CS 5410 - Computer and Network Security: PKI

Professor Patrick Traynor
Fall 2017
Reminders

- Assignment #2 will take a while to be graded.
- Project Ideas due Wednesday
What is a certificate?

• A certificate …
  ▶ … makes an association between a user identity/job/attribute and a private key
  ▶ … contains public key information \{e,n\}
  ▶ … has a validity period
  ▶ … is signed by some certificate authority (CA)

• Issued by CA for some purpose
  ▶ Verisign is in the business of issuing certificates
  ▶ People trust Verisign to vet identity
Example
Why do I trust the certificate?

- A collections of “root” CA certificates
  - … baked into your browser
  - … vetted by the browser manufacturer
  - … supposedly closely guarded (yeah, right)

- Root certificates used to validate certificate
  - Vouches for certificate’s authenticity

CA (signs) Certificate
Signature
# Root Certificates

![Keychain Access](image)

## A-Trust-nQual-03
- **Root certificate authority**
- Expires: Monday, August 17, 2015 at 6:00:00 PM Eastern Daylight Time
- This certificate is valid

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Date Modified</th>
<th>Expires</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-Trust-nQual-03</td>
<td>certificate</td>
<td>--</td>
<td>Aug 17, 2015, 6:00:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AAA Certificate Services</td>
<td>certificate</td>
<td>--</td>
<td>Dec 31, 2028, 6:59:59 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AC Raiz Certímaca S.A.</td>
<td>certificate</td>
<td>--</td>
<td>Apr 2, 2030, 5:42:02 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Actalis Authentication Root CA</td>
<td>certificate</td>
<td>--</td>
<td>Sep 22, 2030, 7:22:02 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Class 1 CA Root</td>
<td>certificate</td>
<td>--</td>
<td>May 30, 2020, 6:38:31 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust External CA Root</td>
<td>certificate</td>
<td>--</td>
<td>May 30, 2020, 6:48:38 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Public CA Root</td>
<td>certificate</td>
<td>--</td>
<td>May 30, 2020, 6:41:50 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AddTrust Qualified CA Root</td>
<td>certificate</td>
<td>--</td>
<td>May 30, 2020, 6:44:50 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Admin-Root-CA</td>
<td>certificate</td>
<td>--</td>
<td>Nov 10, 2021, 2:51:07 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AdminCA-CD-T01</td>
<td>certificate</td>
<td>--</td>
<td>Jan 25, 2016, 7:36:19 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Commercial</td>
<td>certificate</td>
<td>--</td>
<td>Dec 31, 2030, 9:06:06 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Networking</td>
<td>certificate</td>
<td>--</td>
<td>Dec 31, 2030, 9:08:24 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Premium</td>
<td>certificate</td>
<td>--</td>
<td>Dec 31, 2040, 9:10:36 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AffirmTrust Premium ECC</td>
<td>certificate</td>
<td>--</td>
<td>Dec 31, 2040, 9:20:24 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>America Online...ation Authority 1</td>
<td>certificate</td>
<td>--</td>
<td>Nov 19, 2037, 3:43:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>America Online...ation Authority 2</td>
<td>certificate</td>
<td>--</td>
<td>Sep 29, 2037, 10:08:00 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AOL Time Wa...ation Authority 1</td>
<td>certificate</td>
<td>--</td>
<td>Nov 20, 2037, 10:03:00 AM</td>
<td>System Roots</td>
</tr>
<tr>
<td>AOL Time Wa...ation Authority 2</td>
<td>certificate</td>
<td>--</td>
<td>Sep 28, 2037, 7:43:00 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>Apple Root CA</td>
<td>certificate</td>
<td>--</td>
<td>Feb 9, 2035, 4:40:36 PM</td>
<td>System Roots</td>
</tr>
<tr>
<td>And Root CA</td>
<td>certificate</td>
<td>--</td>
<td>Jan 26, 2035, 3:18:08 AM</td>
<td>System Roots</td>
</tr>
</tbody>
</table>

Florida Institute for Cybersecurity (FICS) Research
Public Key Infrastructure

• System to “securely distribute public keys (certificates)”
  ▶ Q: Why is that hard?

• Terminology:
  ▶ Alice signs a certificate for Bob’s name and key
    ▶ Alice is issuer, and Bob is subject
  ▶ Alice wants to find a path to Bob’s key
    ▶ Alice is verifier, and Bob is target
  ▶ Anything that has a public key is a principal
  ▶ Anything trusted to sign certificates is a trust anchor
    ▶ Its certificate is a root certificate
What is a PKI?

