CSE 484 / CSE M 584
Computer Security: SSL/TLS

TA: Adrian Sham

adrsham@cs

Original slides from Franzi

Logistics

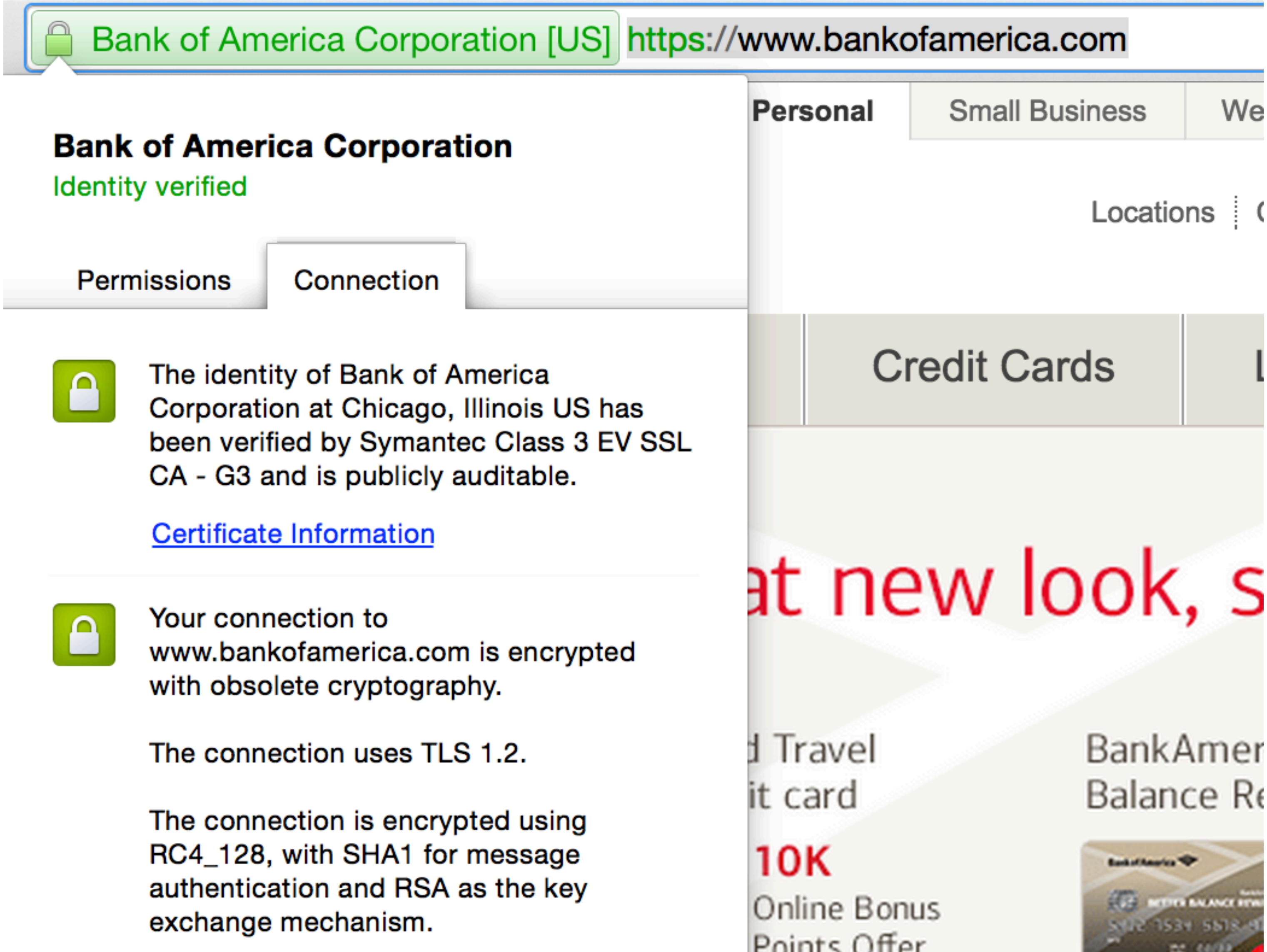
- Lab 1 Final due TOMORROW (5pm).
- Office hours: Friday, 9:30-10:30am, CSE 218
- For quickest response from TAs before 5pm tomorrow, email all of us:

  cse484-tas@cs.washington.edu
- Homework #2 out now (crypto), due on Friday, 5/8, 5pm.

