SSL / TLS

Empirical analysis of SSL/TLS weaknesses in real websites: Who cares?

The purpose

- SSL/TLS vulnerabilities of top global & Korean websites
- “Home-made” tool for checking the flaws
- Based on Nmap & Selenium WebDriver
- Tested 500 most popular websites
- Tested against 6 types of attacks

Logjam

CCS Injection

Heartbleed

DROWN

POODLE

FREAK

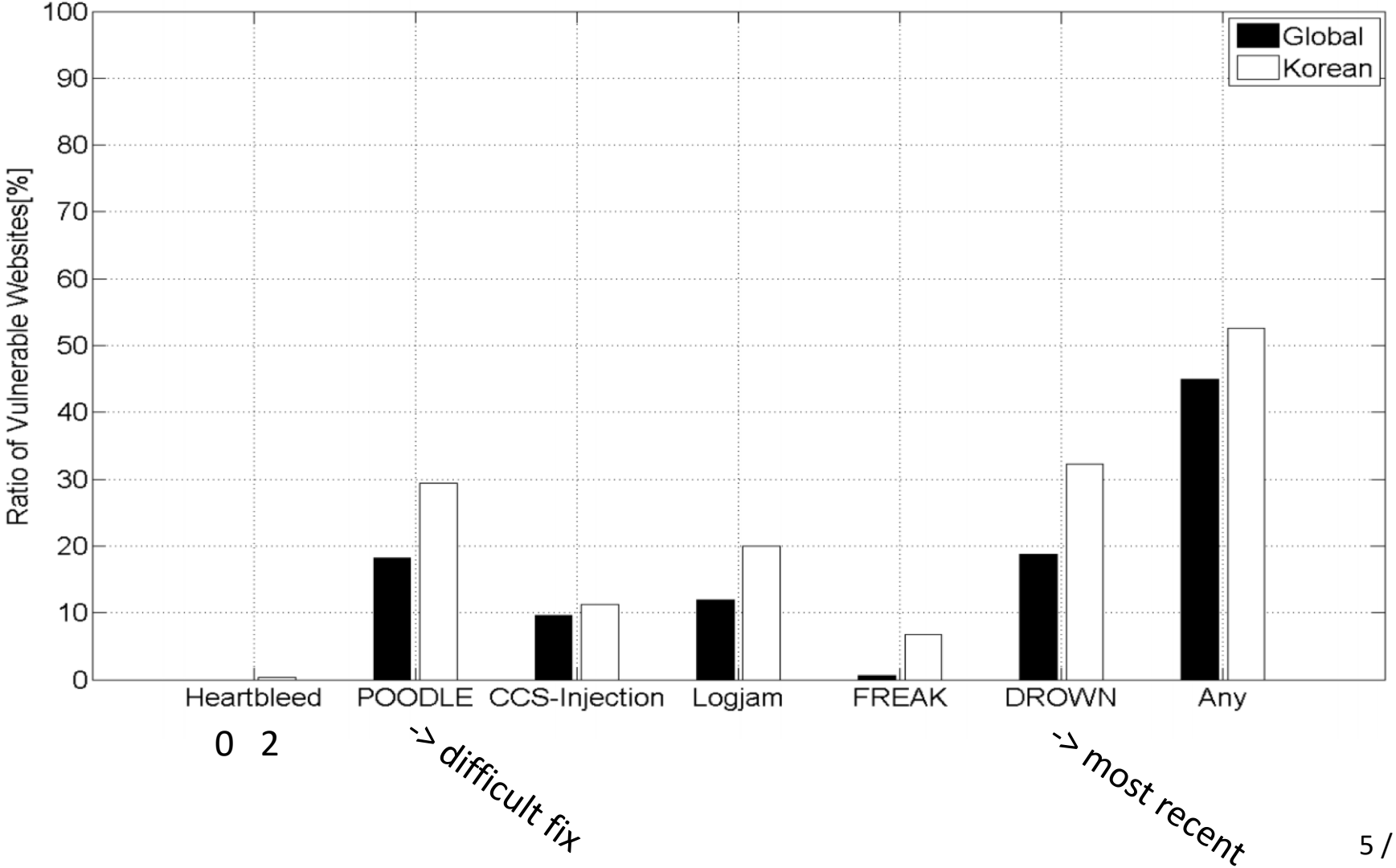
	Site	Daily Time on Site	Daily Pageviews per Visitor	% of Traffic From Search	Total Sites Linking In
1	Google.com Enables users to search the world's information, including webpages, images, and videos. Offers...More	8:18	10.80	0.70%	2,467,386
2	Youtube.com YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your...More	8:51	5.07	11.40%	1,932,838
3	Facebook.com A social utility that connects people, to keep up with friends, upload photos, share links and ...More	9:29	3.94	7.70%	5,047,596
4	Baidu.com The leading Chinese language search engine, provides "simple and reliable" search exp...More	7:13	5.62	8.50%	145,722
5	Wikipedia.org A free encyclopedia built collaboratively using wiki software. (Creative Commons Attribution-Sh...More	4:16	3.15	54.70%	1,310,847
6	Qq.com China's largest and most used Internet service portal owned by Tencent, Inc founded in Nov...More	3:45	3.77	9.20%	315,935
7	Taobao.com Launched in May 2003, Taobao Marketplace (www.taobao.com) is the online shopping destination of...More	7:39	3.98	5.40%	40,002
8	Yahoo.com A major Internet portal and service provider offering search results,	3:53	3.53	8.80%	478,455

