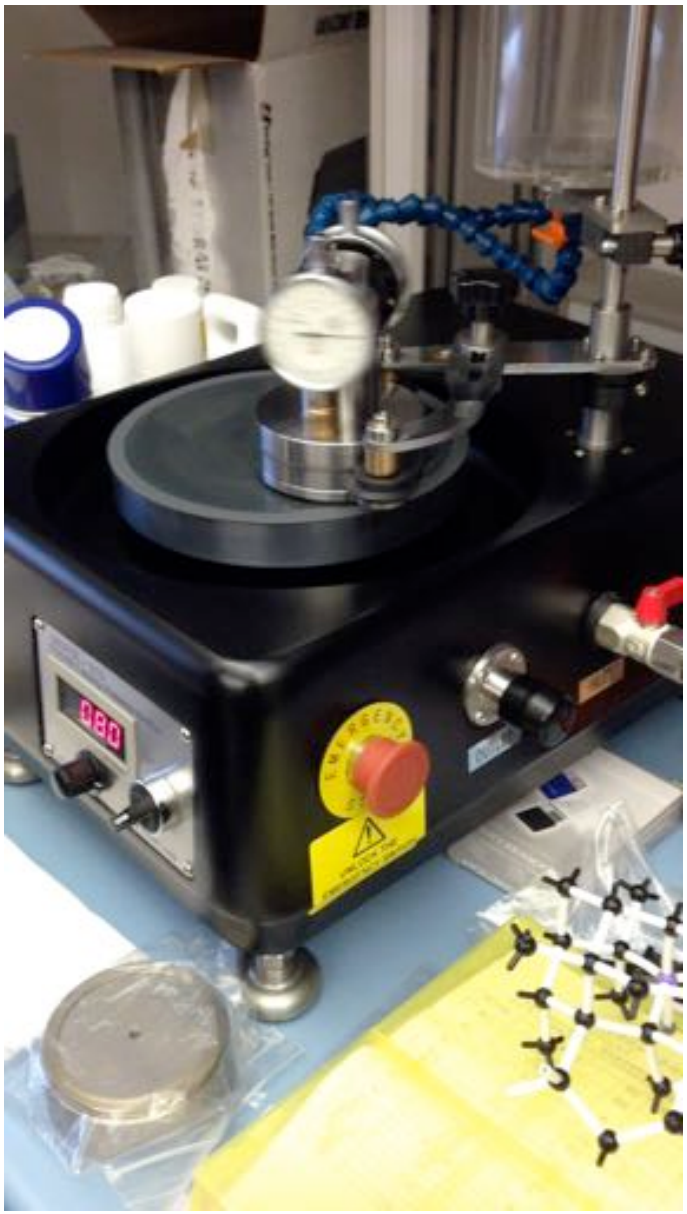


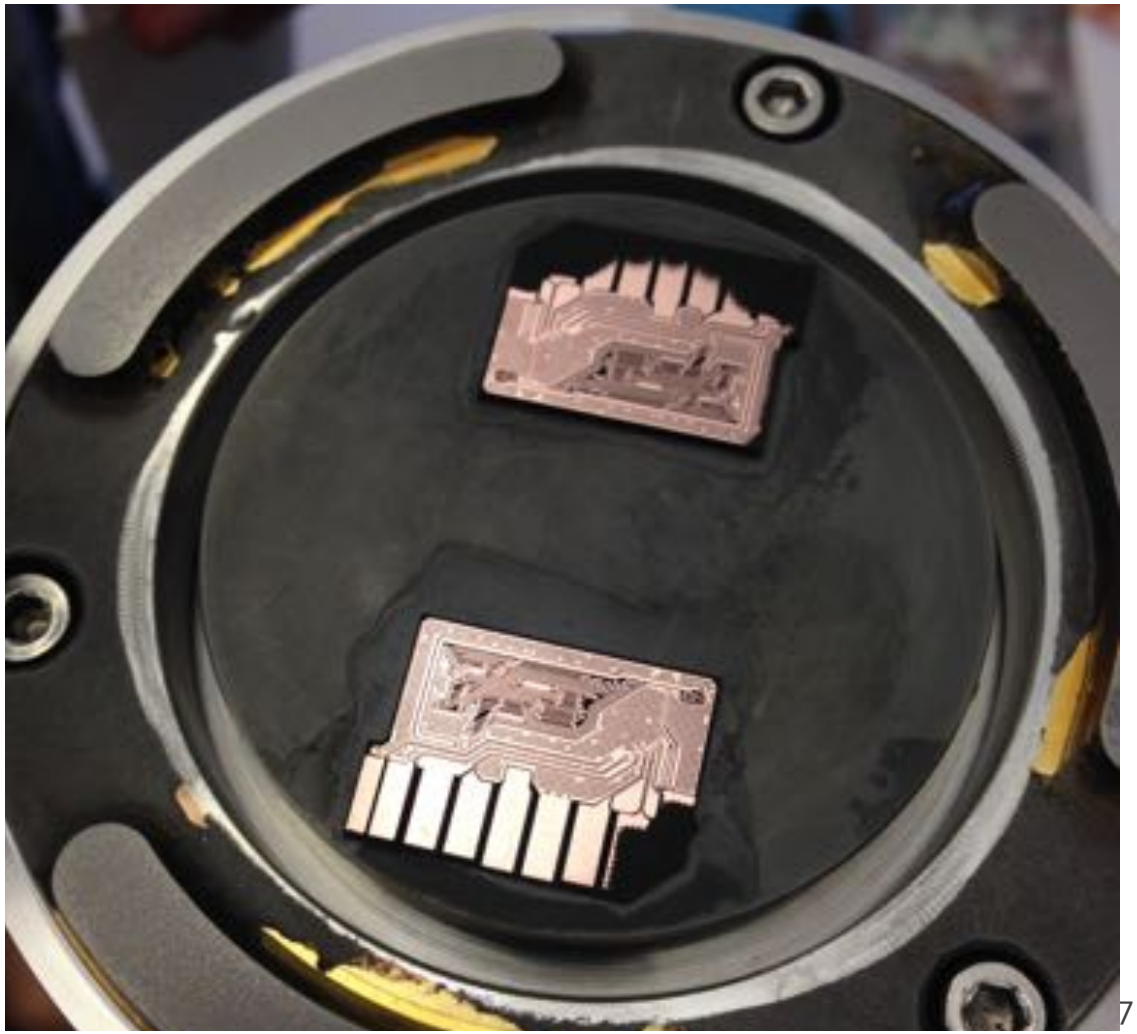
Embedded Security





Embedded Security





HTTPS, TLS, and the CA Ecosystem

How do we translate?

