# Web Security
# (CSC309, Nov. 16/17 2016)

Irving Reid, PagerDuty
irving@pagerduty.com

# This stuff matters.

Getting hacked is no fun.

- Wastes your time cleaning up
- Reputation damage to you, your employer, your users
- Financial damage to the same list
- Stolen information can be used in attacks elsewhere
- Your site could end up hosting malware

# You won’t escape.

- People are constantly scanning for vulnerable servers
- Looking for unpatched systems, trying hacks
- Some exploits fully automated, others followed up by humans

# Goals

Confidentiality

- the correct people have access to information

Integrity

- the information is reliable

Availability

- users can accomplish their tasks

***Risks*** are bad things that could happen:

- Financial
- Reputation
- Physical harm

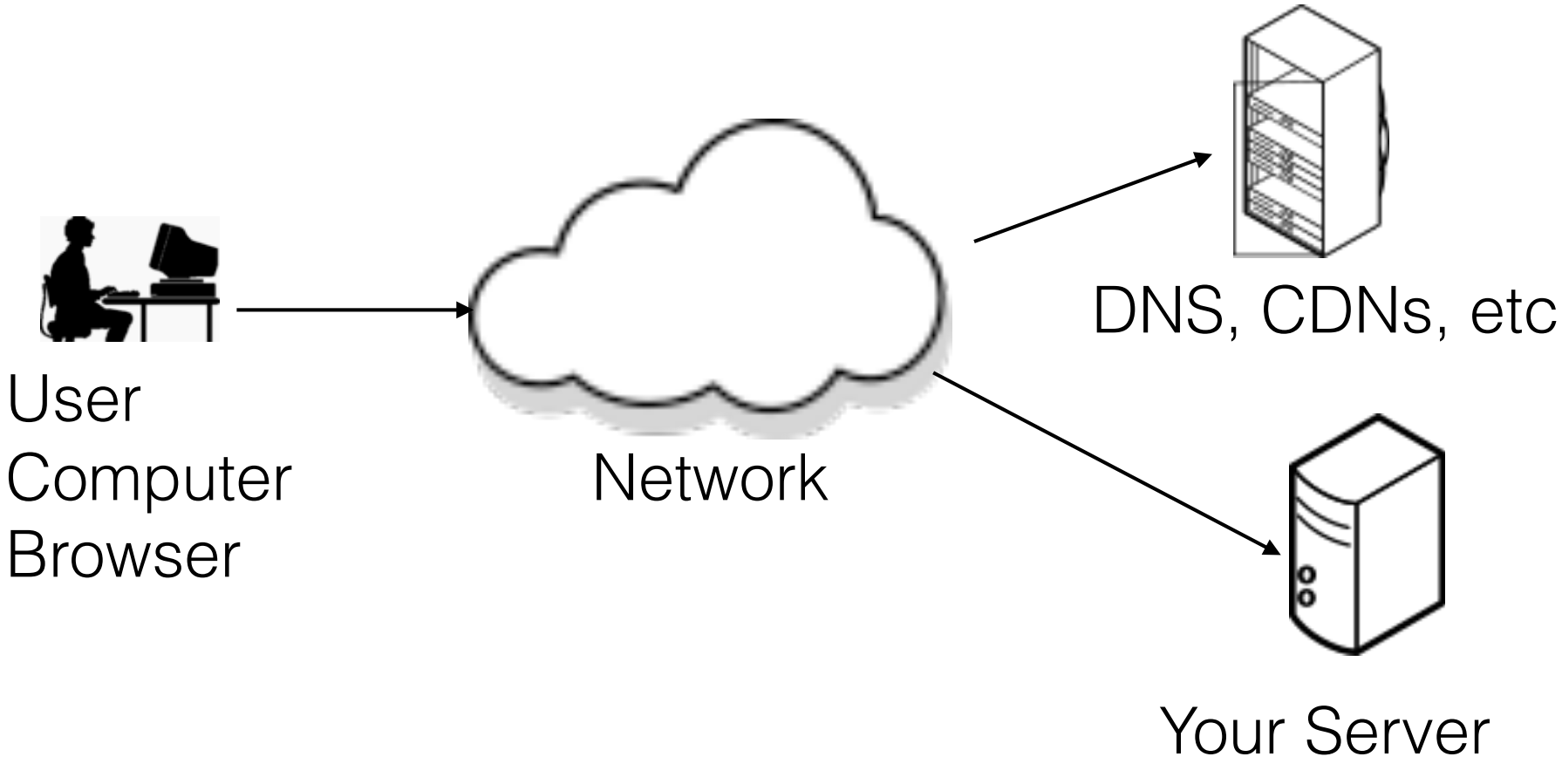
***Threats*** are potential causes of risk:

- Insiders
- Criminals
- Commercial competitors
- Nation-states (intelligence agencies and their proxies)
- Law Enforcement
- Vandals, “security researchers”, “script kiddies”

# All sort of attacks

- Directly on your system
  - stealing data, passwords, credit card numbers
  - defacing, denial of service, link spam
- On your users
  - Cross Site Scripting (XSS), Request Forgery (CSRF), Man-In-The-Middle (MITM), profiling
- Both
  - Hosting bad content / “drive-by download”
- Neither
  - Ad-based malware

# Environment




(https://openclipart.org/)

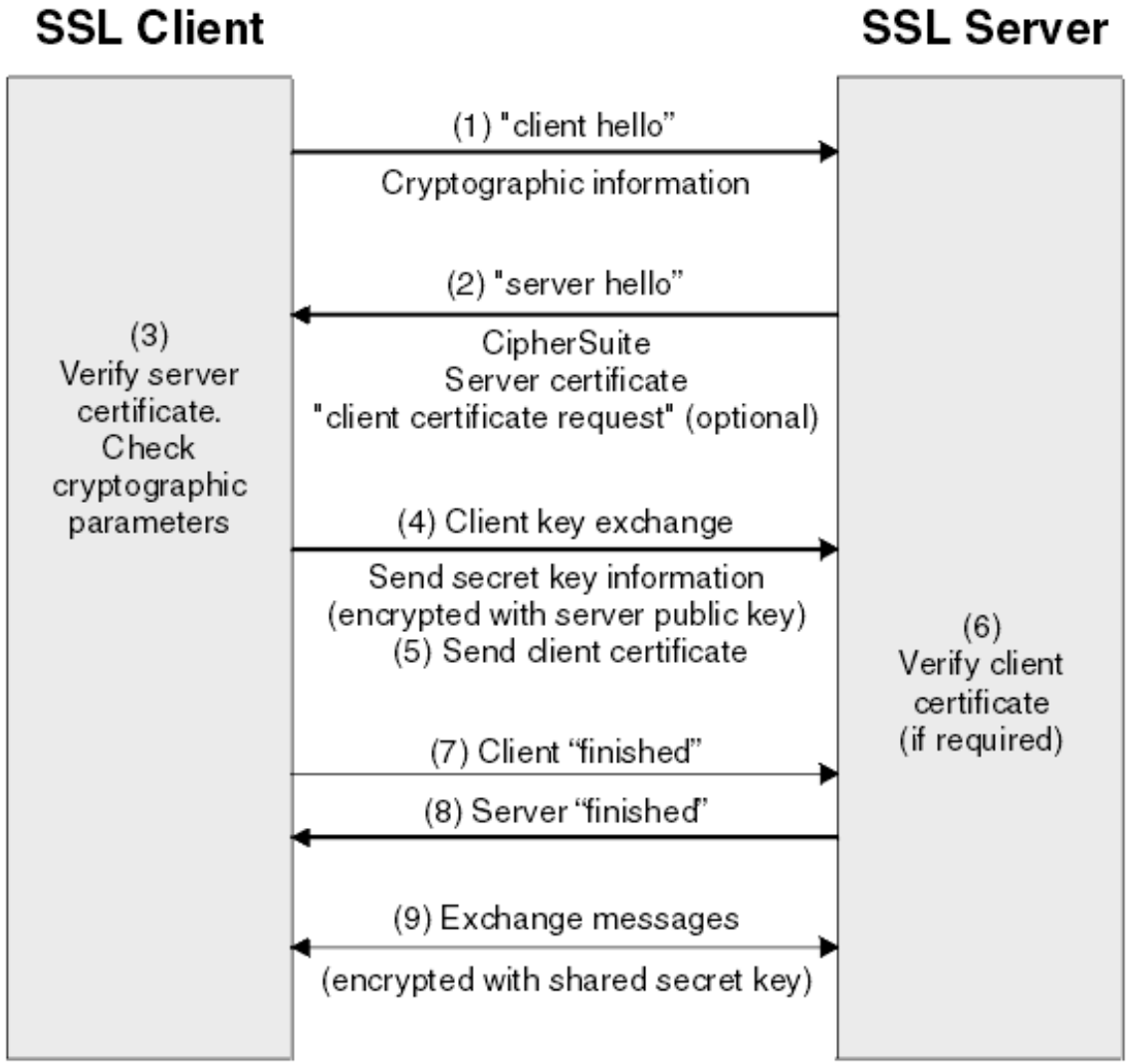
# Transport Layer Security (TLS)