www.alexa.com/topsites

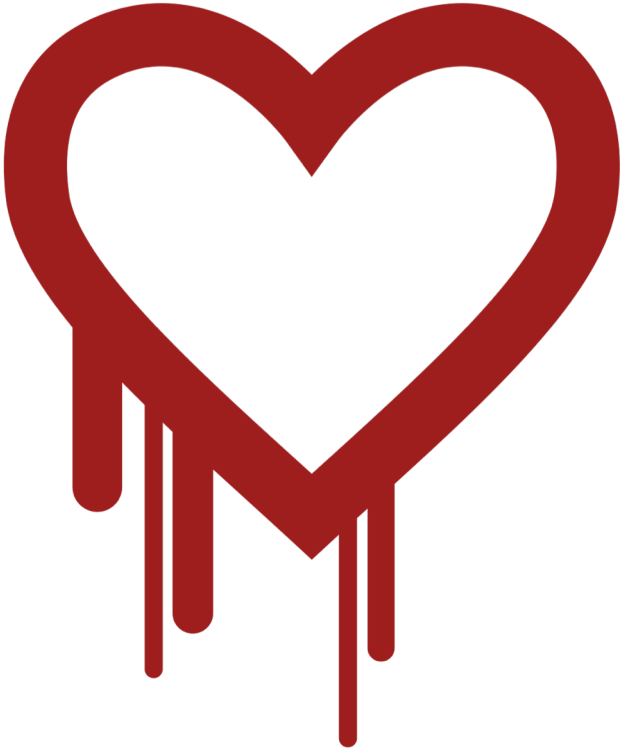
Results

- Vulnerable to at least 1 type
    - **45% global**
    - **52.6% Korean**

- Correlations between attacks
- One SSL/TLS vulnerability might open doors to others


Global
Korean
Ratio of Vulnerable Websites[%]
100
90
80
70
60
50
40
30
20
10
0
Heartbleed
POODLE
CCS-Injection
Logjam
FREAK
DROWN
Any
0 2
-> difficult fix
-> most recent

