Today’s Lecture

- Applying crypto technology in practice
- Two simple abstractions cover 80% of the use cases for crypto:
  - “Sealed blob”: Data that is encrypted and authenticated under a particular key
  - Secure channel: Communication channel that can’t be eavesdropped on or tampered with
- Today: How SSL provides a secure channel
Basic idea

- Browser (client) picks some symmetric keys for encryption + authentication
- Client sends them to server, encrypted using RSA public-key encryption
- Both sides send MACs
- Now they use these keys to encrypt and authenticate all subsequent messages, using symmetric-key crypto
HTTPS Connection (SSL / TLS)

- Browser (client) connects via TCP to Amazon’s HTTPS server
- Client picks 256-bit random number $R_B$, sends over list of crypto protocols it supports
- Server picks 256-bit random number $R_S$, selects protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- **Client now validates cert**
HTTPS Connection (SSL / TLS), cont.

- For RSA, browser constructs “Premaster Secret” \( PS \)
- Browser sends \( PS \) encrypted using Amazon’s public RSA key \( K_{Amazon} \)
- Using \( PS \), \( R_B \), and \( R_S \), browser & server derive symm. cipher keys (\( C_B, C_S \)) & MAC integrity keys (\( I_B, I_S \))
  - One pair to use in each direction
For RSA, browser constructs “Premaster Secret” $PS$.

Browser sends $PS$ encrypted using Amazon’s public RSA key $K_{Amazon}$.

Using $PS$, $R_B$, and $R_S$, browser & server derive symmetric cipher keys ($C_B$, $C_S$) & MAC integrity keys ($I_B$, $I_S$).

- One pair to use in each direction.

These seed a cryptographically strong pseudo-random number generator (PRNG). Then browser & server produce $C_B$, $C_S$, etc., by making repeated calls to the PRNG.
HTTPS Connection (SSL / TLS), cont.

- For RSA, browser constructs “Premaster Secret” PS
- Browser sends PS encrypted using Amazon’s public RSA key $K_{Amazon}$
- Using PS, $R_B$, and $R_S$, browser & server derive symm. *cipher keys* ($C_B, C_S$) & MAC *integrity keys* ($I_B, I_S$)
  - One pair to use in each direction
- Browser & server exchange MACs computed over entire dialog so far
- If good MAC, Browser displays
- All subsequent communication encrypted w/ symmetric cipher (e.g., AES128) cipher keys, MACs
  - Sequence #’s thwart replay attacks

Here’s my cert

~2-3 KB of data

{PS}_{K_{Amazon}}

$\{M_1, \text{MAC}(M_1, I_B)\}_{CB}$

$\{M_2, \text{MAC}(M_2, I_S)\}_{CS}$
Alternative: Key Exchange via Diffie-Hellman

- For Diffie-Hellman, server generates random $a$, sends public params and $g^a \mod p$
  - Signed with server’s private key
- Browser verifies signature
- Browser generates random $b$, computes $PS = g^{ab} \mod p$, sends to server
- Server also computes $PS = g^{ab} \mod p$
- Remainder is as before: from $PS$, $R_B$, and $R_S$, browser & server derive symm. *cipher keys* ($C_B$, $C_S$) and MAC *integrity keys* ($I_B$, $I_S$), etc…
**HTTPS Connection (SSL / TLS)**

- Browser (client) connects via TCP to Amazon’s HTTPS server
- Client picks 256-bit random number $R_B$, sends over list of crypto protocols it supports
- Server picks 256-bit random number $R_S$, selects protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- **Client now validates cert**
Certificates

- Cert = signed statement about someone’s public key
  - Note that a cert does not say anything about the identity of who gives you the cert
  - It simply states a given public key $K_{Bob}$ belongs to Bob …
    - … and backs up this statement with a digital signature made using a different public/private key pair, say from Verisign
- Bob then can prove his identity to you by you sending him something encrypted with $K_{Bob}$ …
  - … which he then demonstrates he can read
- … or by signing something he demonstrably uses
- Works provided you trust that you have a valid copy of Verisign’s public key …
  - … and you trust Verisign to use prudence when she signs other people’s keys
Validating Amazon’s Identity

• Browser compares domain name in cert w/ URL
  – Note: this provides an end-to-end property
    (as opposed to say a cert associated with an IP address)

