University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 4-2

Topic: PKI

Presenter: Matt Niemiec

MitM

Man in the Middle

- There are MANY attacks on cryptography
  - MitM is one of the biggest ones
- When we think about internet communications, assume that the adversary:
  - Can see everything you do
  - Can stop your messages from arriving
  - Can spoof your IP address and other credentials
  - Is basically Comcast

The Internet

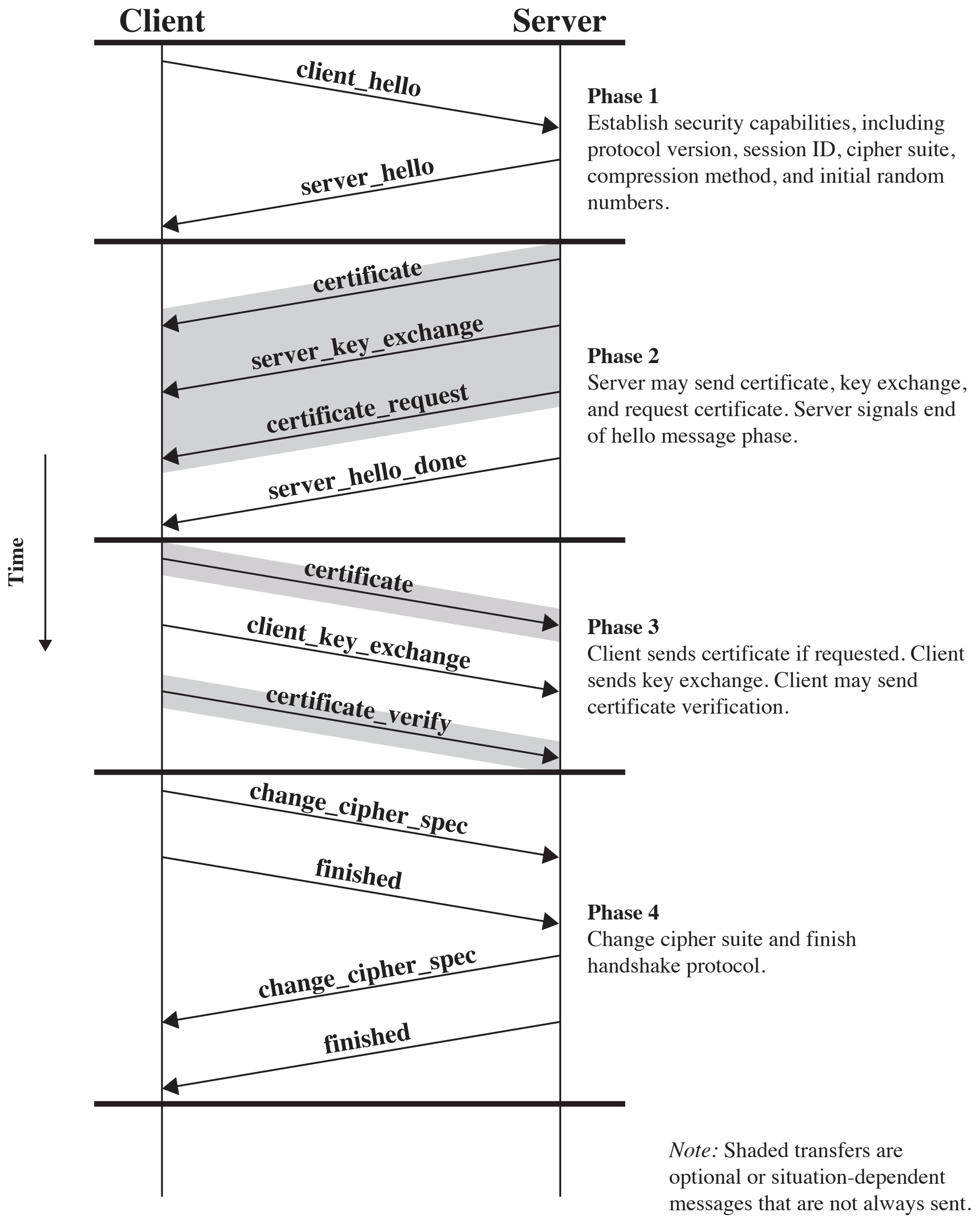
- How can we possibly know who we’re talking to?
  - Distribute keys personally (not feasible)
  - How else?