- Rooted tree of CAs
- Cascading issuance
  - Any CA can issue cert
  - CAs issue certs for children
Certificate Validation

Certificate Validation Diagram:

Root

CA1

CA11 CA12 CA1n

CA2

CA21

CA3

CA22

Certificates:

Cert11a Cert11b Cert11c

Signature:
Cross Validation

Root 1  Root 2

CA 1  CA 2

User 1  User 2
PKI and Revocation

- Certificate may be revoked before expiration
  - Lost private key
  - Compromised
  - Owner no longer authorized

- Revocation is hard …
  - The “anti-matter” problem
  - Verifiers need to check revocation state
    - Loses the advantage of off-line verification
  - Revocation state must be authenticated
OCSP

User — Server

Connect
Certificate

Certificate Status
Good, Revoked, Unknown

CA
10 Risks of PKI

- This is an overview of one of many perspectives of PKI technologies
  - PKI was, like many security technologies, claimed to be a panacea
  - It was intended to solve a very hard problem: build trust on a global level
  - Running a CA -- “license to print money”

- Basic premise:
  - Assertion #1 - e-commerce does not need PKI
  - Assertion #2 - PKI needs e-commerce

- Really talking about a full PKI (everyone has certs.)
Risk 1 - Who do we trust, and for what?

- Argument: CA is not inherently trustworthy
  - Why do/should you trust a CA?
  - In reality, they defer all legal liability for running a bad CA
  - Risk in the hands of the certificate holder

- Counter-Argument: Incentives
  - Any CA caught misbehaving is going to be out of business tomorrow
  - This scenario is much worse than getting sued
  - Risk held by *everybody*, which is what you want

- Everyone has reason to be diligent
Risk 2 - Who is using my key?

• Argument: key is basically insecure
  ▶ Your key is vulnerable, deal with it
  ▶ In some places, you are being held responsible after a compromise

• Counter-Argument: this is the price of technology
  ▶ You have to accept some responsibility in order to get benefit
  ▶ Will encourage people to use only safe technology

• Q: what would happen is same law applied to VISA?
Aside: TEMPEST

- Transient Electromagnetic Pulse Surveillance Technology
  - Monitor EMF emanations to reconstruct signal
  - For example, a video monitor normally exist at around 55-245 MHz, and can be picked up as far as one kilometer away.
  - ... or by a guy in a van across the street, e.g., steal private key.
- Generally, this is the domain of spy/national security issues
- Much classified work on signal eavesdropping and prevention
Risk 3 - How secure is the verif(ier)?

- Argument: the computer that verifies your credential is fundamentally vulnerable
  - Everything is based on the legitimacy of the verifier root public key (integrity of certificate files)
  - Browsers transparently use certificates
- Counter-Argument: this is the price of technology
  - You have to accept some *risk* in order to get benefit
  - Will encourage people to use only safe technology
- Q: What’s in your browser?
An Aside...
Risk 4 - Which John Robinson is he?

• Argument: identity in PKI is really too loosely defined
  ▶ No standards for getting credential
  ▶ No publicly known unique identifiers for people
  ▶ So, how do you tell people apart

• Counter-Argument: due diligence
  ▶ Only use certificates in well known circumstances
  ▶ When in doubt, use other channels to help

• Q: Is this true of other valued items (checks?)
Risk 5 - Is the CA an authority?

- Argument: there are things in certificates that claim authenticity and authorization of which they have no dominion
  - “rights” (such as the right to perform SSL) - this confuses authorization authority with authentication authority
  - DNS, attributes -- the CA is not the arbiter of these things

- Counter-Argument: this is OK, because it is part of the implicit charge we give our CA -- we implicitly accept the CA as authority in several domains
Risks 6 and 7

6: Is the user part of the design?
   • Argument: too many things hidden in use, user has no ability to affect or see what is going on
   • Counter-Argument: too sophisticated for user to understand
   • Ex.: Hosted website has cert. of host(er), not page

7: Was it one CA or CA+RA?
   • Argument: separation of registration from issuance forgery
     • e.g., RA handles vetting, CA makes certificates, so, you better have good binding between these entities or bad things can happen
   • Counter-Argument: this is an artifact of organization, only a problem when CA is bad (you are doomed anyway)
Risks 8 and 9

8 : How was the user authenticated?
   - Argument: CAs do not have good information to work with, so real identification is poor (as VISA)
   - Counter-Argument: It has worked well in the physical work, why not here?