Cryptographic Primitives

Symmetric Encryption

RSA

PKI

HMAC

Certificate

Public Key

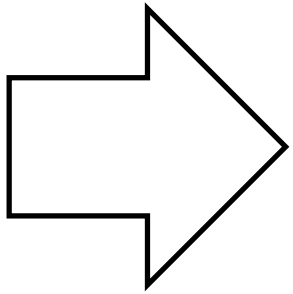
RC4

Diffie-Hellman

DSA

ECDSA

Asymmetric Encryption



Objectives:

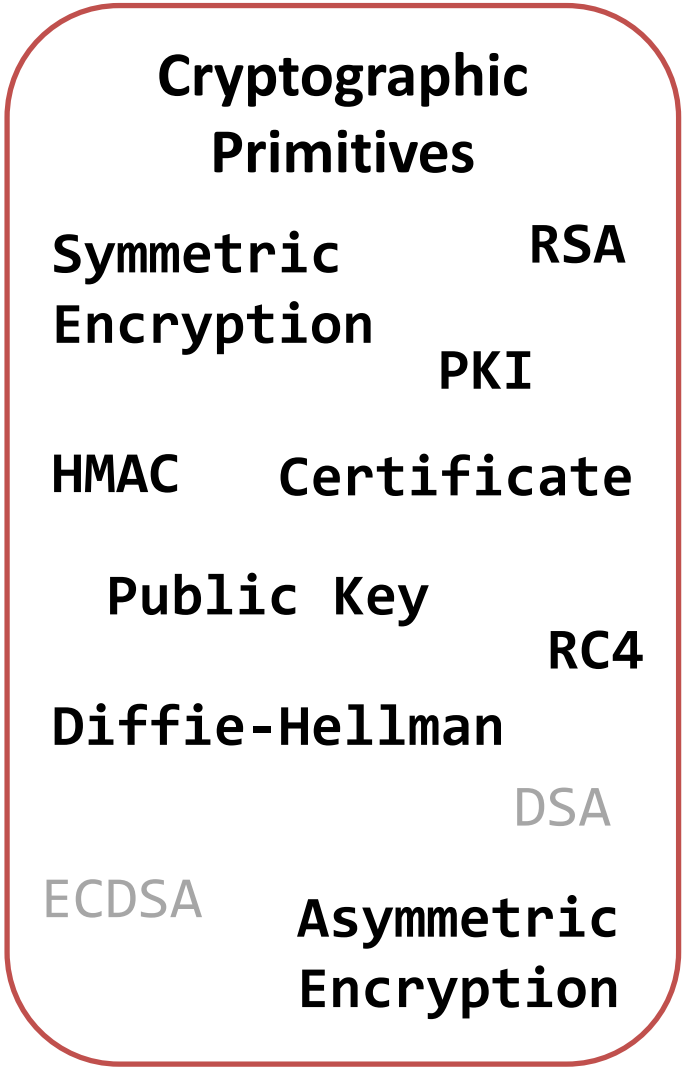
Message Integrity

Confidentiality

Authentication

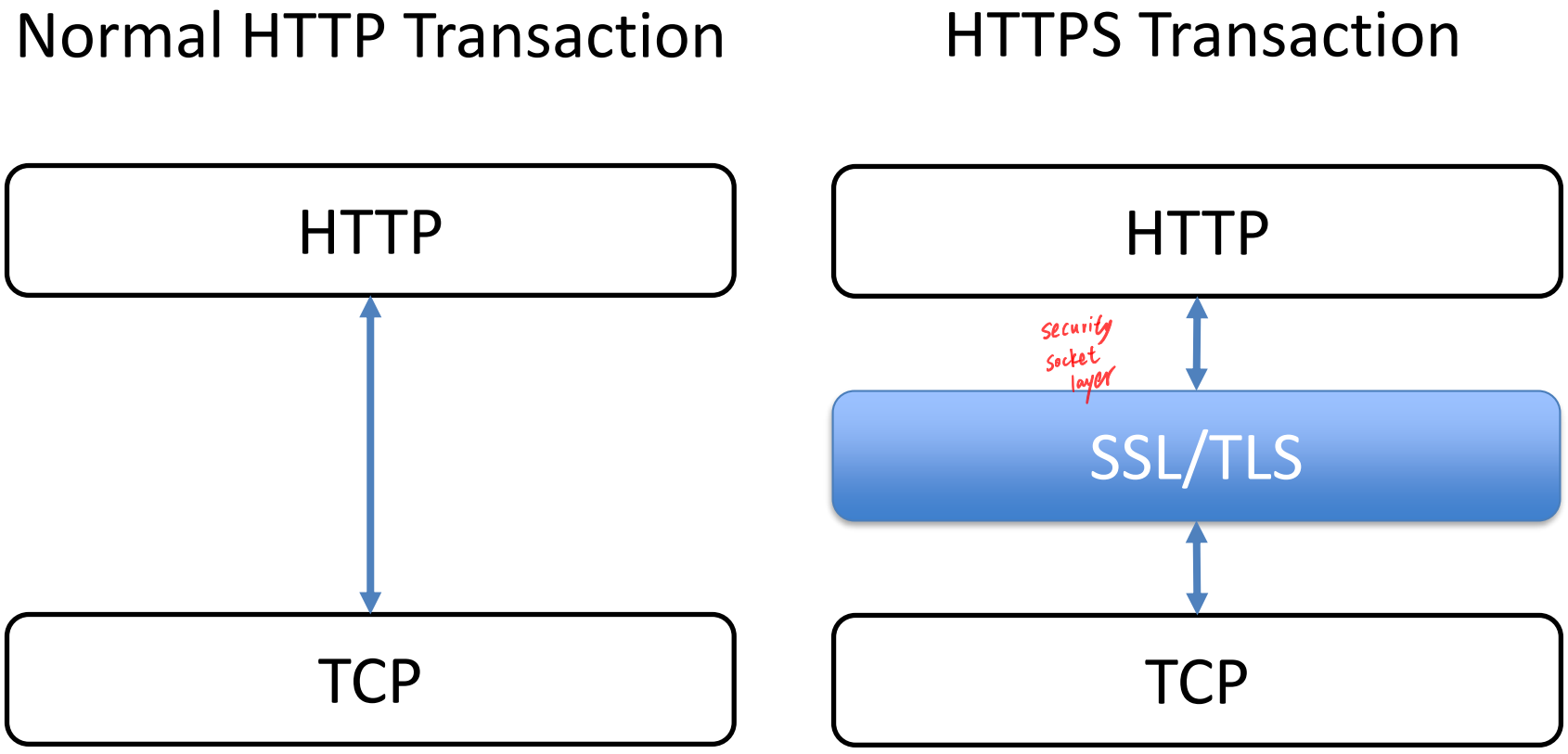
for Websites

How do we translate?