• Browser accesses separate cert belonging to issuer
  – These are hardwired into the browser - trusted!
  – There could be a chain of these …

• Browser applies issuer’s public key to verify signature \( S \), obtaining hash of what issuer signed
  – Compares with its own SHA-1 hash of Amazon’s cert

• Assuming hashes match, now have high confidence it’s indeed Amazon …
  – assuming signatory is trustworthy

= assuming didn’t lose private key; assuming didn’t sign thoughtlessly
End-to-End $\Rightarrow$ Powerful Protections

- Attacker runs a sniffer to capture our WiFi session?
  - *(maybe by breaking crummy WEP security)*
  - **But**: encrypted communication is unreadable
    - No problem!

- DNS cache poisoning?
  - Client goes to wrong server
  - **But**: detects impersonation
    - No problem!

- Attacker hijacks our connection, injects new traffic
  - **But**: data receiver rejects it due to failed integrity check
    - No problem!
Powerful Protections, cont.

• DHCP spoofing?
  – Client goes to wrong server
  – But: detects impersonation
    • No problem!

• Attacker manipulates routing to run us by an eavesdropper or take us to the wrong server?
  – But: they can’t read; we detect impersonation
    • No problem!

• Attacker slips in as a Man In The Middle?
  – But: they can’t read, they can’t inject
  – They can’t even replay previous encrypted traffic
  – No problem!
Validating Amazon’s Identity, cont.

• Browser retrieves cert belonging to the **issuer**
  – These are hardwired into the browser - **trusted**!

• What if browser can’t find a cert for the issuer?
This Connection is Untrusted

You have asked Firefox to connect securely to www.mikestoolbox.org, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

www.mikestoolbox.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is not trusted.

(Error code: sec_error_untrusted_issuer)

I Understand the Risks

Verify Certificate

Safari can't verify the identity of the website “www.mikestoolbox.org”.

The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be “www.mikestoolbox.org”, which could put your confidential information at risk. Would you like to connect to the website anyway?

Show Certificate  Cancel  Continue
Validating Amazon’s Identity, cont.

- Browser retrieves cert belonging to the **issuer**
  - These are hardwired into the browser - **trusted!**

- What if browser can’t find a cert for the issuer?

- If it can’t find the cert, then warns the user that site has not been verified
  - Note, can still proceed, just **without authentication**

- Q: Which end-to-end security properties do we lose if we incorrectly trust that the site is whom we think?

- **A:** All of them!
  - Goodbye confidentiality, integrity, authentication
  - Active attacker can read everything, modify, impersonate
SSL / TLS Limitations

- Properly used, SSL / TLS provides powerful end-to-end protections

- So why not use it for *everything*??

- Issues:
  - Cost of public-key crypto (fairly minor)
    - Takes non-trivial CPU processing (but today a minor issue)
    - Note: *symmetric* key crypto on modern hardware is non-issue
  - Hassle of buying/maintaining certs (fairly minor)
SSL / TLS Limitations

• Properly used, SSL / TLS provides powerful end-to-end protections

• So why not use it for everything??

• Issues:
  – Cost of public-key crypto (fairly minor)
    o Takes non-trivial CPU processing (but today a minor issue)
    o Note: symmetric key crypto on modern hardware is non-issue
  – Hassle of buying/maintaining certs (fairly minor)
  – Integrating with other sites that don’t use HTTPS
  – **Latency**: extra round trips ⇒ 1st page slower to load
SSL / TLS Limitations, cont.

• Problems that SSL / TLS does not take care of?

• TCP-level denial of service
  – SYN flooding
  – RST injection
    o (but does protect against data injection!)

• SQL injection / XSS / server-side coding/logic flaws

• Vulnerabilities introduced by server inconsistencies
Regular web surfing - http: URL

So *no integrity* - a MITM attacker can alter pages returned by server …

And when we click here … … attacker has changed the corresponding link so that it’s ordinary http rather than https!

We never get a chance to use TLS’s protections! :-(

“sslstrip” attack
SSL / TLS Limitations, cont.

