Heartbleed

EECS3482 - Computer Security

Farhan Arshad
Jonathan Lebon
Tsilavina Ratovonirina

HTTP[S] and SSL/TLS

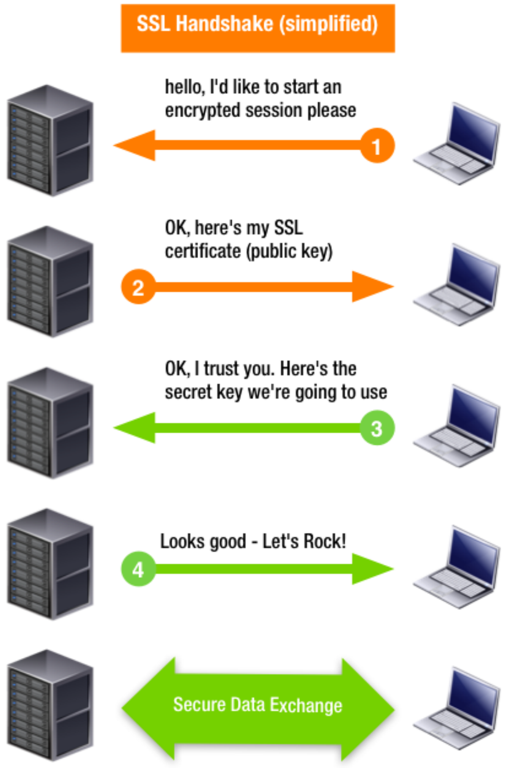
- HTTP (Hypertext Transfer Protocol)
  - Protocol for non-encrypted communication (e.g. blogs, public sites)
- SSL (Secure Sockets Layer)
  - Protocol for encrypted communication (e.g. banks, emails)
  - Marked by “https” URLs
- TLS (Transport Layer Security)
  - Latest and most secure version of SSL
- OpenSSL
  - Implementation in C of the SSL/TLS protocol for secure communication
  - Used by two thirds of all web servers

What is Heartbleed?

- ➔ Heartbeat: periodic exchange between two computers consisting of sending and getting information back to check and maintain conversation

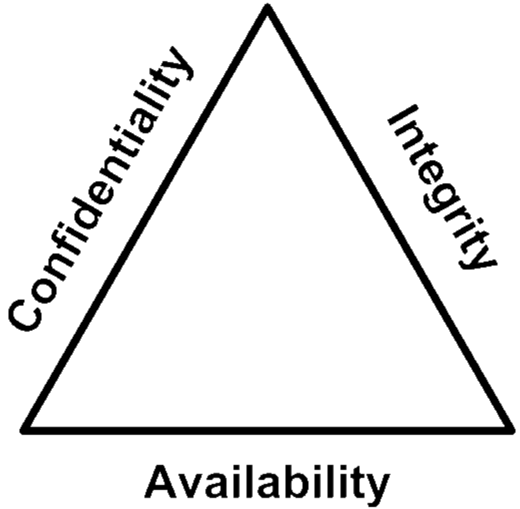
- ➔ Heartbleed: security bug in the OpenSSL cryptographic software library

- ➔ A buffer over-read vulnerability where more data can be read than should be allowed