HTTPS Protocol

Adding Crypto to HTTP



SSL/TLS

Transport Layer Security

Arguably the most important (and widely used) cryptographic protocol on the Internet

Almost all popular encrypted protocols (except SSH) use SSL/TLS for transport encryption

HTTPS, POP3, IMAP, SMTP, FTP, NNTP, XMPP (Jabber), OpenVPN, SIP (VoIP), …

When you need an encrypted socket for your application, use SSL/TLS

SSL/TLS

SSL (Secure Socket Layer) – Netscape, late 1990s

- Version 2.0: Broken, don't use
  (disabled by default in modern browsers)
- Version 3.0: Broken, don’t use
  (starting to be disabled by browsers)

TLS (Transport Layer Security) – IETF Standard

- 1.0, 1.1: Outdated, prefer not to use
- 1.2: Commonly used
- 1.3: Standard being defined now

TLS Threat Model

Adversarial Network

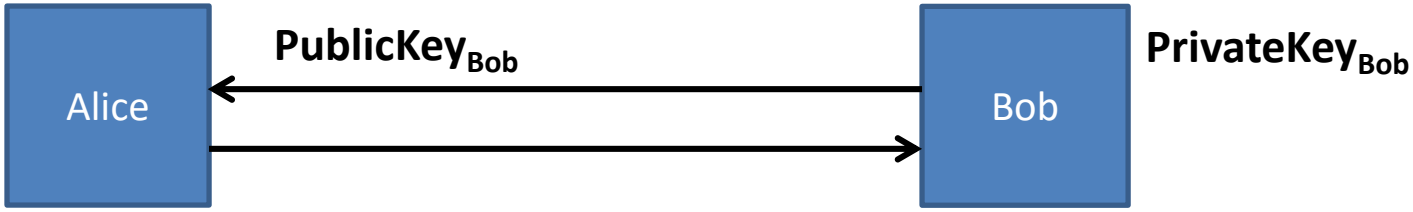
- Attacker controls infrastructure (routers, DNS, wireless access points)
- Passive attacker: only eavesdrops
- Active attacker: eavesdrops, injects, blocks, and modifies packets

Examples: Internet Café, Hotel, CSE

Does not protect against:

- Intruder on server
- Malware on client

Review: Public-key Crypto



Bob generates **PrivateKey$_{Bob}$, PublicKey$_{Bob}$** and distributes public key to Alice.

Alice can encrypt messages to Bob:

She uses **PublicKey$_{Bob}$** to encrypt message,

Bob can decrypt using **PrivateKey$_{Bob}$**

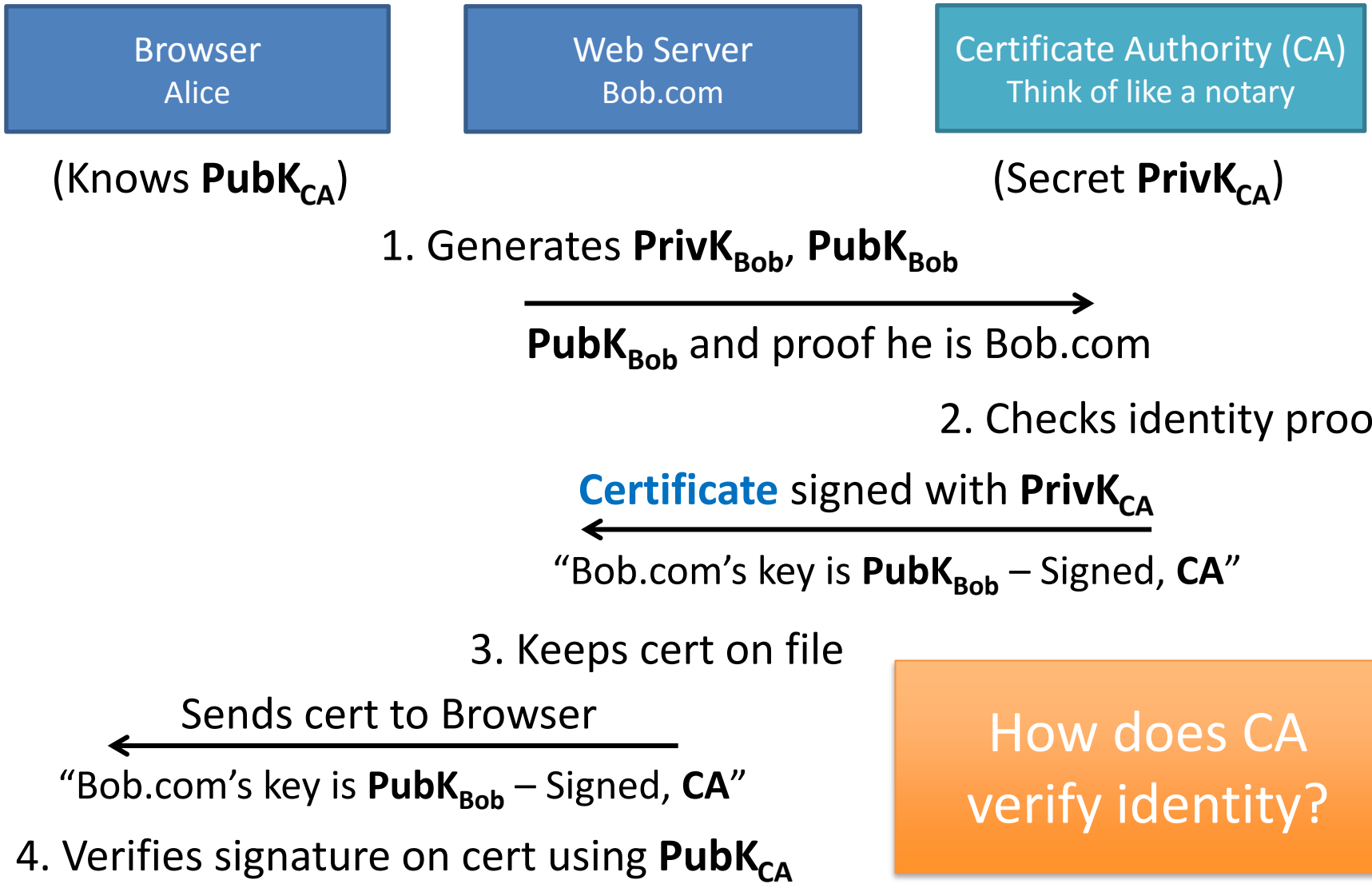
Bob can sign messages that Alice can verify:

He uses **PrivateKey$_{Bob}$** to generate signature,

Alice can verify using **PublicKey$_{Bob}$**

Certificates

How does the browser obtain the server's public key?



