Agenda

- The Heartbleed Vulnerability

The Heartbleed Bug/Vulnerability

image source: http://heartbleed.com

Class Survey

Before today's class, which one of the following statements describes you correctly?

- A. I have never heard of the Heartbleed bug.
- B. I have heard of the Heartbleed bug, but that's it. I have no idea what exactly it is or what are the techniques behind this bug.
- C. I have heard of the Heartbleed bug, I know it has something to do with SSL/TLS or HTTPS, and may have affected many famous websites, but I don't know further details.
- D. I know what Heartbleed bug is, and I can explain it in a detailed fashion.

Terminology

- CVE Common Vulnerabilities and Exposures. CVE-2014-0160.
- SSL/TLS Secure Sockets Layer/Transport Layer Security. A protocol used for establishing an encrypted link between a server and a client (typically a web server and a browser). TLS is the successor of SSL.
- Heartbeat Request The RFC 6520 Heartbeat Extension tests TLS secure communication links by allowing a computer at one end of a connection to send a Heartbeat Request message, consisting of a payload, typically a text string, along with the payload's length as a 16-bit integer. (see next slide)
- HTTPS A protocol for secure communication over a computer network. HTTPS consists of communication over HTTP within a connection enrypted by SSL/TLS: The webpage you are viewing is transmitted to you in an encrypted form, default port 443.

The Heartbleed Vulerability

- a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol.
- introduced into the software in 2012.
- publicly disclosed in April 2014.
- results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension.
- the vulnerability is classified as a buffer over-read. (a situation where more data can be read than should be allowed)

The Heartbeat Extension and the Heartbleed Attack/Vulerability

- The SSL standard includes a "heartbeat" extension, which provides a way for a computer at one end of the SSL connection to double-check that there's still someone at the other end of the line. This feature is useful because some internet routers will drop a connection if it's idle for too long.
- The heartbeat message has three parts: a request for acknowledgement, a short, randomly-chosen message (in this case, "banana"), and the number of characters in that message. The server is simply supposed to acknowledge having received the request and parrot back the message.
- The Heartbleed attack takes advantage of the fact that the server can be too trusting. When someone tells it that the message has 6 characters, the server automatically sends back 6 characters in response.

