CSE 484 / CSE M 584: Computer Security and Privacy

#### Web Security [Certificates and Overview]

Spring 2020

Franziska (Franzi) Roesner <u>franzi@cs.washington.edu</u>

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

## Admin

• Today:

- Transition to web security

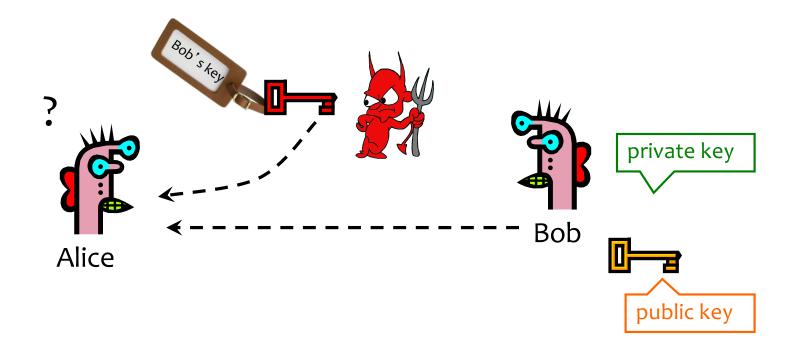
• Lab 1 due on Friday

- See FAQs on discussion board

# Cryptography Summary

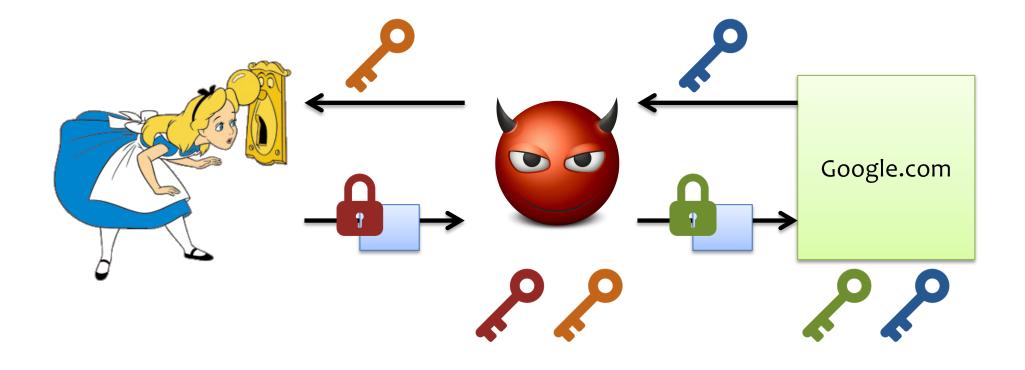
- Goal: Privacy
  - Symmetric keys:
    - One-time pad, Stream ciphers
    - Block ciphers (e.g., DES, AES) → modes: EBC, CBC, CTR
  - Public key crypto (e.g., Diffie-Hellman, RSA)
- Goal: Integrity
  - MACs, often using hash functions (e.g, SHA-256)
- Goal: Privacy and Integrity – Encrypt-then-MAC
- Goal: Authenticity (and Integrity)
  - Digital signatures (e.g., RSA, DSS)

## **Authenticity of Public Keys**



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

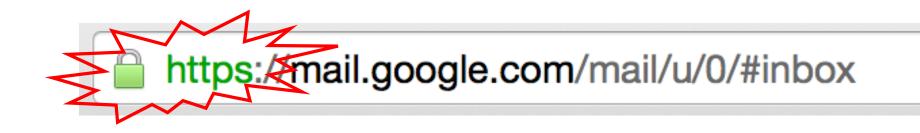
#### **Threat: Person-in-the Middle**



## **Distribution of Public Keys**

- Public announcement or public directory
  - Risks: forgery and tampering
- Public-key certificate
  - Signed statement specifying the key and identity
    - sig<sub>CA</sub>("Bob", PK<sub>B</sub>)
- Common approach: certificate authority (CA)
  - Single agency responsible for certifying public keys
  - After generating a private/public key pair, user proves his identity and knowledge of the private key to obtain CA's certificate for the public key (offline)
  - Every computer is <u>pre-configured</u> with CA's public key