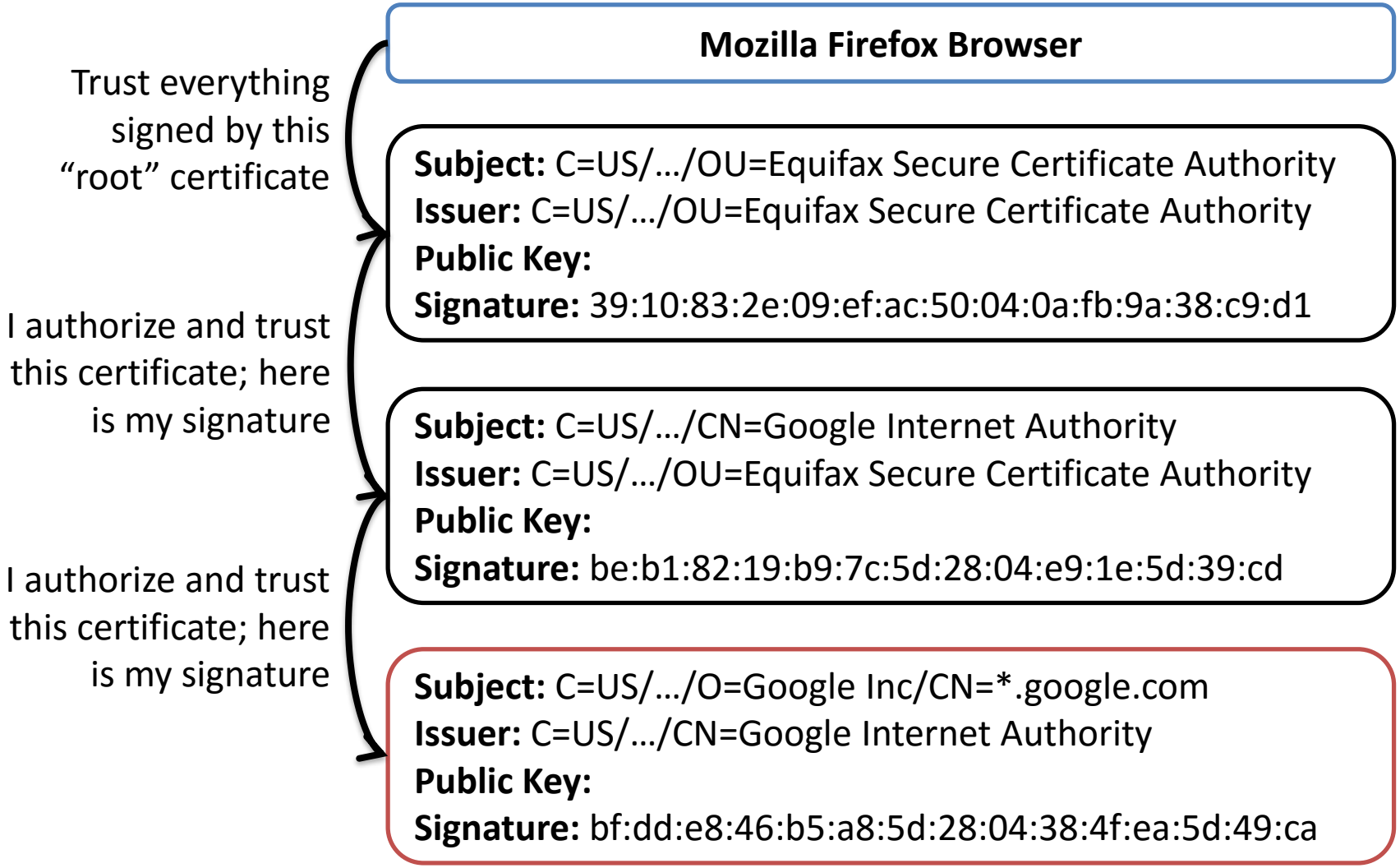
x.509 Certificates

Subject: CN=www.google.com
Issuer: C=US/O=Google Inc/CN=Google Internet Authority
Serial Number: 01:b1:04:17:be:22:48:b4:8e:1e:8b:a0:73:c9:ac:83
Validity Period: Jul 20 2015 - Jul 19 2016
Public Key Algorithm: rsaEncryption
Public Key: 43:1d:53:2e:09:ef:dc:50:54:0a:fb:9a:f0:fa:14:58:ad:a0:81:b0:3d
7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4
:ff:b5:8a:3a:a2:29:e2:6c:7c3:8:04:e9:1e5d:b5:7c3:8:04:e9:39:23:46

Signature Algorithm: sha1WithRSAEncryption

Signature: 39:10:83:2e:09:ef:ac:50:04:0a:fb:9a:f0:fa:14:58:ad:a0:81:b0:3d
7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4
:ff:b5:8a:3a:a2:29:e2:6c:7c3:8:04:e9:1e5d:b5:7c3:8:04:e9:1e:5d:b5

Certificate Chains



Certificate Authority Ecosystem

Each browser trusts a set of CAs

- CAs can sign certificates for new Cas
- CAs can sign certificates for *any* web site

If a single CA is compromised, then the entire system is compromised

We ultimately place our complete trust of the Internet in the weakest CA

Getting a Certificate

Embedded Security Intermission Highlights: Prof. Wenyuan Xu

环球科学 SCIENTIFIC AMERICAN 《科学美国人》中文版

Embedded Security: Ultrasound

DolphinAttack: Inaudible Voice Commands

- http://www.usslab.org/projects/dolphinAttack.html
  ACM CCS 2017

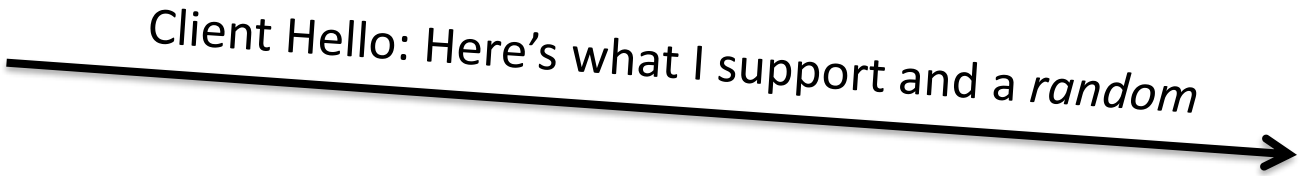
Manuf.	Model	OS/Ver.	SR System	Attacks		Modulation Parameters		Max Dist. (cm)	
				Recog.	Activ.	f_c (kHz) & [Prime f_c] ‡	Depth	Recog.	Activ.
Apple	iPhone 4s	iOS 9.3.5	Siri	√	√	20–42 [27.5]	> 9%	175	110
Apple	iPhone 5s	iOS 10.0.2	Siri	√	√	24.1 26.2 27 29.3 [24.1]	100%	7.5	10
Apple	iPhone SE	iOS 10.3.1	Siri	√	√	22–28 33 [22.6]	≥ 43%	30	25
			Chrome	√	N/A	22–26 28 [22.6]	≥ 37%	16	N/A
Apple	iPhone SE ?	iOS 10.3.2	Siri	√	√	21–29 31 33 [22.4]	≥ 43%	21	24
Apple	iPhone 6s +	iOS 10.2.1	Siri	√	√	26 [26]	100%	4	12
Apple	iPhone 6 Plus +	iOS 10.3.1	Siri	×	√	— [24]	—	—	7
Apple	iPhone 7 Plus +	iOS 10.3.1	Siri	√	√	21 24-29 [25.3]	≥ 50%	18	12
Apple	watch	watchOS 3.1	Siri	√	√	20–37 [22.3]	≥ 5%	111	164
Apple	iPad mini 4	iOS 10.2.1	Siri	√	√	22–40 [28.8]	≥ 25%	91.6	30.5
Apple	MacBook	macOS Sierra	Siri	√	N/A	20-22 24-25 27-37 39 [22.8]	≥ 76%	31	N/A
LG	Nexus 5X	Android 7.1.1	Google Now	√	√	30.7 [30.7]	100%	6	11
Asus	Nexus 7	Android 6.0.1	Google Now	√	√	24–39 [24.3]	≥ 5%	88	87
Samsung	Galaxy S6 edge	Android 6.0.1	S Voice	√	√	20–38 [28.4]	≥ 17%	36.1	36.2
Huawei	Honor 7	Android 6.0	HiVoice	√	√	29–37 [29.5]	≥ 17%	13	14
Lenovo	ThinkPad T440p	Windows 10	Cortana	√	√	23.4–29 [23.6]	≥ 35%	58	8
Amazon	Echo +	3589	Alexa	√	√	20-21 23-31 33-34 [24]	≥ 20%	165	165
Audi	Q3	N/A	N/A	√	N/A	21–23 [22]	100%	10	N/A