• Problems that SSL / TLS does not take care of?
  • TCP-level denial of service
    – SYN flooding
    – RST injection
      o (but does protect against data injection!)
  • SQL injection / XSS / server-side coding/logic flaws
  • Vulnerabilities introduced by server inconsistencies
  • Browser coding/logic flaws
  • User flaws
    – Weak passwords
    – Phishing
  • Issues of trust …
TLS/SSL Trust Issues

• User has to make correct trust decisions …
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID: [Enter User ID]
I forgot my user ID

Password: [Enter Password]
I forgot my password

[Keep me signed in for today] Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the bidding fun for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Register

Your account

Create a unique password by using a combination of letters and numbers that are not

Having problems with signing in? Get help.

Protect your account

Internet Explorer

When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

- In the future, do not show this message.

Yes No
Please confirm your identity.

Please answer security question!

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another's account you have access to?

What email used to be associated with this account?

Have you ever sold something on eBay?

Do you want to proceed?

Yes  No  View Certificate
Please confirm your identity.

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this account?

Have you ever sold something on eBay?
  ○ No
  ○ Yes

Certificate Information

This certificate is intended for the following purpose(s):
  • Ensures the identity of a remote computer

Issued to: rover.ebay.com

Issued by: VeriSign Class 3 Secure Server CA - G3

Valid from 10/22/2010 to 12/1/2012

Install Certificate...  Issuer Statement
Please confirm your identity.

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this account?

Have you ever sold something on eBay?

- No
- Yes

Certificate

Field | Value
------|------
Version | V3
Serial number | 4d ab c9 a6 0a 30 20 57 f9 23 ...
Signature algorithm | sha1RSA
Issuer | VeriSign Class 3 Secure Server
Valid from | Friday, October 22, 2010 4:00...
Valid to | Saturday, December 01, 2012...
Subject | rover.ebay.com, Site Operatio...
Public key | RSA (1024 Bits)
**Please confirm your identity**

**Please answer security question**

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another email address used to be associated with this account?

Have you ever sold something on eBay?
- No
- Yes

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Alternative Name</td>
<td>DNS Name=rover.ebay.com, ...</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End Entity, Pat...</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Digital Signature, Key Encipher...</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>[1]CRL Distribution Point: Distrib...</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6....)</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>KeyID=0d 4f 5c 16 53 44 c1 ...</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>[1]Authority Info Access: Access...</td>
</tr>
</tbody>
</table>
Please confirm your identity.

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this ac

Have you ever sold something on eBay?
  No
  Yes

Certificate status:

This certificate is OK.

OK
The equivalent as seen by most Internet users:

![Internet Explorer error message](image)

*(note: an actual Windows error message!)*
TLS/SSL Trust Issues, cont.

• “Commercial certificate authorities protect you from anyone from whom they are unwilling to take money.”
  – Matt Blaze, circa 2001

• So how many CAs do we have to worry about, anyway?
## Keychain Access

Click to lock the System Roots keychain.

### Keychains

- login
- Microsoft certificates
- System
- System Roots

### Certificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Expires</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-Trust-nQual-01</td>
<td>certificate</td>
<td>Nov 30, 2014 3:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>A-Trust-nQual-03</td>
<td>certificate</td>
<td>Aug 17, 2015 3:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>A-Trust-Qual-01</td>
<td>certificate</td>
<td>Nov 30, 2014 3:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td><strong>A-Trust-Qual-02</strong></td>
<td><strong>certificate</strong></td>
<td><strong>Dec 2, 2014 3:00:00 PM</strong></td>
<td><strong>System Roots</strong></td>
</tr>
<tr>
<td>AAA Certificate Services</td>
<td>certificate</td>
<td>Dec 31, 2028 3:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AC Raíz Certicámaras S.A.</td>
<td>certificate</td>
<td>Apr 2, 2030 2:42:02 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Class 1 CA Root</td>
<td>certificate</td>
<td>May 30, 2020 3:38:31 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust External CA Root</td>
<td>certificate</td>
<td>May 30, 2020 3:48:38 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Public CA Root</td>
<td>certificate</td>
<td>May 30, 2020 3:41:50 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Qualified CA Root</td>
<td>certificate</td>
<td>May 30, 2020 3:44:50 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Admin-Root-CA</td>
<td>certificate</td>
<td>Nov 9, 2021 11:51:07 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AdminCA-CD-T01</td>
<td>certificate</td>
<td>Jan 25, 2016 4:36:19 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Commercial</td>
<td>certificate</td>
<td>Dec 31, 2030 6:06:06 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Networking</td>
<td>certificate</td>
<td>Dec 31, 2030 6:08:24 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Premium</td>
<td>certificate</td>
<td>Dec 31, 2040 6:10:36 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Premium ECC</td>
<td>certificate</td>
<td>Dec 31, 2040 6:20:24 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>America Online...ation Authority 1</td>
<td>certificate</td>
<td>Nov 19, 2037 12:43:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>America Online...ation Authority 2</td>
<td>certificate</td>
<td>Sep 29, 2037 7:08:00 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AOL Time W...cation Authority 1</td>
<td>certificate</td>
<td>Nov 20, 2037 7:03:00 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AOL Time W...cation Authority 2</td>
<td>certificate</td>
<td>Sep 28, 2037 4:43:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Apple Root CA</td>
<td>certificate</td>
<td>Feb 9, 2035 1:40:36 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Apple Root Certificate Authority</td>
<td>certificate</td>
<td>Feb 9, 2025 4:18:14 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Application CA G2</td>
<td>certificate</td>
<td>Mar 31, 2016 7:59:59 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>ApplicationCA</td>
<td>certificate</td>
<td>Dec 12, 2017 7:00:00 AM</td>
<td>System Roots</td>
</tr>
</tbody>
</table>