SSL/TLS in an encrypted nutshell

- Used to provide security over a insecure network
- SSL originally developed by Netscape, SSL 3.0 released 1996
- TLS 1.2 is the latest standard defined 2008

Snapshot from chrome



Bank of America Corporation

Identity verified

Permissions | Connection

The identity of Bank of America Corporation at Chicago, Illinois US has been verified by Symantec Class 3 EV SSL CA - G3 and is publicly auditable.

Certificate Information

Your connection to www.bankofamerica.com is encrypted with obsolete cryptography.

The connection uses TLS 1.2.

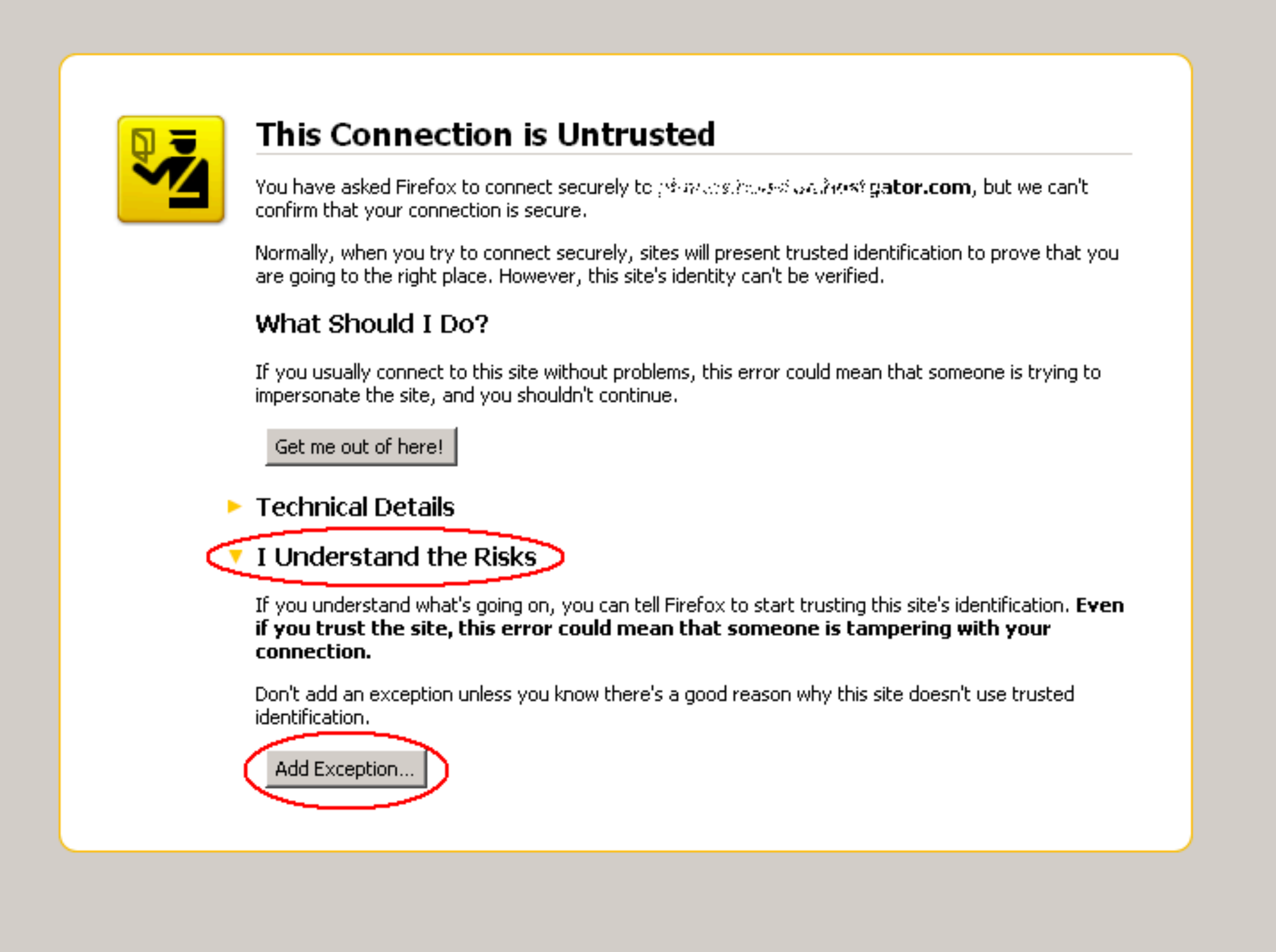
The connection is encrypted using RC4_128, with SHA1 for message authentication and RSA as the key exchange mechanism.