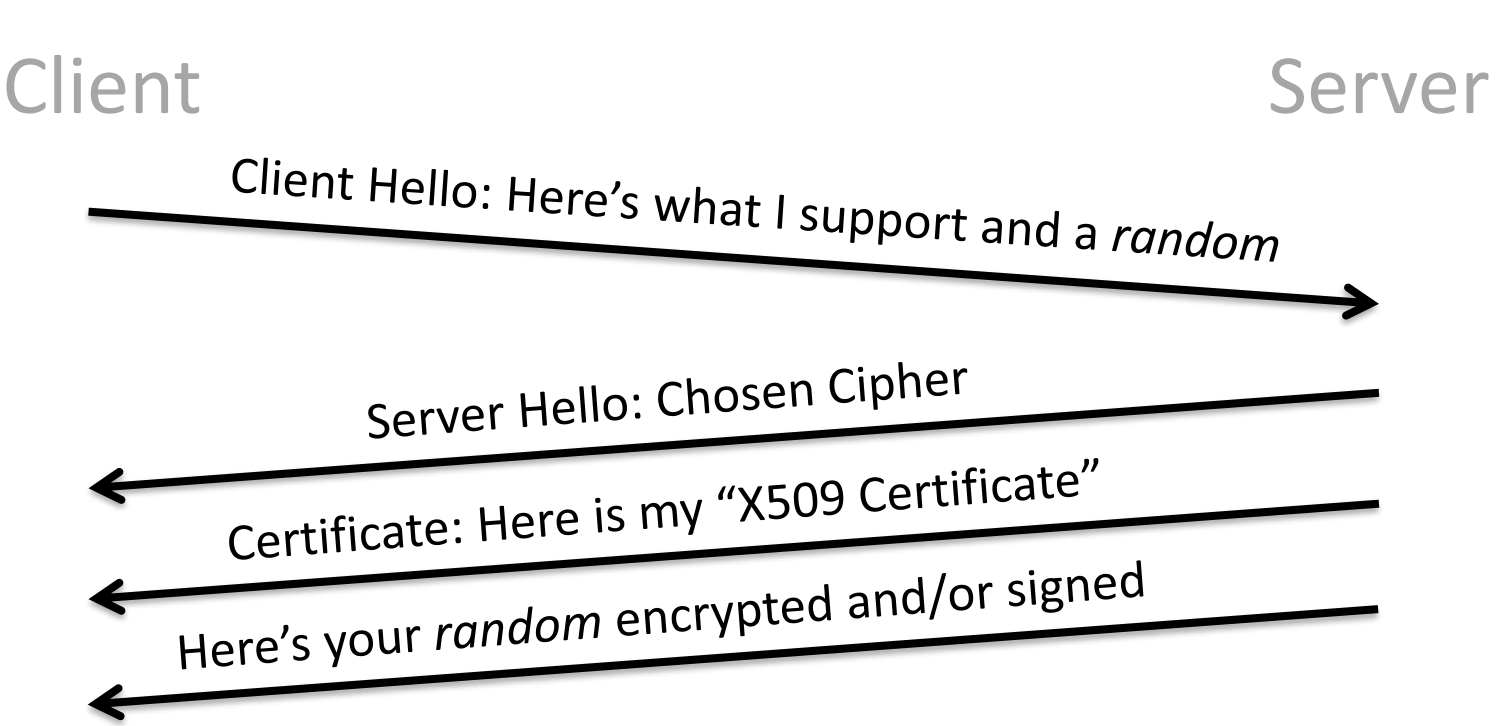
Client Server

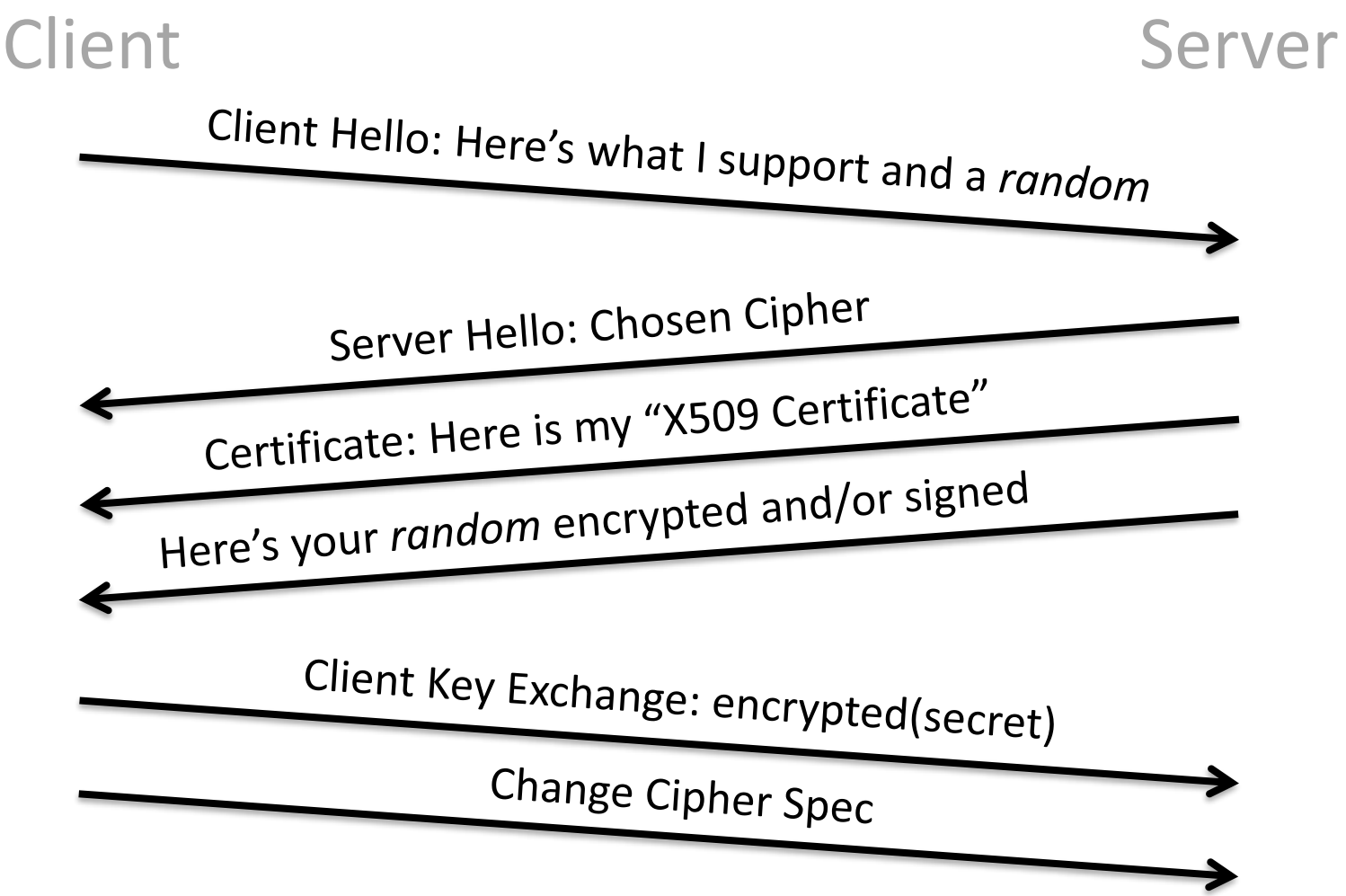
The TLS “handshake”