SSL?

What is Secure Socket Layer (SSL)?

- Came onto the encryption scene in 1995 with SSL 2.0
  - SSL 1.0 was so bad it was never released
- SSL 2.0 was replaced by SSL 3.0 in 1996
- SSL 3.0 is the most modern version of SSL
  - Released in 1996

SSL Process



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

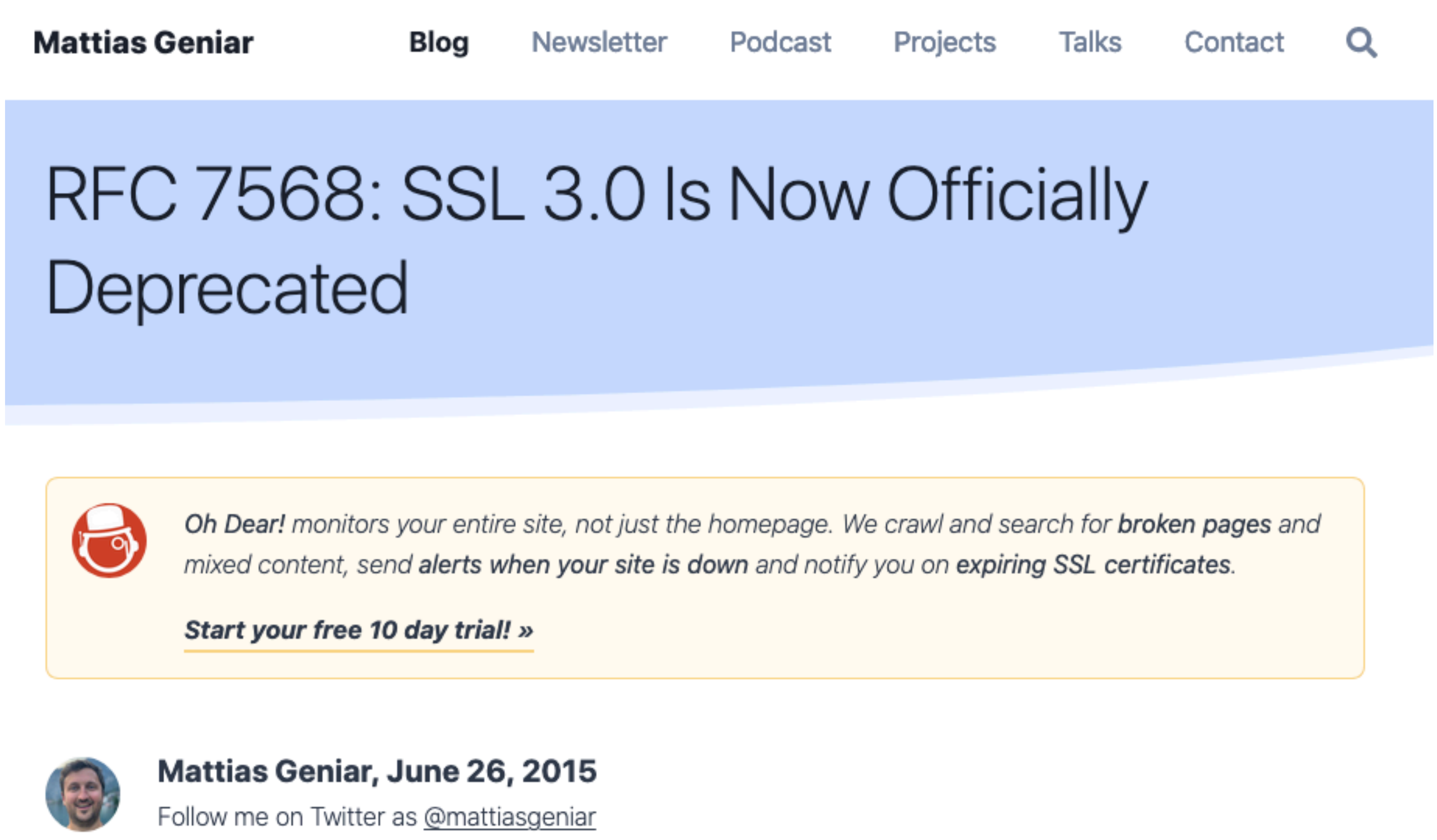
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 22.6 Handshake Protocol Action