**167 items**
TLS/SSL Trust Issues

• “Commercial certificate authorities protect you from anyone from whom they are unwilling to take money.”
  – Matt Blaze, circa 2001

• So how many CAs do we have to worry about, anyway?

• Of course, it’s not just their greed that matters …
Solo Iranian hacker takes credit for Comodo certificate attack

Security researchers split on whether 'ComodoHacker' is the real deal

By Gregg Keizer
March 27, 2011 08:39 PM ET

Computerworld - A solo Iranian hacker on Saturday claimed responsibility for stealing multiple SSL certificates belonging to some of the Web's biggest sites, including Google, Microsoft, Skype and Yahoo.

Early reaction from security experts was mixed, with some believing the hacker's claim, while others were dubious.

Last week, conjecture had focused on a state-sponsored attack, perhaps funded or conducted by the Iranian government, that hacked a certificate reseller affiliated with U.S.-based Comodo.

On March 23, Comodo acknowledged the attack, saying that eight days earlier, hackers had obtained nine bogus certificates for the log-on sites of Microsoft's Hotmail, Google's Gmail, the Internet phone and chat service Skype and Yahoo Mail. A certificate for Mozilla's Firefox add-on site was also acquired.
Solo Iranian hacker takes credit for Comodo certificate attack

Security researchers split on whether 'ComodoHacker' is the real deal

By Gregg Keizer
March 27, 2011 08:39 PM ET

Where did you learn about cryptography and hacking. Are there books in Persian? English books? Or are you self-taught, learning from the Internet?

d) I'm self taught, books in Persian and English, but mostly papers in internet, short papers from experts like Bruce Schneier, RSA people (Ron, Adi and Leonard) and specially David Wagner. I learned programming in Qbasic when I was 9, I started learning cryptography when I was 13

... funded or conducted by the Iranian government, that hacked a certificate reseller affiliated with U.S.-based Comodo.

On March 23, Comodo acknowledged the attack, saying that eight days earlier, hackers had obtained nine bogus certificates for the log-on sites of Microsoft's Hotmail, Google's Gmail, the Internet phone and chat service Skype and Yahoo Mail. A certificate for Mozilla's Firefox add-on site was also acquired.
Fraudulent Google certificate points to Internet attack

Is Iran behind a fraudulent Google.com digital certificate? The situation is similar to one that happened in March in which spoofed certificates were traced back to Iran.

A Dutch company appears to have issued a digital certificate for Google.com to someone other than Google, who may be using it to try to re-direct traffic of users based in Iran.

Yesterday, someone reported on a Google support site that when attempting to log in to Gmail the browser issued a warning for the digital certificate used as proof that the site is legitimate, according to this thread on a Google support forum site.
This appears to be a fully valid cert using normal browser validation rules.