Security in SSL/TLS

- Building a secure system is complex, things can go wrong.
- Computers get more powerful, attackers get smarter.
- What are the some of the attack vectors?
  - User
  - Browser
  - Crypto library
  - Server
  - Certificate Authority

User

- Browser warnings often ignored



This Connection is Untrusted

You have asked Firefox to connect securely to [redacted]gator.com, 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?

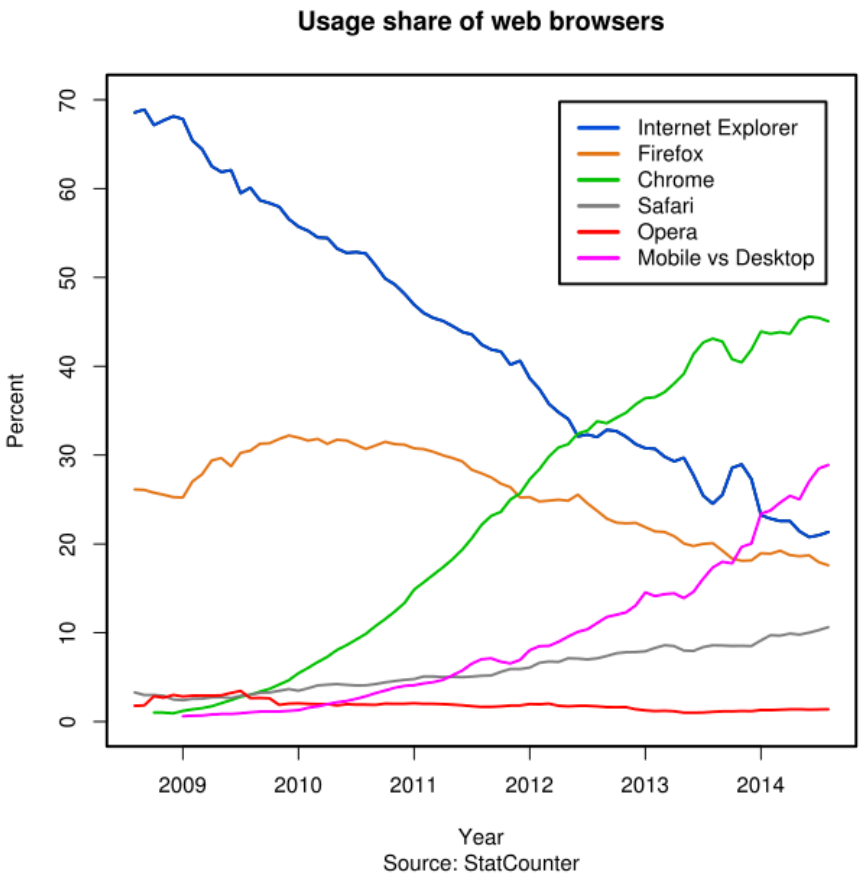
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

User

- Outdated browsers



2015 March	% Usage
Chrome	63.7%
IE	7.7%
Firefox	22.1%
Safari	3.9%
Opera	1.5%

Wikipedia

http://www.w3schools.com/browsers/browsers_stats.asp

SSL User Interface Attacks

[Figures thanks to Elie Bursztein]

SSL User Interface Attacks

[Figures thanks to Elie Bursztein]

SSL User Interface Attacks

[Figures thanks to Elie Bursztein]

SSL Strip Attack

[Figures thanks to Elie Bursztein. See also http://www.thoughtcrime.org/software/sslstrip/.]

SSL Strip Attack

[Figures thanks to Elie Bursztein. See also http://www.thoughtcrime.org/software/sslstrip/.]

SSL Strip Attack

- Mitigated by HTTP Strict Transport Security (HSTS), which tells the web browser to use only https
- If user visiting site the first time, this may be intercepted
- Modern browsers “pre-loaded” with list of HSTS sites

Certificate Authority

- A group of companies responsible for certifying public keys
- Browsers pre-configured with 100+ trusted CAs
- If public key is signed by one of these CAs and common name matches domain name, certificate is accepted

Can you trust the certificates?