Mattias Geniar Blog Newsletter Podcast Projects Talks Contact

RFC 7568: SSL 3.0 Is Now Officially Deprecated

Mattias Geniar, June 26, 2015

Follow me on Twitter as @mattiasgeniar

Transport Layer Security (TLS)

- Superseded SSL 3.0 in 1999
  - A long time ago!
  - Why did we mention SSL?!
- TLS v1.1 published at some point
- Today: use TLS v1.2 or TLS v1.3
- Don’t use SSL!

HTTP over SSL (HTTPS)

HTTPS

- Is just HTTP over SSL. That's all
- Encrypts the following:
  - URL of the encrypted document
  - Contents of the document
  - Contents of browser forms
  - Cookies sent back and forth
  - Contents of HTTP header

HTTPS

- It does NOT encrypt:
  - Source IP address (your location)
  - Destination IP address (who you're talking to)
  - The type of traffic (port numbers, etc.)
  - The length of the packet

Still one problem...

- Never addressed the Man in the Middle attack!

Public Key Infrastructure (PKI)

Proving Identity

What Is PKI?

- The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography

PKI: Somebody Else Vouches for us

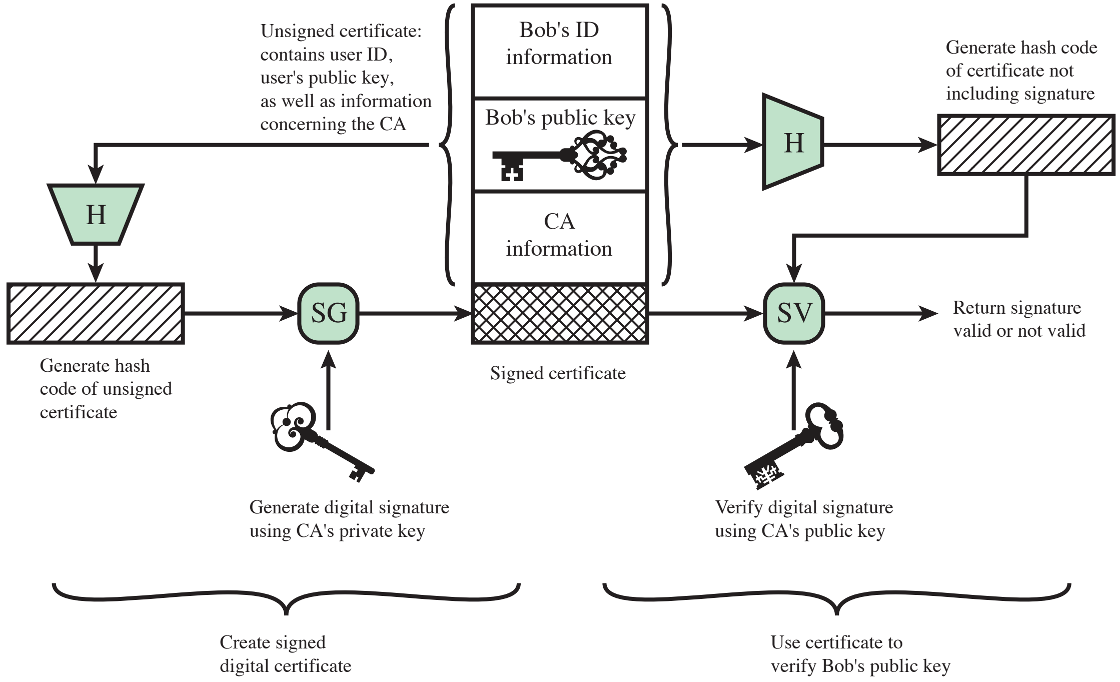


Figure 2.8 Public-Key Certificate Use

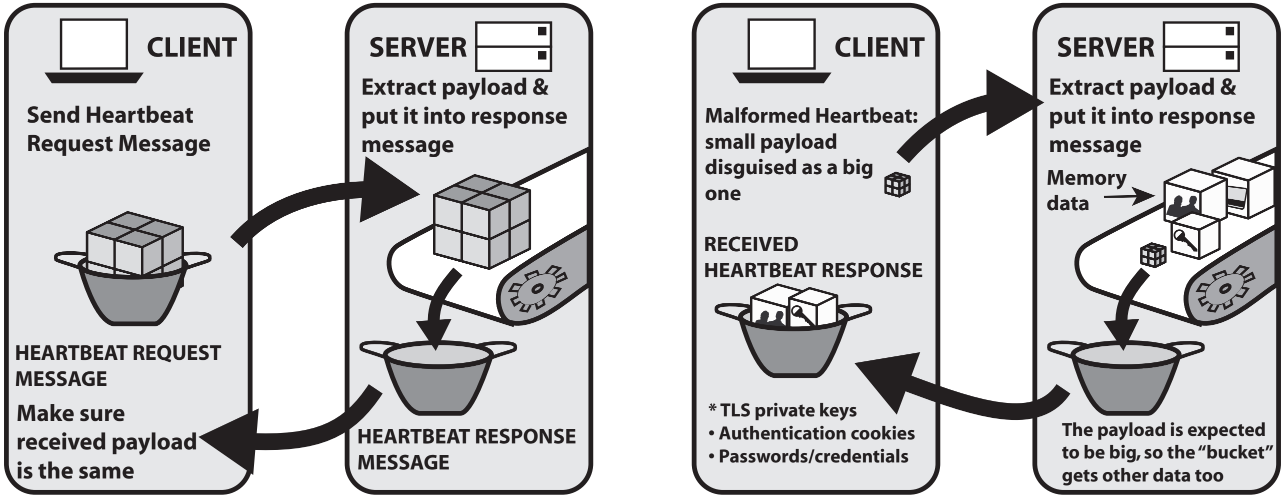
Authenticating Server

- Create a cert
  - As simple as ssh-keygen
- Create a Certificate Signing Request (CSR)
- Have the server sign it
- Install your certificate into Apache

Seeing Certificates

Attacks on SSL

Attacks on the SSL Implementation



CLIENT
Send Heartbeat Request Message
HEARTBEAT REQUEST MESSAGE
Make sure received payload is the same
SERVER
Extract payload & put it into response message
HEARTBEAT RESPONSE MESSAGE
CLIENT
Malformed Heartbeat: small payload disguised as a big one
RECEIVED HEARTBEAT RESPONSE
* TLS private keys
• Authentication cookies
• Passwords/credentials
SERVER
Extract payload & put it into response message
Memory data
The payload is expected to be big, so the "bucket" gets other data too

