The Holy Grail of Cryptography

Or the power of client certificates

By Guido Witmond
At BruCON 2013.

Holy Grail

The Holy Grail of Cryptography

Is to know WHO you are talking to.

Or you may talk encrypted
to the wrong person: MitM, Phishing.
Not a secure channel.

Person-to-Person Authentication

It's easy:

- Meet in person;

  You have a secure channel.

- Agree on a shared secret;

  You can recognise/authenticate the other later.

Remote Authentication of friends

Send your public key in non-secure email;

- Receive their key in return;

- Setup an encrypted video channel with
  - Their not-trusted key and your own private key.
- Validate by voice/face recognition

  And fingerprint reading.
  - Now you know that the key you received belongs to them.

How to Authenticate Strangers

- Who have never met in person;
- Who don't know anything about the other.

- Can they set up a secure channel?

  Is that possible?
- In real life: It's called a blind date.
- But online?

Authenticate Strangers Anonymously

Let's up the ante.

We will authenticate them to each other:

- Completely anonymously!

  They will be able to communicate securely

    Without knowing WHO the other one is.

- Even anonymous to us.

    We don't learn their identities either.

Answer this question first

Q: Why would two total strangers ...

… WANT to exchange keys and authenticate?

A: They WON'T.

- Unless they find something in common.

Something in common

Let's give em that.

- We run our blog site.

  Person 1 has a blog, full of articles.

- Person 2 comes across the blog (search)

  and finds it interesting.

Private message

Person 2 wants to send a private message to Person 1.

- Were we a normal blog site, we could read that message as we transmit it.
- Person 2 doesn't want us to read it.
  - It's a private message.

- There is our use case!

Client certificates

- We only accept client certificates to log in
  - No passwords; no email addresses
- We run our own CA; we trust no one (else)
- A Certificate is:
  - A user's public key; from a new key pair;
  - A user chosen nick name; not their real name;
  - Signed into certificate with our CA's private key;
  - Binding all three together.

Signed blogs

- Bloggers sign their blog with their private keys.
  - Before they submit it to our site.
  - We publish the signature alongside the blog text.
- Readers can verify the signature
  - It proves authenticity of the blog;
  - Validates the public key of the writer;
  - You know WHO wrote it
    - The owner of the private key; Whoever that may be.

Private messages

- Person 2 encrypts the message
  - On their own computer;
  - With the validated public key of Person 1;
  - Only the owner of the private key can decrypt it.
  - Only Person 1. No one else. Not even us.

- But, how does the message get to Person 1?
  - A public key is not an email address.

Message delivery

- Our site will do message transport.
  - But we require a certificate to log in.
- Person 2 requests a certificate
  - With a chosen nick name;
  - Public key from a newly generated key pair
- Person 2 signs the encrypted message
  - And hands that to the site for delivery.

Receiving the message

Person 1 logs in, receives the message;

- Decrypts it with their private key;
- Reads the message.
- Validates the signature
- It's from someone at the blog site;
- Called Person 2

- Person 1 has all that's needed to write a reply.
  - A validated public key and our site to deliver it.

Going independent

So far, our site did the message transport.

- What if one of them wrote:

  “Call me at https://1.2.3.4:port/

  Expect me to use my certificate from here.

  Please use your certificate as well.”

- They've created an independent channel.
  - We can not prevent. Nor know about.

Our site is not needed anymore

- With that independent channel:
  - They don't need our site anymore.
  - Nor do they need our CA.
  - We can get hacked, bankrupt, nuked from orbit.
- All they need is a channel
  - And their validated public keys;
  - To prove their identities to each other.
- Our site goes away, their identities live on.

Q.E.D.

What we did:

- Introduce strangers;
- Who publish signed messages;
- With signature to validate public keys;
- Use that public key to encrypt messages;
- Creating a secure channel between them;
- Without revealing any real identities.

Advanced use of Local CA

- Site uses server certificate signed by local CA
- Clients only use client certificates that match the server certificate at connection time.
- Phishers can duplicate the site's look;

  But not our server certificate.
- Nor will we ever sign one for them.

- Our clients are protected against Phising

Demo time

- I'll be playing person 1 and 2

Being Subversive

- By watching this demo

  Of me creating client certificates,
- You've implicitly authenticated these:
  - Person-1@@cryptoblog.wtmnd.nl
  - Person-2@@cryptoblog.wtmnd.nl

  These are mine.

- Feel free to send encrypted messages.

Here's the site

Http://eccentric-authentication.org

Look for the “Run it yourself” blog entry.

Questions?

Don't trust me

Visitors have to trust me that I (site operator) do not MitM them.

- Visitors are urged to submit their client certificate to the Registry of Dishonesty

  It records all certificates for each nick name,
- There should be only one for each nick.
- Inspiration: Perspectives; Convergence; Certificate Transparency.