## You encounter this every day...



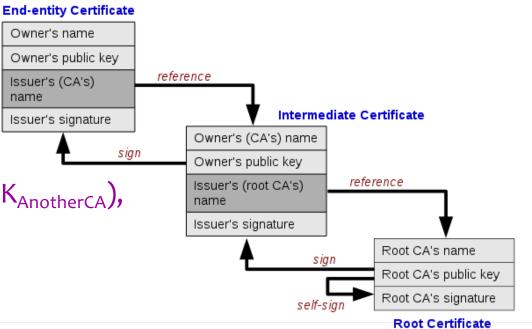
#### SSL/TLS: Encryption & authentication for connections

## **Example of a Certificate**

	1		
Expires: Mo This cert	<b>com</b> Google Internet Authority G2 onday, July 6, 2015 at 5:00:00 P ifficate is valid	M Pacific Daylight Time	
Organization G Common Name *	California Aountain View Google Inc	Parameters Not Valid Before Not Valid After	SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 ) none Wednesday, April 8, 2015 at 6:40:10 AM Pacific Daylight Time Monday, July 6, 2015 at 5:00:00 PM Pacific Daylight Time
		Public Key Info Algorithm Parameters Public Key Key Size Key Usage Signature	256 bits

## **Hierarchical Approach**

- Single CA certifying every public key is impractical
- Instead, use a trusted root authority (e.g., Verisign)
  - Everybody must know the root's public key
  - Instead of single cert, use a certificate chain
    - sig<sub>Verisign</sub>("AnotherCA", PK<sub>AnotherCA</sub>), sig<sub>AnotherCA</sub>("Alice", PK<sub>A</sub>)



– What happens if root authority is ever compromised?

# **Trusted(?) Certificate Authorities**

		Keychain Ac	cess	
Click to unlo	ock the System Roots k	Q Search		
Keychains Iogin Local Items System System Roo	Certificate Root	Boot contificate authority		
	Name		∧ Kind	Expires
	📷 AdminCA	-CD-T01	certificate	Jan 25, 2016, 4:36:19 AM
Category	Carter AffirmTru	st Commercial	certificate	Dec 31, 2030, 6:06:06 AM
All Items	📷 AffirmTru	st Networking	certificate	Dec 31, 2030, 6:08:24 AM
<ul> <li>Passwords</li> <li>Secure Note</li> <li>My Certifica</li> <li>Keys</li> <li>Certificates</li> </ul>	es AffirmTru tes America America America Apple Ro Apple Ro Apple Ro Apple Ro	ot CA - G2 ot CA - G3 ot Certificate Authorit on CA G2	2 certificate certificate certificate certificate	Dec 31, 2040, 6:10:36 AM Dec 31, 2040, 6:20:24 AM Nov 19, 2037, 12:43:00 PM Sep 29, 2037, 7:08:00 AM Feb 9, 2035, 1:40:36 PM Apr 30, 2039, 11:10:09 AM Apr 30, 2039, 11:19:06 AM Feb 9, 2025, 4:18:14 PM Mar 31, 2016, 7:59:59 AM Dec 12, 2017, 7:00:00 AM
	+ i Cop	y	213 items	

#### **Turtles All The Way Down...**



The saying holds that the world is supported by a chain of increasingly large turtles. Beneath each turtle is yet another: it is "turtles all the way down".

[Image from Wikipedia]

## Many Challenges...

- Hash collisions
- Weak security at CAs

- Allows attackers to issue rogue certificates

- Users don't notice when attacks happen
   We'll talk more about this later in the course
- How do you revoke certificates?

DigiNotar is a Dutch Certificate Authority. They sell SSL certificates.



#### **Attacking CAs**

<u>Security of DigiNotar</u> <u>servers:</u>

- All core certificate servers controlled by a single admin password (Prod@dm1n)
- Software on publicfacing servers out of date, unpatched
- No anti-virus (could have detected attack)

Somehow, somebody managed to get a rogue SSL certificate from them on **July 10th**, **2011**. This certificate was issued for domain name **.google.com**.

What can you do with such a certificate? Well, you can impersonate Google — assuming you can first reroute Internet traffic for google.com to you. This is something that can be done by a government or by a rogue ISP. Such a reroute would only affect users within that country or under that ISP.