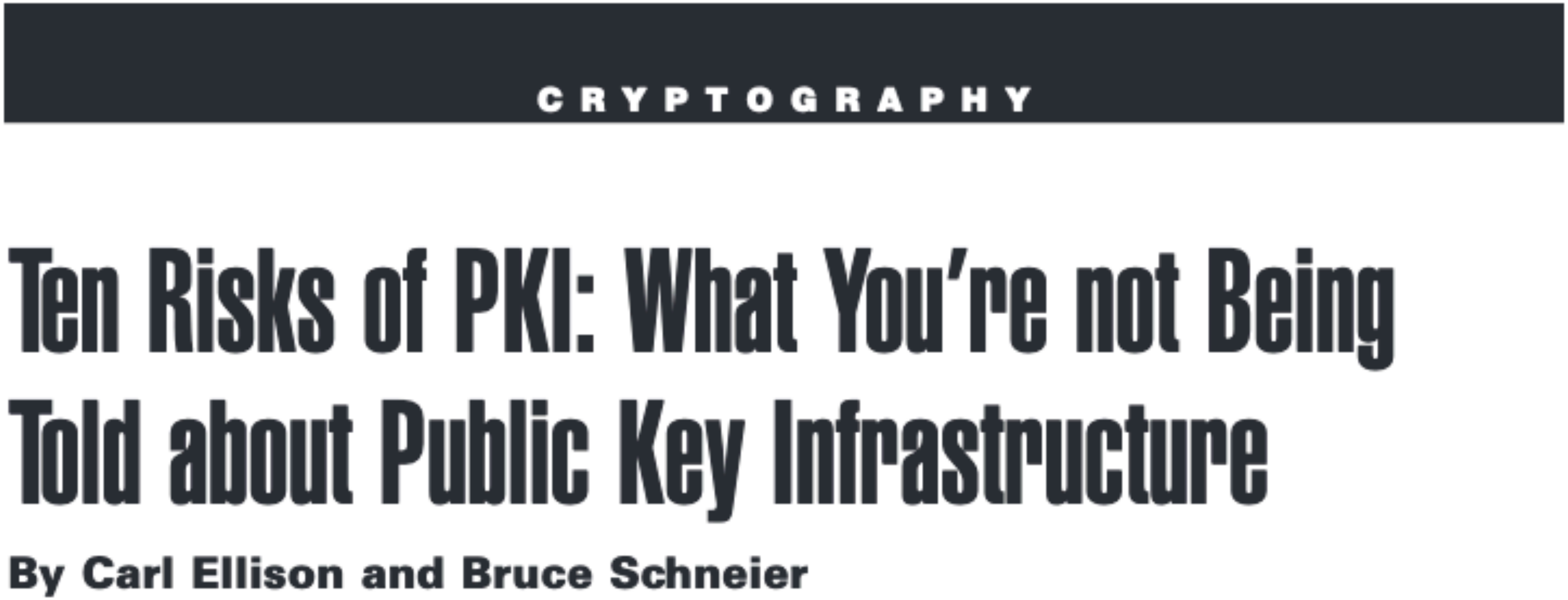
(a) How TLS Heartbeat Protocol works

(b) How TLS Heartbleed exploit works

Figure 22.7 The Heartbleed Exploit
Source: BAE Systems

SSL Strip

- How do we know the website we want uses HTTPS?
- A MitM can return the HTTP connection
- Solution: https://hstspreload.org/