Learn from Taylor Swift

image source: https://i.ytimg.com/vi/FRh98vYzBEI/maxresdefault.jpg

The Heartbeat Protocol: When Used by Good Users

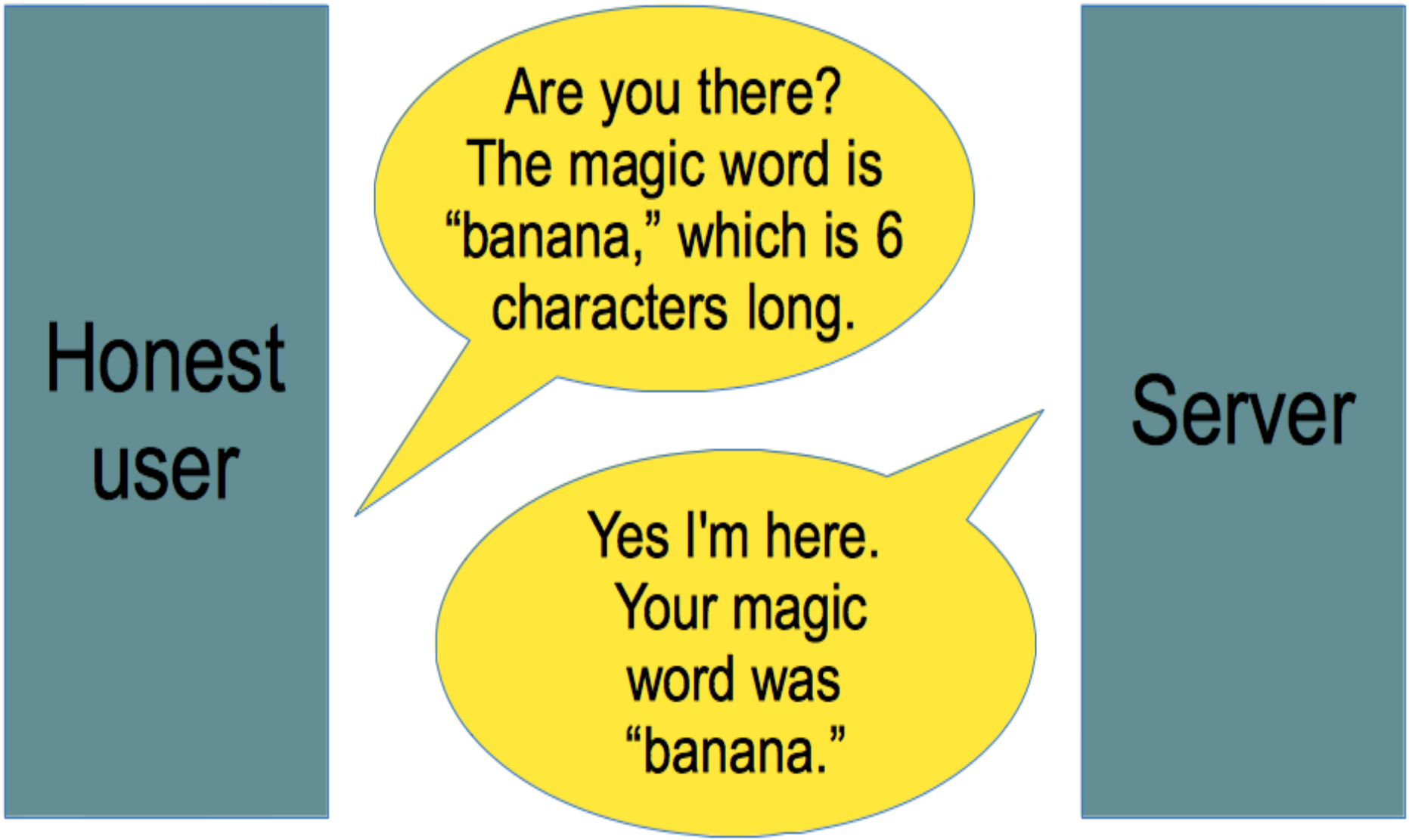

image source: http://www.vox.com/2014/4/8/5593654/heartbleed-explainer-big-new-web-security-flaw-compromise-privacy

The Hearbeat Protocol: When Used by Evil Users

image source: http://www.vox.com/2014/4/8/5593654/heartbleed-explainer-big-new-web-security-flaw-compromise-privacy

What information can you get with a Heartbleed attack?

Any information handled by web servers is potentially vulnerable. That includes

- passwords
- credit card numbers
- medical records
- contents of private email or social media messages.
- server's private encryption key