#### Consequences

- Attacker needs to first divert users to an attackercontrolled site instead of Google, Yahoo, Skype, but then...
  - For example, use DNS to poison the mapping of mail.yahoo.com to an IP address
- ... "authenticate" as the real site
- ... decrypt all data sent by users
  - Email, phone conversations, Web browsing

Attempt to Fix CA Problems: Certificate Transparency

- **Problem:** browsers will think nothing is wrong with a rogue certificate until revoked
- **Goal:** make it impossible for a CA to issue a bad certificate for a domain without the owner of that domain knowing

- (Then what?)

• Approach: auditable certificate logs

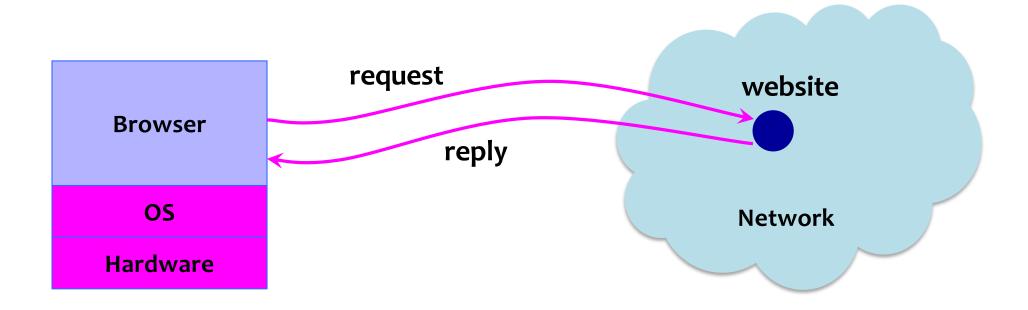
#### www.certificate-transparency.org

#### Attempt to Fix CA Problems: Certificate Pinning

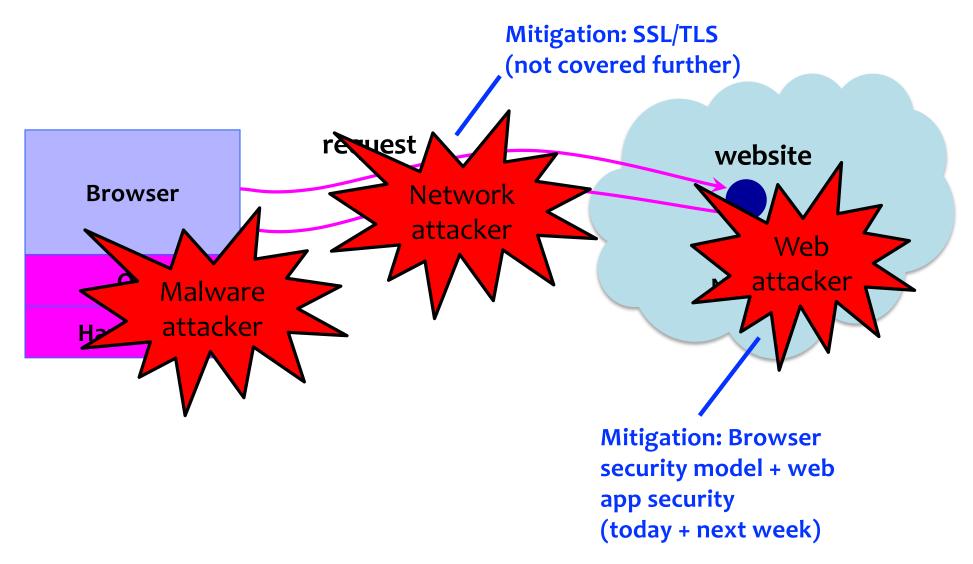
- Trust on first access: tells browser how to act on subsequent connections
- HPKP HTTP Public Key Pinning
  - Use these keys!
  - HTTP response header field "Public-Key-Pins"
- HSTS HTTP Strict Transport Security
  - Only access server via HTTPS
  - HTTP response header field "Strict-Transport-Security"

## Web+Browser Security

#### **Big Picture: Browser and Network**



#### Where Does the Attacker Live?



### Web Attacker

- Controls a malicious website (attacker.com)
   Can even obtain SSL/TLS certificate for site Secure https://
- User visits attacker.com why?
  - Phishing email, enticing content, search results, placed by an ad network, blind luck ...
- Attacker has no other access to user machine!
- Variation: good site **honest.com**, but:
  - An iframe with malicious content included
  - Website has been compromised