- CAs can also be hacked, and issue rogue certificates
- Breaches allowed fraudulent issue of certificates for domains like mail.google.com
- Secret keys used to identify service providers can be stolen, such as due to Heartbleed
- Certificate Revocation Lists can help

Certificate Transparency

- Developed by Ben Laurie and Adam Langley in response to DigiNotar intrusion
- Allows for the monitoring of SSL certificate issued by CAs either by mistake or maliciously acquired
- Allows owner of domain to monitor certificates being issued

Software

- Server side software may be difficult to configure
- Cryptographic libraries may have bugs

Debian OpenSSL PRNG bug

- Following lines removed

```
MD_Update(&m, buf, j); /*Purify complains*/
```

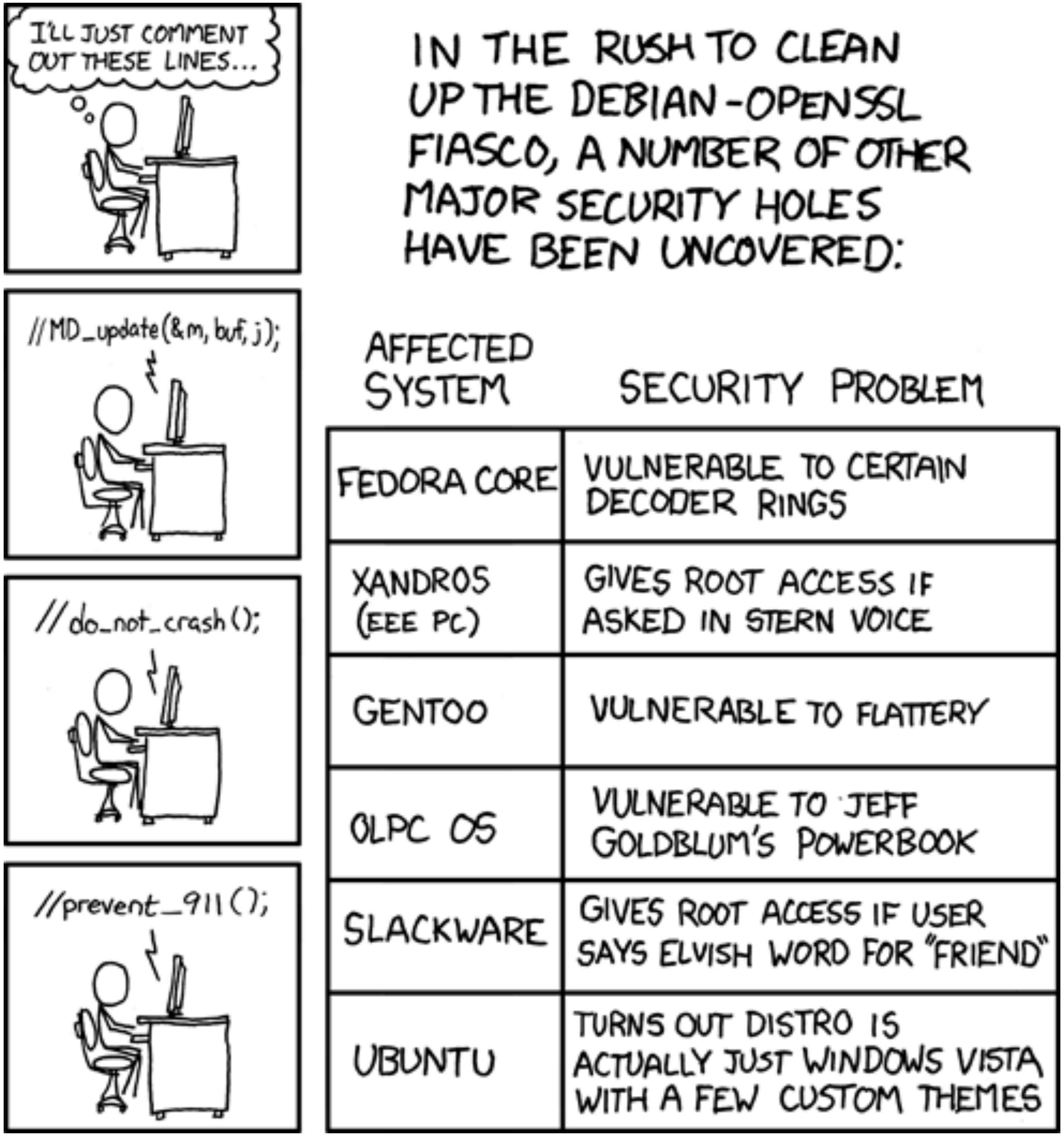
- Due to warnings from Valgrind and Purify about uninitialized data
- Result: the only random value used is the process id, with a max of 32,768

Forward secrecy

- What happens if your private key is compromised?
- Use algorithms with forward secrecy
- Prevents attacker from using stolen private key to decrypt previous communications
- Example: RSA with DHE

Some tools

- SSL Server Test : www.ssllabs.com/ssltest/
- Performs an analysis of the configuration of SSL web server
- Tells you which browser is supported with your crypto choices
- SSLMate: sslmate.com
- Automate certificate renewal/issuance from command line



IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

http://xkcd.com/424/