Affected Sites

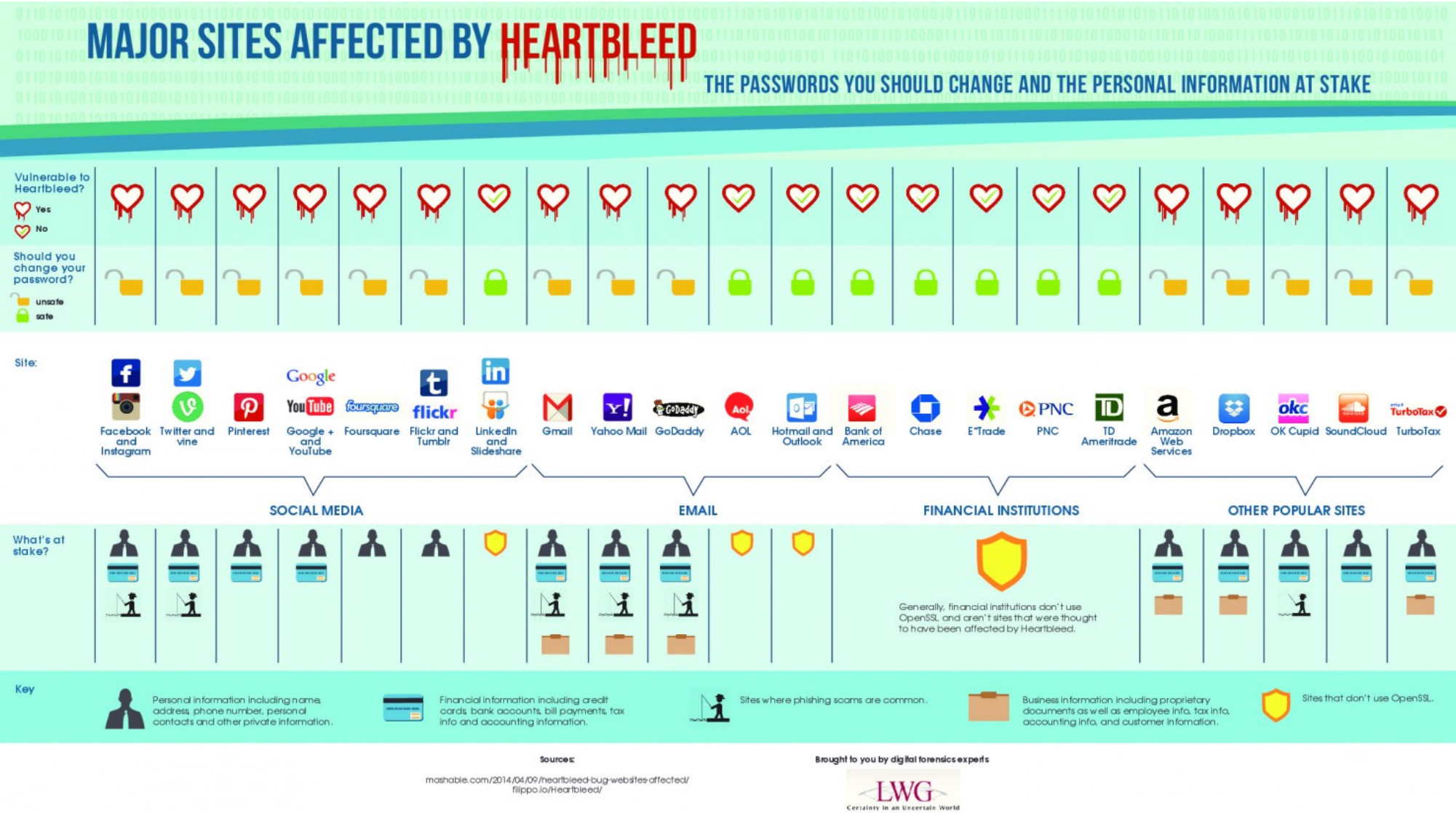

image source: http://visual.ly/major-sites-affected-heartbleed, designed by Athens Chen.

Heartbleed Test

https://filippo.io/Heartbleed/

The Fix in OpenSSL

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902

"Add heartbeat extension bounds check"

if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0; /* silently discard per RFC 6520 sec. 4 */

Vulnerability to Heartbleed is resolved by updating OpenSSL to a patched version (1.0.1g or later).

Impact on the Client Side

- Although the bug received more attention due to the threat it represents for servers, TLS clients using affected OpenSSL instances are also vulnerable.
- Malicious servers are able to exploit Heartbleed to read data from a vulnerable client's memory.
- The stolen data could contain usernames and passwords.

References

A large portion of the material is adapted from:

- HTTPS wikipedia: - https://en.wikipedia.org/wiki/HTTPS
- Heartbleed wikipedia: - https://en.wikipedia.org/wiki/Heartbleed
- OpenSSL Heartbeat (Heartbleed) Explained (BEST ON YouTube!) Steals Credit Card INFO https://www.youtube.com/watch?v=hTK0pywfmDE

Backup Slides

Importance of Making Contributions to Open Source Projects

- Jidong's own experience
- Google Summer of Code https://developers.google.com/open-source/gsoc/
- Google Summer of Code 2017 https://summerofcode.withgoogle.com/archive/2017/projects/