Heartbleed attack



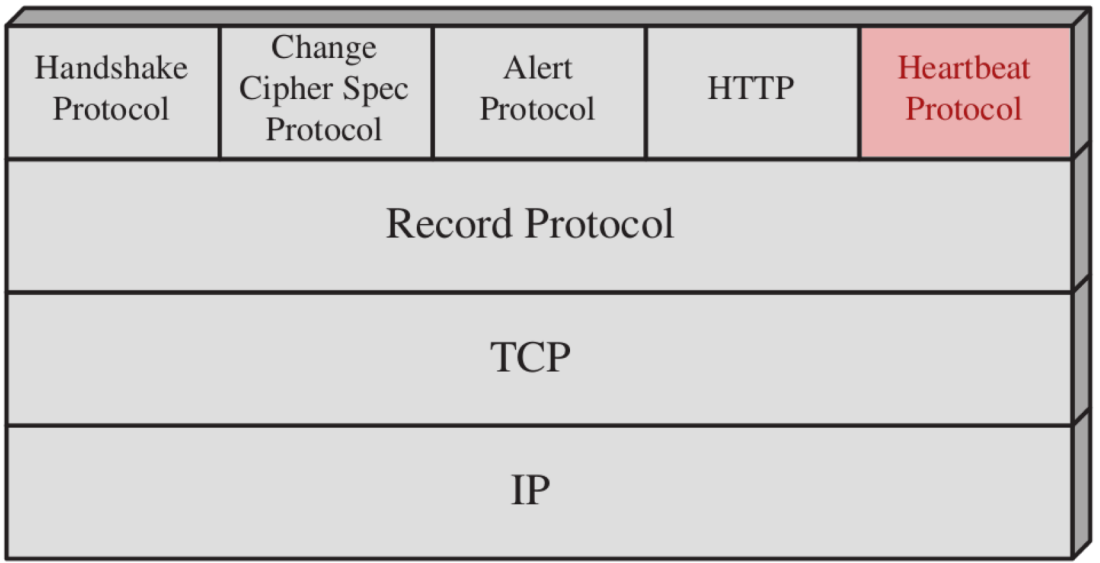
Heartbeat

- Part of the TLS protocol stack

- Ensures that the client/server is still active

- **Request-response** model

- Request contains **random number** and the response should **send it back**



Heartbleed

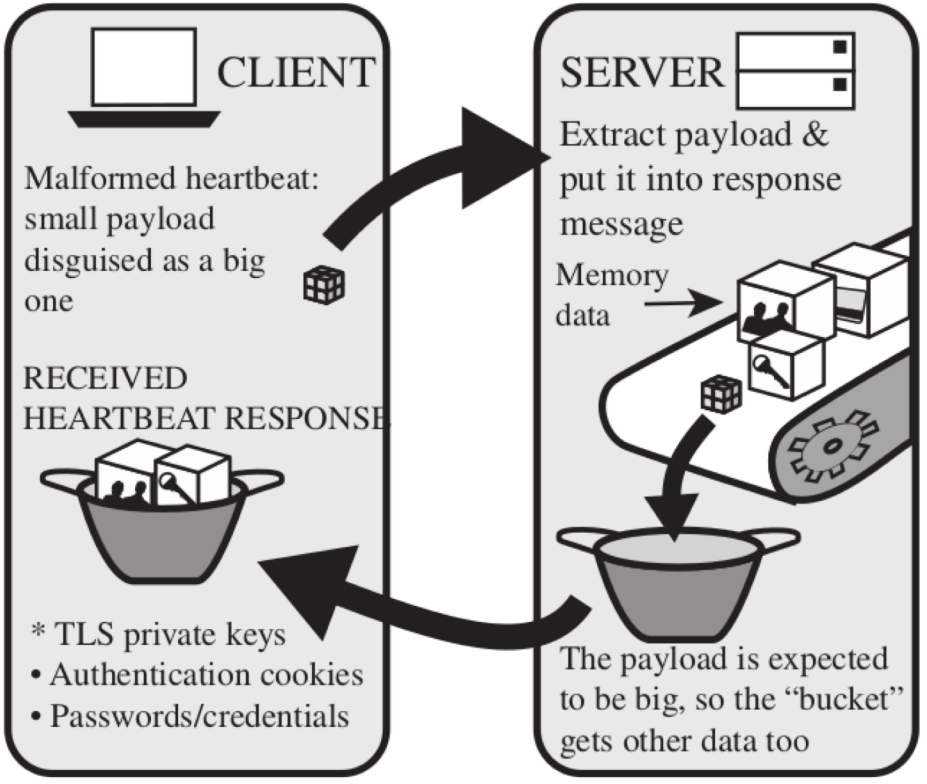
- Not a design flaw but an **actual bug** in the code
- Discovered in April 2014
- **2/3** of the world's servers affected
- January 23, 2017 report by shodan.io
    - 2 years and 9 months since the fix was released
    - **Over 199 500** websites still vulnerable
    - thehackernews.com/2017/01/heartbleed-openssl-vulnerability.html

Heartbleed

- The server “believed” the client about the request length

- Server allocates memory according to the message length header

- If the actual **length is smaller** than the one in the header, the server still sent back the whole allocated chunk of memory – this could contain data for **other application** or **sensitive data**



Heartbeat sent to victim

SSLv3 record:

Length
4 bytes

HeartbeatMessage:

Type	Length	Payload data	
TLS1_HB_REQUEST	65535 bytes	1 byte	

Victim's response

SSLv3 record:

Length
65538 bytes

HeartbeatMessage:

Type	Length	Payload data	
TLS1_HB_RESPONSE	65535 bytes	65535 bytes	

Last remarks

- Decreasing trend in SSL/TLS vulnerabilities
- No enforcement

"Here, government could have a role in periodically performing such security checks and publishing the checking results for system administrators to encourage them to keep their systems up-to-date with latest security patches."

Thank you for your attention

Lukas Kucerik