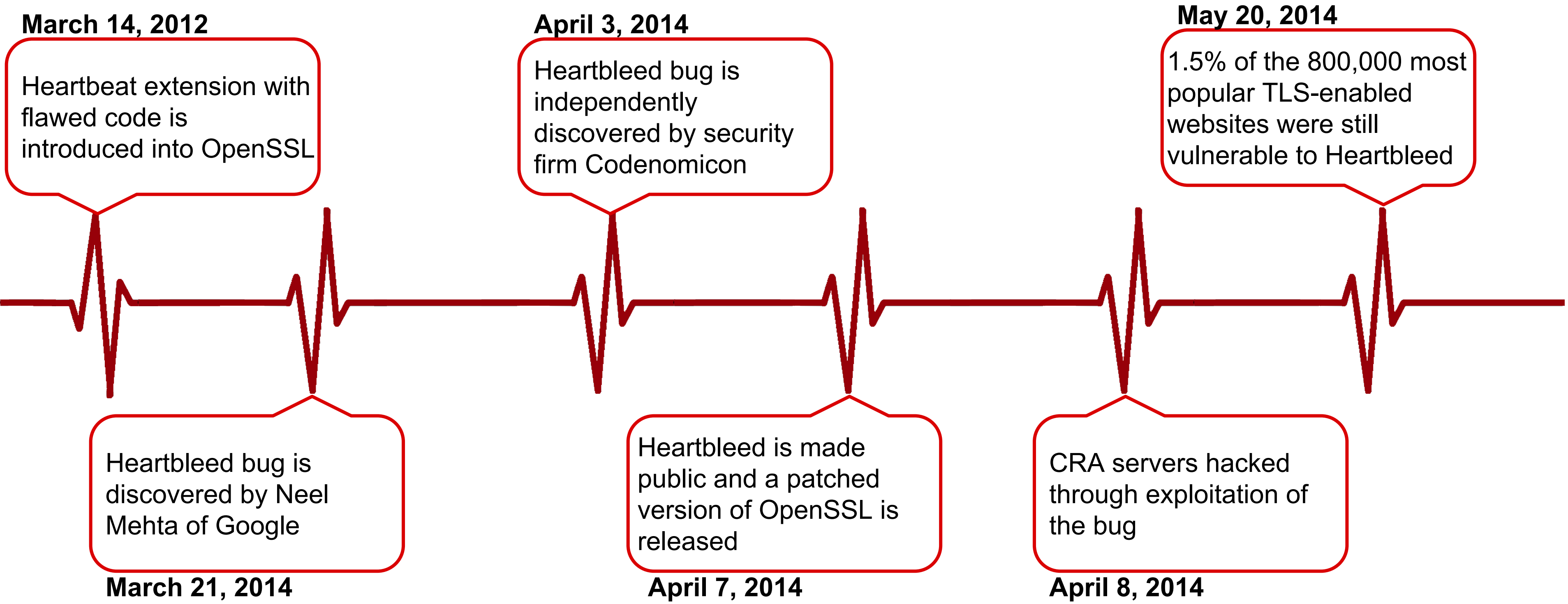

SSL Handshake (simplified)
hello, I'd like to start an encrypted session please
1
OK, here's my SSL certificate (public key)
2
OK, I trust you. Here's the secret key we're going to use
3
Looks good - Let's Rock!
4
Secure Data Exchange

What is Heartbleed?

- ➔ CIA triangle: compromised confidentiality
- ➔ Requires no privileged information
- ➔ Random but high likelihood of critical security information



Timeline



March 14, 2012

Heartbeat extension with flawed code is introduced into OpenSSL

Heartbleed bug is discovered by Neel Mehta of Google

March 21, 2014

April 3, 2014

Heartbleed bug is independently discovered by security firm Codenomicon

Heartbleed is made public and a patched version of OpenSSL is released

April 7, 2014

CRA servers hacked through exploitation of the bug

April 8, 2014

May 20, 2014

1.5% of the 800,000 most popular TLS-enabled websites were still vulnerable to Heartbleed

How did this happen?

- Heartbeat TLS extension:
  - Client: say the 4-letter word “duck”
  - Server: “duck”
- But data and length both controlled by user
  - Bad client: say the 65535-letter word “duck”
  - Server: “duck...garbagedata...change_admin_pw_to_qwerty…”

Damages

- ➔ Canada Revenue Agency
  - ◆ Social insurance numbers of approximately 900 taxpayers stolen
  - ◆ CRA temporarily shut down access to website
  - ◆ Western University engineering student charged by RCMP

Do you owe taxes this year?

Post-date your payment with the CRA pre-authorized debit service.

- ➔ Community Health Systems
  - ◆ Happened a week after Heartbleed was first made public
  - ◆ Enabled hackers to steal security keys
  - ◆ Compromising the confidentiality of 4.5 million patient records

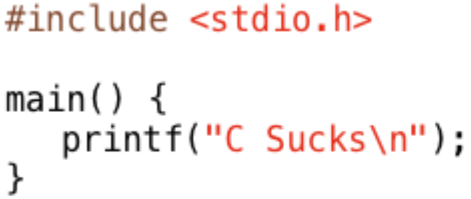
Damages

- mumsnet
  - Several user accounts hijacked, CEO impersonated
  - Hacker actually announced him/herself on the network; wanted to show how serious Heartbleed problem is