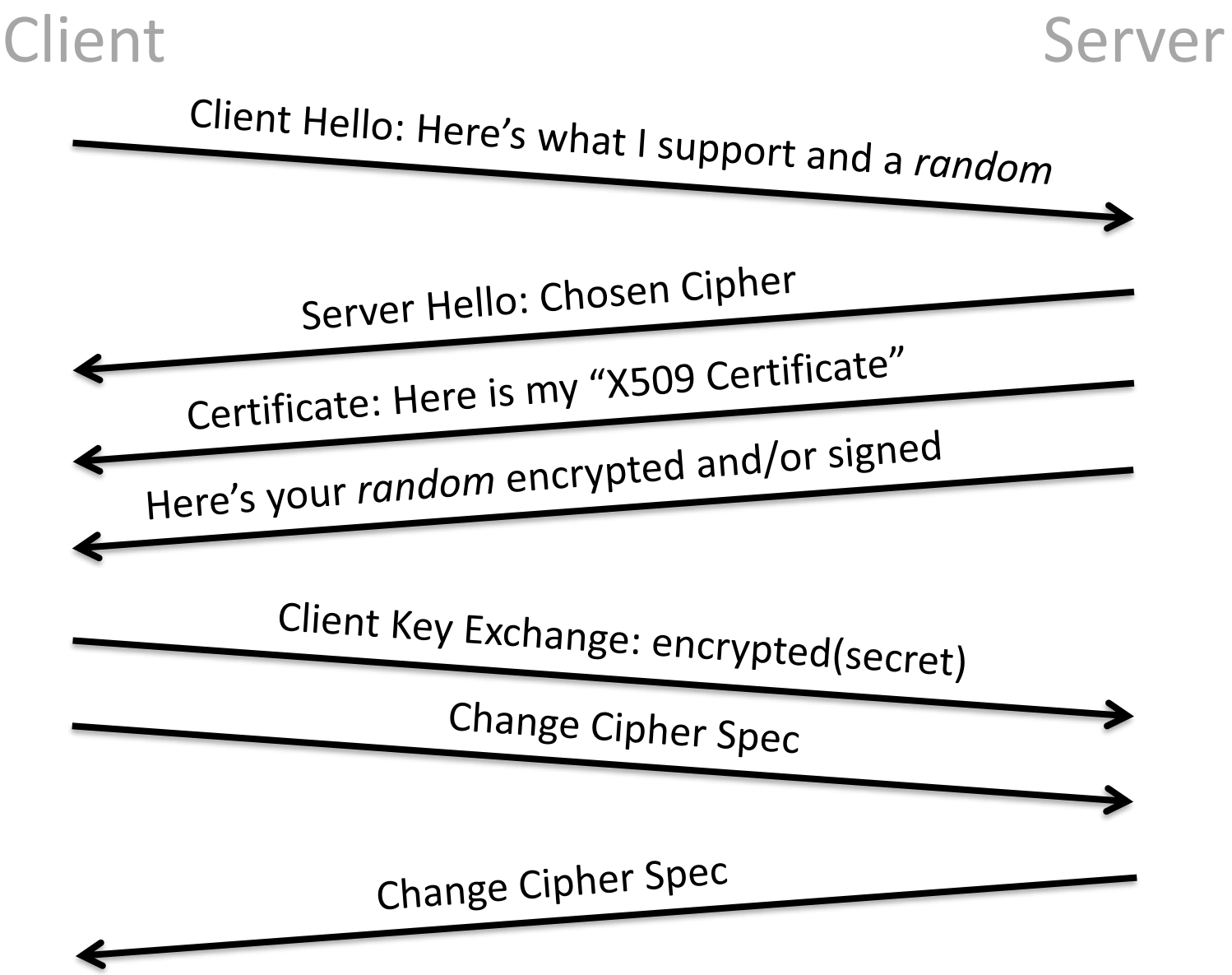
Client

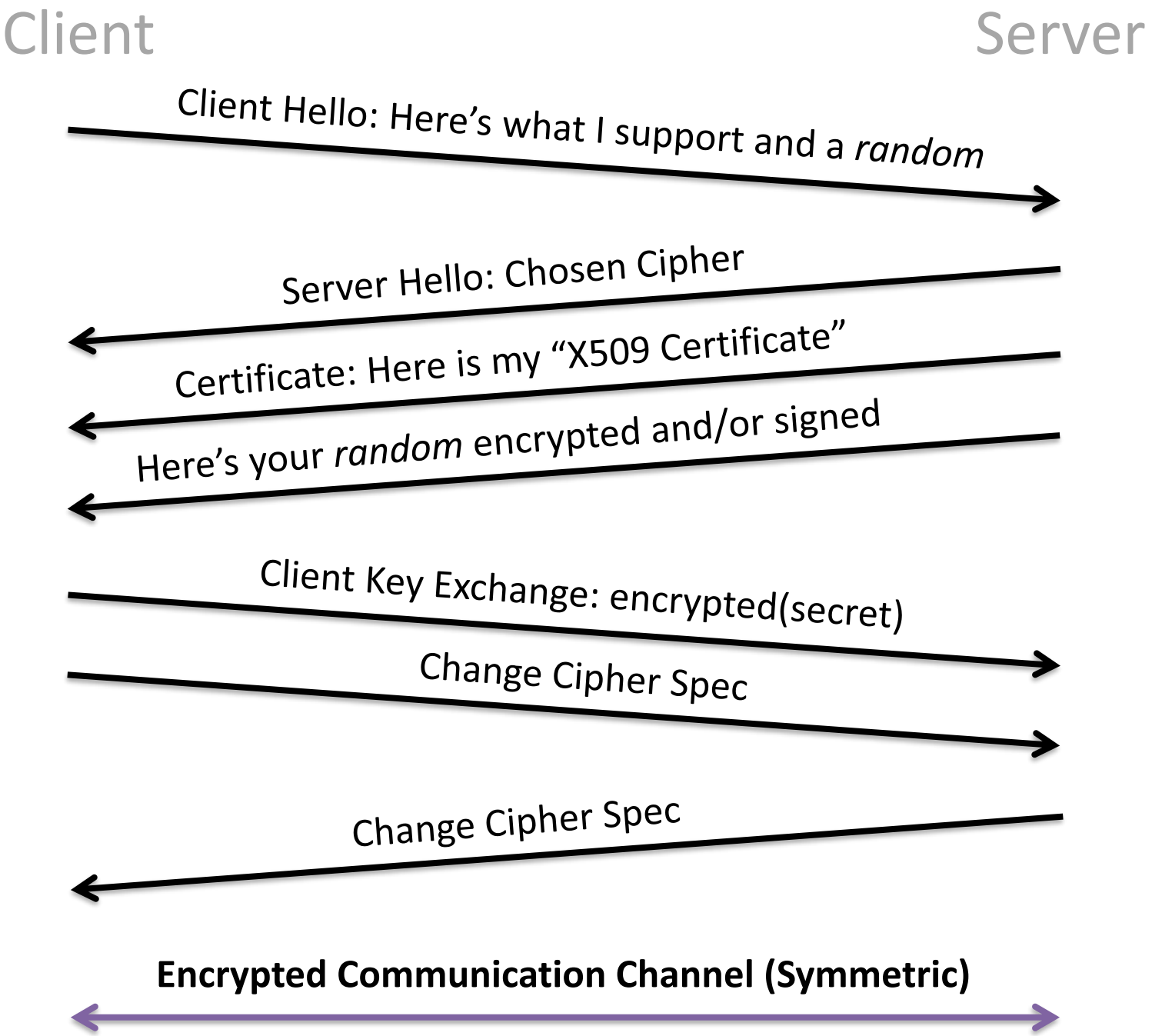
Server



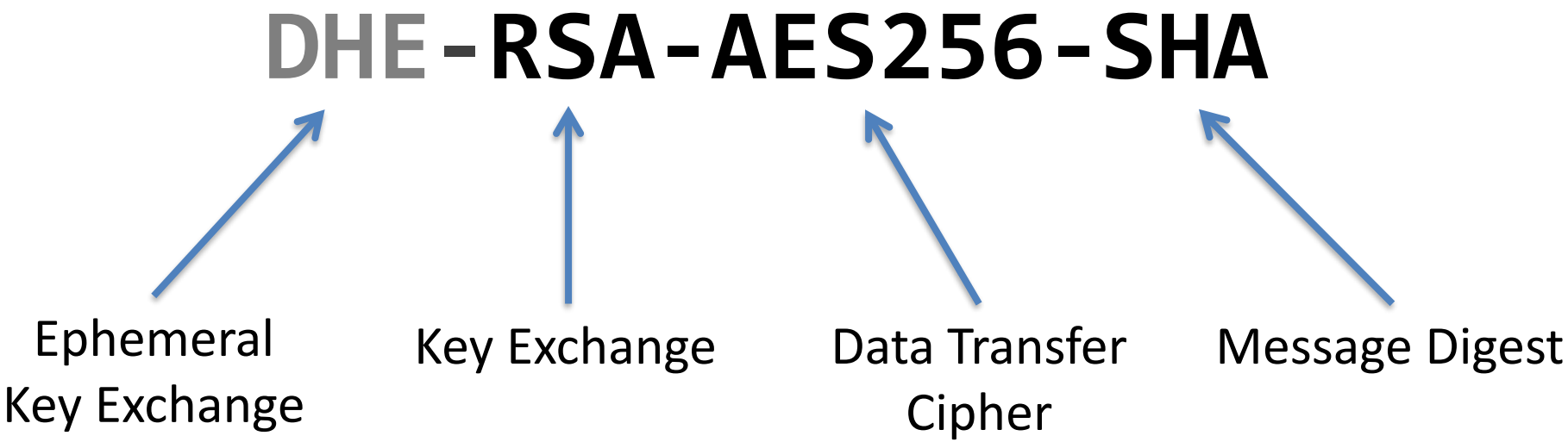

Client
Server
Client Hello: Here's what I support and a *random*
Server Hello: Chosen Cipher
Certificate: Here is my "X509 Certificate"
Here's your *random* encrypted and/or signed


Client
Server
Client Hello: Here's what I support and a *random*
Server Hello: Chosen Cipher
Certificate: Here is my "X509 Certificate"
Here's your *random* encrypted and/or signed
Client Key Exchange: encrypted(secret)
Change Cipher Spec


Client
Server
Client Hello: Here's what I support and a *random*
Server Hello: Chosen Cipher
Certificate: Here is my "X509 Certificate"
Here's your *random* encrypted and/or signed
Client Key Exchange: encrypted(secret)
Change Cipher Spec
Change Cipher Spec


Client
Server
Client Hello: Here's what I support and a *random*
Server Hello: Chosen Cipher
Certificate: Here is my "X509 Certificate"
Here's your *random* encrypted and/or signed
Client Key Exchange: encrypted(secret)
Change Cipher Spec
Change Cipher Spec
Encrypted Communication Channel (Symmetric)

Cipher Suites



HTTPS User Interface (Tricky!)

Goal: Help users authenticate site

Lock icon — Displayed when all elements of page fetched using HTTPS

HTTPS cert must be issued by a CA trusted by browser
HTTPS cert is valid (e.g., not expired or revoked)
CommonName in cert matches domain in URL

Must check all of these or else a problem!

Extended Validation (EV) certificates

Green Bar in Firefox with name of the organization.
(Mostly for banks and large e-commerce sites)

CA does extra work to verify identity — expensive, more secure?