Security mechanism underlying HTTPS

Often still called SSL, but the older SSL protocol versions are obsolete and broken

Client and Server use public-key encryption to agree on a shared per-session secret, then use that secret to encrypt session data.

http://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm



# TLS and You

- You owe it to your users
- Get a server certificate from Let's Encrypt https://letsencrypt.org/
- Test your configuration, e.g. https://www.ssllabs.com/ssltest/

# Authentication

- Who is the user?
- Don’t write your own
- Always store passwords salted & hashed, using trusted algorithms (PBKDF2, scrypt, bcrypt - see https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)

# “Social” login

- Facebook Login, Google Identity, Sign In With Twitter, etc.
- OAuth 2.0 (https://oauth.net/2/)
- Federated Identity
- SAML (https://wiki.oasis-open.org/security/FrontPage#SAML_V2.0_Standard)

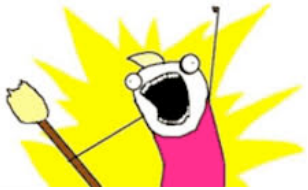
# Authorization

We know who you are, what can you do?

- No silver bullet
- Look for support in your web framework
- Check every operation

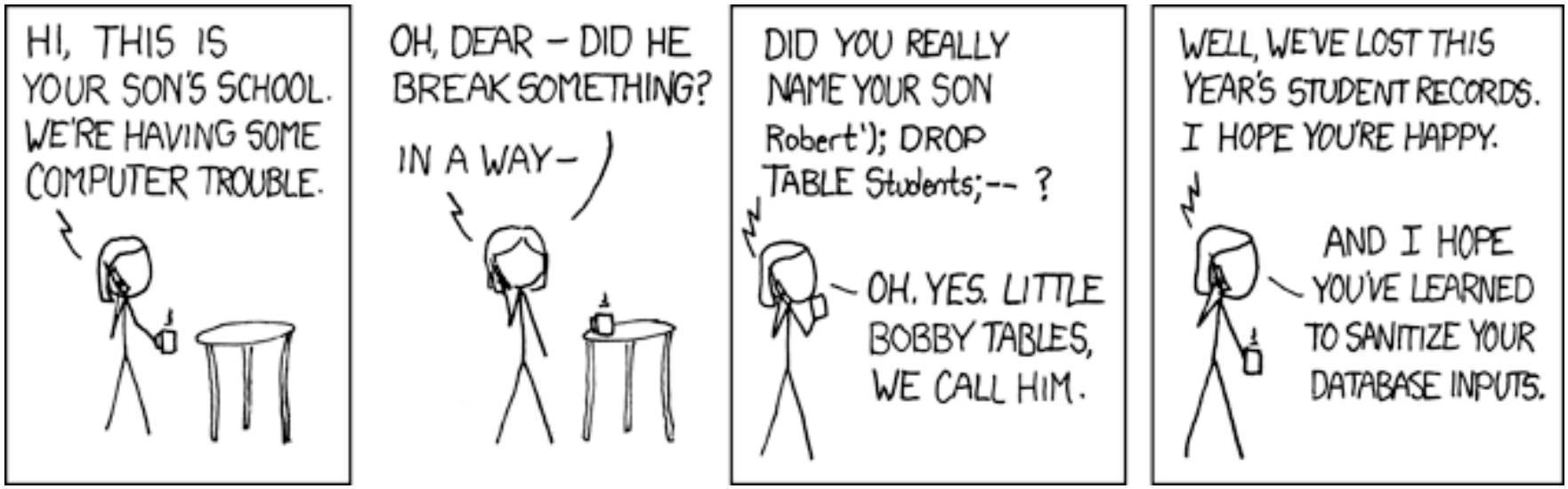
# What you need to do

- Patch all the things



- Monitor everything (Pingdom, Wormly, NewRelic, DataDog, Splunk, BugSnag, …)
- Alert someone if a monitor detects problems (PagerDuty :-)
- Backups - reliable, tested, isolated, archived
- Everything OWASP says

http://hyperboleandahalf.blogspot.ca/2010/06/this-is-why-ill-never-be-adult.html




https://xkcd.com/327/

# Open Web Application Security Project

- https://www.owasp.org/index.php/About_OWASP
- Not for profit, registered charity in US and Europe
- Unbiased advice about common web security flaws and how to address them
- Top 10 last updated 2013, but things haven't changed much
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013

# Learn and Practice

Lists of security teaching web sites you can explore and try to hack:

- https://www.checkmarx.com/2015/04/16/15-vulnerable-sites-to-legally-practice-your-hacking-skills/

- https://hack.me/