CRYPTOGRAPHY

Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure

By Carl Ellison and Bruce Schneier

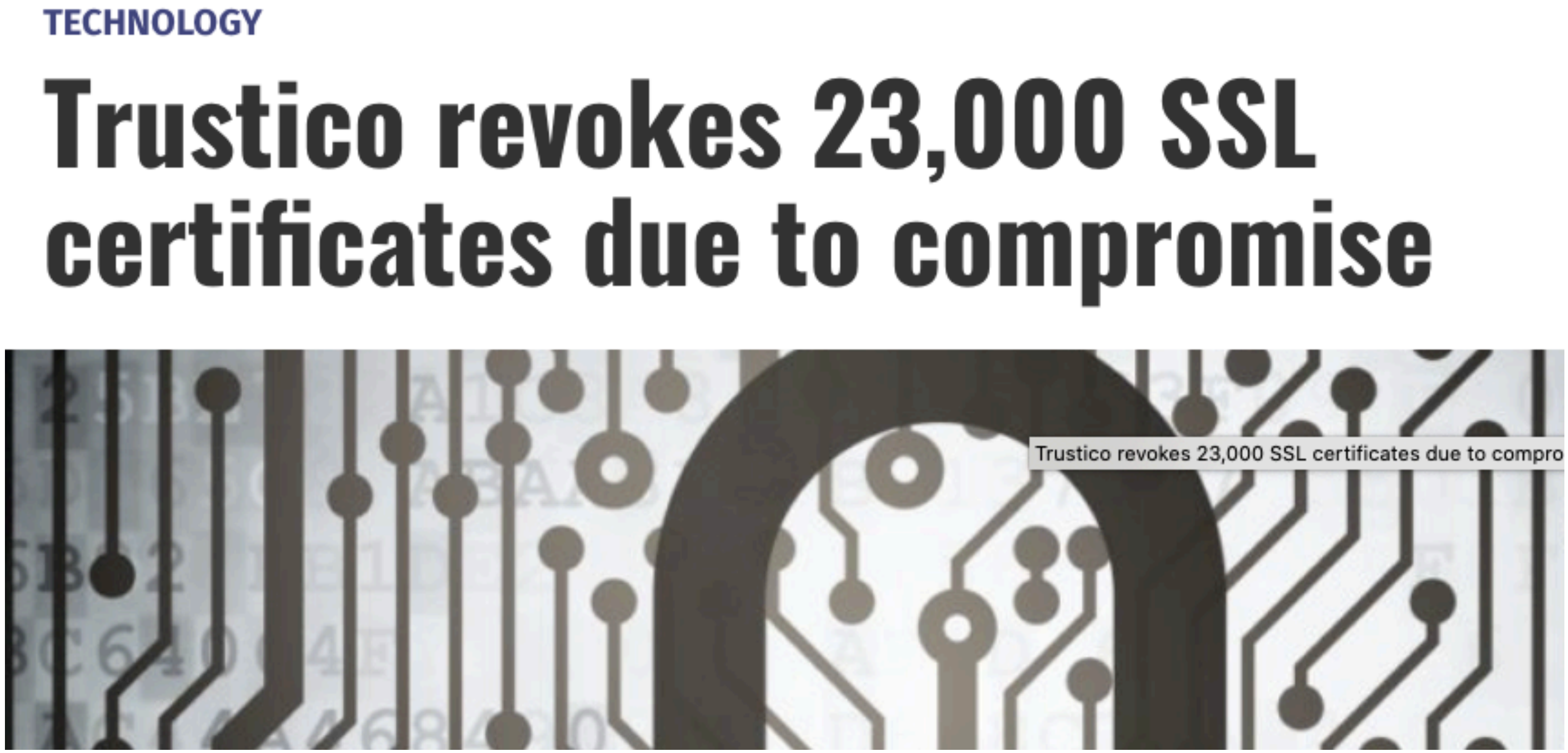
Can We Trust the CA?

- If so, what do we trust them to do?
- Nobody gave them a license
    - Anybody can generate an SSL certificate – you will!
- The CA is not the authority on my domain name
- Identification practices are not always secure