Invalid certificate warnings

(Deliberately hard to override, users do anyway)


The site's security certificate is not trusted!
You attempted to reach [redacted], but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

Goals

Confidentiality (Symmetric Crypto)

Message Integrity (HMACs)

Authentication (Public Key Crypto)

Attacks Against HTTPS

1. Attacking the Browser UI

Picture-in-picture Attack

Spoof the user interface
Attacker page draws fake browser window with lock icon

Semantic Attacks

Example: micros0ft.com

Example: International character sets contains chars that look similar to English letters

Example: Hiding domain later in long URL
"www.bank.com/accounts/login.php@attacker.com"

Invalid Certs

Expired, Common Name != URL, unknown CA (e.g., self-signed)

Warning overload — Many users will click through

Accepting enables man-in-the-middle attack (active adversary)

Defense: Make it hard for users to click through (Firefox takes 4 clicks!)

2. Attacking Site Design

ssl_strip attack

Many sites:
- browse via HTTP, switch to HTTPS for checkout
- connect via HTTP, switch to HTTPS for login
- Simple attack: Transparent proxy strips out redirects, relays HTTP to HTTPS on server

Defenses?

Mixed Content attack

Page loads over HTTPS but contains content over HTTP (common)
e.g. JavaScript, Flash

Active attacker can tamper with HTTP content to hijack session

Defense: Browser warnings, ("This page contains insecure content“), but inconsistent and often ignored

3. Attacking the CA Ecosystem

Distributed architecture: *Nobody knows* complete set of trusted intermediate CAs…
(1,733 visible in UMich Internet-wide scans CAs)

History of CAs being hacked (e.g., **DigiNotar**)

Oops! Korea gave every elementary school, library, and agency a CA certificate (1,324)

Luckily, were invalid due to a higher-up constraint

DigiNotar

- DigiNotar ***was*** a Dutch Certificate Authority
- On June 10, 2011, **`*.google.com`** cert was issued to an attacker and subsequently used to orchestrate MITM attacks in Iran
- Nobody noticed the attack until someone found the certificate in the wild…

DigiNotar Contd.

- DigiNotar later admitted that dozens of fraudulent certificates were created
- Google, Microsoft, Apple and Mozilla all revoked the root DigiNotar certificate
- Dutch Government took over DigiBotar
- DigiBotar went bankrupt

"-----BEGIN RSA PRIVATE KEY-----" -openssl

Search

About 274,000 results (0.24 seconds)

Everything
Images
Maps
Videos
News
Shopping
More

All results
Related searches
More search tools

-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...
pastebin.com/TbaeU93m
19 Apr 2010 – ... the difference. Copied. -----**BEGIN RSA PRIVATE KEY**-----.
MIICXwIBAAKBpenis1ePqHkVN9lKaGBESjV6zBrIsZc+XQYTtSiVa9Ri4SAXoYpl ...

-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...
pastebin.com/sC7bGw30
18 Apr 2010 – ... difference. Copied. -----**BEGIN RSA PRIVATE KEY**-----.
MIIEogIBAAKCAQEAvxBaihzKMewLvmIr1ptID1gO7EWGFyudzOAHLqm3+0+gpPbk ...

site:pastebin.com "-----BEGIN RSA PRIVATE KEY-----" - Posterous
cdevers.posterous.com/site-pastebin-com-**begin-rsa-private-key**-google
20 Apr 2010 – Apr 19, 2010 ... -----**BEGIN RSA PRIVATE KEY**-----
MIICXwIBAAKBpenis1ePqHkVN9lKaGBESjV6zBrIsZc+ XQYTtSiVa9Ri4SAXoYpl .

help/en/howto/sftp – Cyberduck
trac.cyberduck.ch/wiki/help/en/howto/sftp
Private keys containing a DSA or RSA private key in PEM format are supported (look for -----BEGIN DSA PRIVATE KEY----- or -----**BEGIN RSA PRIVATE KEY**----- ...

SSH access with a private RSA key [Archive] - VanDyke Software For...
forums.vandyke.com/archive/index.php/t-2185.html
2 Sep 2011 – -----**BEGIN RSA PRIVATE KEY**-----
MIIEogIBAAKCAQBujdbtxyIX4KaQPeTf5F/
aOSBwSpZN4MjTixU2Yq8JkipjMYpYwpNj1TODzRJf ...

4. Attacking Implementations

Null Prefix Attack, 2009

(x.509 uses Pascal-style strings, browsers use C strings; what if a common name contains "\0"?)

`gmail.com\0.badguy.com`

Apple Goto Fail, Feb. 2014

(Apple SSL bug; skipped certificate check for almost a year!)

OpenSSL Heartbleed, April 2014

(OpenSSL bug; leaked data, including private key!)

Mozilla BERsek, October 2014

(Bug in verifying cert signatures, allowed spoofing certs, probably since the beginning….!)

Takeaways

- Use HTTPS! It’s so much better than nothing.
- TLS will keep breaking.
  Use it, but don't rely on it exclusively.
- Have a backup plan for times when it's broken.

ANDY GREENBERG SECURITY 11.03.16 08:00 PM

GOOGLE'S CHROME HACKERS ARE ABOUT TO UPEND YOUR IDEA OF WEB SECURITY

Parisa Tabriz, center, and the Chrome security team. AMY HARRITY FOR WIRED

Next Time: HTTPS Attacks

- Leading the Chrome security team's push for HTTPS
- Post questions on Piazza for Adrienne Porter Felt

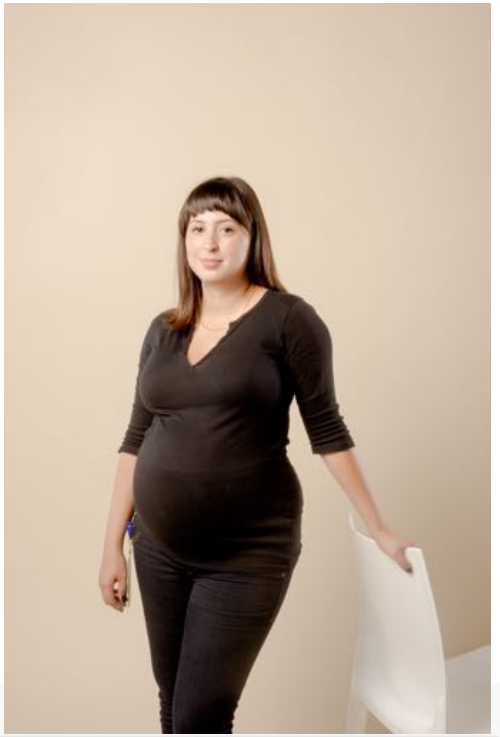


Photo: Amy Harrity for WIRED

Percentage of HTTPS pages viewed in Chrome over time.Google

Next Time: HTTPS Attacks

Post HTTPS questions on Piazza for Adrienne Porter Felt!!