Only detected by Chrome due to its recent introduction of cert “pinning” – requiring that certs for certain domains must be signed by specific CAs rather than any generally trusted CA.
Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company’s certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a

Evidence Suggests DigiNotar, Who Issued Fraudulent Google Certificate, Was Hacked Years Ago

from the diginot dept

The big news in the security world, obviously, is the fact that a fraudulent Google certificate made its way out into the wild, apparently targeting internet users in Iran. The Dutch company DigiNotar has put out a statement saying that it discovered a breach back on July 19th during a security audit, and that fraudulent certificates were generated for “several dozen” websites. The only one known to have gotten out into the wild is the Google one.
TLS/SSL Trust Issues

• “Commercial certificate authorities protect you from anyone from whom they are unwilling to take money.”
  – Matt Blaze, circa 2001

• So how many CAs do we have to worry about, anyway?

• Of course, it’s not just their greed that matters …

• … and it’s not just their diligence & security that matters …
  – “A decade ago, I observed that commercial certificate authorities protect you from anyone from whom they are unwilling to take money. That turns out to be wrong; they don't even do that much.” - Matt Blaze, circa 2010
Law Enforcement Appliance Subverts SSL

By Ryan Singel  |  March 24, 2010 | 1:55 pm | Categories: Surveillance, Threats

That little lock on your browser window indicating you are communicating securely with your bank or e-mail account may not always mean what you think its means.

Normally when a user visits a secure website, such as Bank of America, Gmail, PayPal or eBay, the browser examines the website’s certificate to verify its authenticity.

At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections. To use the appliance, the government would need to acquire a forged certificate from any one of more than 100 trusted Certificate Authorities.
Note: the cert is “forged” in the sense that it doesn’t really belong to Gmail, PayPal, or whomever. But it does not appear forged because it includes a legitimate signature from a trusted CA.
Security Warning: Do you trust the Russian government?

Firefox has detected that your connection to this website is probably not secure. If you are attempting to access or transmit sensitive data, you should stop this task, and try again using a different Internet connection.

Firefox has detected a potential security problem while trying to access www.bankofamerica.com, a website visited at least 131 times in the past by persons using this computer.

In these previous browsing sessions, www.bankofamerica.com provided a security certificate verified by a company in the United States.

However, this website is now presenting a different security certificate verified by a company based in Russia.

If you do not trust the government of Russia with your private data, or think it unlikely that Bank of America would obtain a security certificate from a company based there, this could be a sign that someone is attempting to intercept your secure communications.

Click here to learn more about security certificates and this potentially risky situation.

If you trust the government of Russia and companies located there to protect your privacy and security, click here to accept this new certificate and continue with your visit to the site.

Get me out of here!
**CNNIC ROOT**
Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT

- This certificate is valid

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Expires</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 1 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 1 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 2 Primary CA</td>
<td>certificate</td>
<td>Jul 6, 2019 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 2 Publication Authority</td>
<td>certificate</td>
<td>Aug 2, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 2 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 3 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 3 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 3 Publication Authority</td>
<td>certificate</td>
<td>Aug 2, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 3 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Class 4 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>CNNIC ROOT</td>
<td>certificate</td>
<td>Apr 16, 2027 12:09:14 AM System Roots</td>
<td></td>
</tr>
<tr>
<td>Common Policy</td>
<td>certificate</td>
<td>Oct 15, 2027 9:08:00 AM System Roots</td>
<td></td>
</tr>
<tr>
<td>COMODO Certification Authority</td>
<td>certificate</td>
<td>Dec 31, 2029 3:59:59 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>Deutsche Telekom Root CA 2</td>
<td>certificate</td>
<td>Jul 9, 2019 4:59:00 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>DigiCert Assured ID Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>DigiCert Global Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>DigiCert High Assurance EV Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM System Roots</td>
<td></td>
</tr>
<tr>
<td>DigiNotar Root CA</td>
<td>certificate</td>
<td>Mar 31, 2025 11:19:21 AM System Roots</td>
<td></td>
</tr>
<tr>
<td>DoD CLASS 3 Root CA</td>
<td>certificate</td>
<td>May 14, 2020 6:13:00 AM System Roots</td>
<td></td>
</tr>
<tr>
<td>Certificate Details</td>
<td>Value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CNNIC ROOT</strong></td>
<td>Root certificate authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Expires</strong></td>
<td>Friday, April 16, 2027 12:09:14 AM PT</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>This certificate is valid</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trust</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subject Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td><strong>CN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td><strong>CNNIC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td><strong>CNNIC ROOT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Issuer Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td><strong>CN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td><strong>CNNIC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td><strong>CNNIC ROOT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td><strong>1228079105</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td><strong>3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Not Valid Before</strong></td>
<td>Monday, April 16, 2007 12:09:14 AM PT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CNNIC ROOT

Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT
☑️ This certificate is valid

▼ Trust

When using this certificate: [Use System Defaults] [?] (no value specified)

- Secure Sockets Layer (SSL) (no value specified)
- Secure Mail (S/MIME) (no value specified)
- Extensible Authentication (EAP) (no value specified)
- IP Security (IPsec) (no value specified)
- iChat Security (no value specified)
- Kerberos Client (no value specified)
- Kerberos Server (no value specified)
- Code Signing (no value specified)
- (12840113635100119) (no value specified)
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>no value specified</td>
</tr>
<tr>
<td>Secure Mail (S/MIME)</td>
<td>no value specified</td>
</tr>
<tr>
<td>Extensible Authentication (EAP)</td>
<td>no value specified</td>
</tr>
<tr>
<td>IP Security (IPsec)</td>
<td>no value specified</td>
</tr>
<tr>
<td>iChat Security</td>
<td>no value specified</td>
</tr>
<tr>
<td>Kerberos Client</td>
<td>no value specified</td>
</tr>
<tr>
<td>Kerberos Server</td>
<td>no value specified</td>
</tr>
<tr>
<td>Code Signing</td>
<td>no value specified</td>
</tr>
</tbody>
</table>

**CNNIC ROOT**

Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT

- This certificate is valid

**Trust**

- Use System Defaults
- Always Trust
- Never Trust

(12840113635100119)
CNNIC ROOT
Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT
✓ This certificate is valid

▼ Trust

When using this certificate: Never Trust

Secure Sockets Layer (SSL) Never Trust

Secure Mail (S/MIME) Never Trust

Extensible Authentication (EAP) Never Trust

IP Security (IPsec) Never Trust

iChat Security Never Trust

Kerberos Client Never Trust

Kerberos Server Never Trust

Code Signing Never Trust

( 1 2 840 113635 100 1 19 ) Never Trust
## Keychain Access

**CNNNIC ROOT**

Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT

⚠️ This certificate is marked as not trusted for all users

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Expires</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 1 Publication Authority</td>
<td>certificate</td>
<td>Aug 2, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 1 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 2 Primary CA</td>
<td>certificate</td>
<td>Jul 6, 2019 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 2 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 2 Publication Authority</td>
<td>certificate</td>
<td>Aug 2, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 2 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 3 Publication Authority</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 3 Publication Authority</td>
<td>certificate</td>
<td>Aug 2, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 3 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Class 4 Publication Authority – G2</td>
<td>certificate</td>
<td>Aug 1, 2028 4:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>CNNNIC ROOT</td>
<td>certificate</td>
<td>Apr 16, 2027 12:09:14 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Common Policy</td>
<td>certificate</td>
<td>Oct 15, 2027 9:08:00 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>COMODO Certification Authority</td>
<td>certificate</td>
<td>Dec 31, 2029 3:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Deutsche Telekom Root CA 2</td>
<td>certificate</td>
<td>Jul 9, 2019 4:59:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>DigiCert Assured ID Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>DigiCert Global Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>DigiCert High Assurance EV Root CA</td>
<td>certificate</td>
<td>Nov 9, 2031 4:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>DigiNotar Root CA</td>
<td>certificate</td>
<td>Mar 31, 2025 11:19:21 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>DoD CLASS 3 Root CA</td>
<td>certificate</td>
<td>May 14, 2020 6:13:00 AM</td>
<td>System Roots</td>
</tr>
</tbody>
</table>
Securing DNS Lookups

• Topic for next time: How can we ensure that when clients look up names with DNS, they can trust the answers they receive?
Think about these before Friday

- **Problem 1.** We have a database $D = \{d_1, d_2, \ldots, d_n\}$ of strings. A client anywhere in the world wants to be able to query it with a string $s$ and determine whether $s \in D$; if the answer is “yes”, client should get a proof of this fact. We want to store copies of $D$ on untrusted mirror servers. How do we do it securely?

- **Problem 2.** Same as Problem 1, but now if the answer is “no”, we also want a proof of that fact. How do we do it securely?