Example

VeriSign Hit by Hackers in 2010

Example



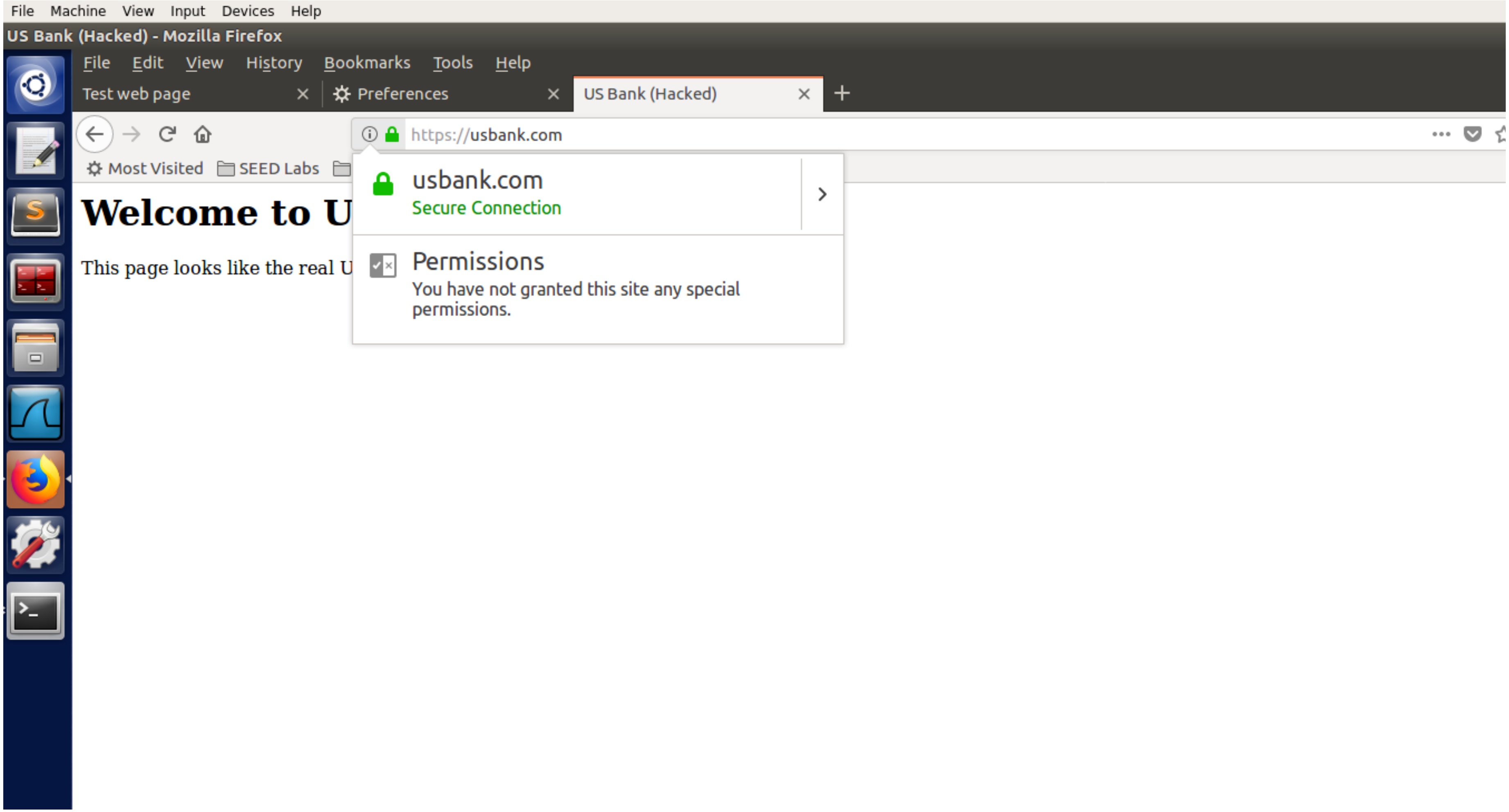
TECHNOLOGY

Trustico revokes 23,000 SSL certificates due to compromise

Trustico revokes 23,000 SSL certificates due to compro

Is the User Part of the Security Design?

- Is the user’s computer secure?
    - Are they running (up-to-date) antivirus?
    - Has their computer been compromised
- Do you check the green lock?
- Have you ever ignored the browser’s warning?
    - That site looked really helpful from Google!
- Do you ever check who signed the certificate you’re using?
    - Was it DigiCert? Sectigo? TUBITAK Kamu SM SSL Kok?



File Machine View Input Devices Help
US Bank (Hacked) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Test web page
Preferences
US Bank (Hacked)
https://usbank.com
Most Visited
SEED Labs

Welcome to U

This page looks like the real U

usbank.com

Secure Connection

Permissions

You have not granted this site any special permissions.

Certificate Revocation

- What happens when a certificate is compromised?
- Some reasons for revocation
  - Key compromise
  - CA compromise
  - Affiliation changed
  - Cessation of operation
  - Certificate hold
  - Privilege withdrawn

Certificate Revocation Lists (CRL)

- Make HTTPS query to CRL
- Very difficult to maintain
- Bulky
- Not very timely

Happy browsing!