9 : How secure are the certificate practices?
   - Argument: people don’t use them correctly, and don't know the implications of what they do use
   - Point in fact: revocation and expiration are largely ignored in real system deployments
   - Counter-Argument: most are pretty good now, probably won't burn us anytime soon
Risk 9 - How secure cert. practices?

• Argument: certificates have to be used properly to be secure
  ▶ Everything is based on the legitimacy of the verifier root public key, protection of its key
  ▶ Lifetime & revocation have to be done

• Counter-Argument: this is the price of technology
  ▶ You have to accept some risk in order to get benefit
  ▶ Will encourage people to use only safe technology

• Q: What’s in your browser?
Risk 10 - Why are we using PKI?

• Argument: We are trying to solve a painful problem: authenticating users.
  ▶ However, certificates don’t really solve the problem, just give you another tool to implement it
  ▶ Hence, it is not a panacea
  ▶ Has not delivered on its promises

• Counter-argument?
Resource PKI (RPKI)

- CA infrastructure may be a necessary part of securing the Internet (i.e., BGPSEC).
- The Resource PKI (RPKI) was developed for BGP and allows autonomous systems (ASes)
  - ARIN offers both Hosted RPKI and Delegated RPKI.
- Regional Internet Registries (RIRs) serve as the root for every AS.
- What problems does this model fix? Ignore?
Burning question ...

• Can we solve the PKI problem with better crypto?
Identity Based Cryptography

- What if your email address was your public key?
  - E.g., $E(\text{traynor@cise.ufl.edu}, \text{data}) = \text{ciphertext}$
  - E.g., $\text{Verify( signature, traynor@cise.ufl.edu )}$

- 1984 - Shamir asked for such a system, but it (largely) remained out of reach until Boneh/Franklin 2001
  - The public key is any arbitrary string
  - Based on “Weil pairings” -- a new cryptographic device with lots and lots of uses (IBE among them)

- Advances from theory community, few systems
IBE System

• Functionally, you receive your private key from a trusted third party who is responsible for generating all keys in the system.

• Thereafter you (and others) can use the system as if you generated the private key yourself.

• Advantages
  • No public key distribution
  • No name binding problems (?)
  • Key space flexibility
  • Others?
Basic IBE Construction

- **Setup** (generate by TTP)
  
  \[ \text{Global Parameters} = G \]
  
  \[ \text{Master Key} = K_G \]

- **Extract** (by TTP for user, sting “str”)
  
  \[ \text{Extract}(G, K_G, Str) = K_{Str}^- \]

- **Encrypt** (by user)
  
  \[ E(G, Str, \text{data}) = \text{ciphertext} \]

- **Decrypt** (by user)
  
  \[ D(G, K_{Str}^-, \text{ciphertext}) = \text{data} \]
IBE Reality

- Many thought that IBE would lead to a revolution in public key system (solve PKI problems), it didn't.

- Why - IBE moves the problems around
  - Is there any TTP that everyone trusts?
  - String ambiguity is still a problem? (John Robinson?)
  - Revocation is still a problem (potentially worse)
  - ... (see 10 reasons above)

- Fundamentally
  - IBE really does not solve the CA problem, as the TTP is fulfilling that role.
  - Having strings instead of obscure numbers does not get at the problems with PKI ...
  - Existence of certificates is not really the problem ...
A thought...

• Can we build secure systems without a centralized authority?
SDSI/SPKI

- Two parallel efforts to solve this problem
  - SDSI: Simple Distributed Security Infrastructure
  - SPKI: Simple Public Key Infrastructure
- Not widely used

- In SDSI/SPKI, principals/organizations declare groups of keys that they use for communicating with others

- To find a key for “Luis Vargas” (my student), instead of searching for Luis’ key and seeing who claimed to sign it, you would look for “Patrick Traynor’s Keys” and find the listings for his colleagues and students.
Pretty Good Privacy

• PGP: Developed by Phil Zimmerman in 1992
  • Widely used

• Suppose Alice Knows Bob. If Bob makes his key public, Alice can sign it after Bob proves his identity.

• Charlie can look up Bob’s key in a directory
  • If Charlie knows Alice’s key, he can trust using Bob’s key

• PGP uses a web of trust: instead of PKI tree, we have a PKI graph.
  • We can trust a key declaration if there is one or more trusted graph traversals
Problems with distributed models

- Key Distribution?
- Strangers?
- General Usability?