- Cost
  - Damage estimated to be $500 Million
  - Embedded devices are mostly unpatchable
  - Human Resources, Certificate Revocation, Stolen Data
  - Years until the final true cost is ever tallied

Aftermath

- Discoverer rewarded $15K
- OpenSSL scrutinized
- The C language criticized
- OpenSSL forked → LibreSSL
- Core Infrastructure Initiative



```
#include <stdio.h>

main() {
   printf("C Sucks\n");
}
```

References

[1] IETF -- RFC6520: TLS and DTLS Heartbeat Extension
http://www.rfc-editor.org/rfc/rfc6520.txt

[2] Gizmodo -- How Heartbleed Works
http://gizmodo.com/how-heartbleed-works-the-code-behind-the-internets-se-1561341209

[3] Sean Cassidy -- Diagnosis of the OpenSSL Heartbleed Bug
http://www.seancassidy.me/diagnosis-of-the-openssl-heartbleed-bug.html

[4] Linux Foundation -- Core Infrastructure Initiative
http://www.linuxfoundation.org/programs/core-infrastructure-initiative/

[5] Theo de Raadt -- OpenSSL is not developed by a responsible team
http://article.gmane.org/gmane.os.openbsd.misc/211963

[6] The Conversation -- How the Heartbleed bug reveals a flaw in online security
https://theconversation.com/how-the-heartbleed-bug-reveals-a-flaw-in-online-security-25536

References

[7] Coverity -- Coverity Releases Platform Update for OpenSSL ‘Heartbleed’ Defect
http://www.coverity.com/press-releases/coverity-releases-platform-update-for-openssl-heartbleed-defect/

[8] Ars Technica -- OpenSSL code beyond repair, claims creator of “LibreSSL” fork
http://arstechnica.com/information-technology/2014/04/openssl-code-beyond-repair-claims-creator-of-libressl-fork/

[9] The Register -- Anatomy of OpenSSL’s Heartbleed: Just four bytes trigger horror bug
http://www.theregister.co.uk/2014/04/09/heartbleed_explained/

[10] CWE -- CWE-126: Buffer over-read
http://cwe.mitre.org/data/definitions/126.html

[11] Wikipedia -- Heartbleed
http://en.wikipedia.org/wiki/Heartbleed

References

[12] The Age -- Heartbleed disclosure timeline: who knew what and when
http://www.theage.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html

[13] CBC News -- Heartbleed bug: RCMP asked Revenue Canada to delay news of SIN thefts
http://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192

[14] United States Securities And Exchange Commission -- FORM 8-K
http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm

[15] Time -- Report: Devastating Heartbleed Flaw Was Used in Hospital Hack
http://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/

[16] The Register -- AVG on Heartbleed: It's dangerous to go alone. Take this (an AVG tool)
http://www.theregister.co.uk/2014/05/20/heartbleed_still_prevalent/

References

[17] CBC News -- Baloney Meter: Are there discrepancies in the CRA's Heartbleed timeline?
http://www.cbc.ca/news/politics/baloney-meter-are-there-discrepancies-in-the-cra-s-heartbleed-timeline-1.2613725

[18] Data Breach Today -- Is Heartbleed Behind Healthcare Breach?
http://www.databreachtoday.asia/heartbleed-behind-healthcare-breach-a-7215

[19] CBC News -- Stephen Arthuro Solis-Reyes charged in Heartbleed-related SIN theft
http://www.cbc.ca/news/politics/stephen-arthuro-solis-reyes-charged-in-heartbleed-related-sin-theft-1.2612526

[20] eWeek -- Heartbleed SSL Flaw's True Cost Will Take Time to Tally
http://www.eweek.com/security/heartbleed-ssl-flaws-true-cost-will-take-time-to-tally.html#sthash.T2fPrlIQ.dpuf

[21] Einstein Medical Blog -- Dealing with the “Price Question"
http://www.einsteinmedical.com/blog/2013/05/28/dealing-with-the-price-question-128958

References

[22] Wikipedia -- All your base are belong to us
http://en.wikipedia.org/wiki/All_your_base_are_belong_to_us#mediaviewer/File:Aybabtu.png

[23] Search Security -- Transport Layer Security
http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

[24] Ars Technica -- Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping
http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/

[25] Hallman internet -- Migrating your Website from HTTP to HTTPS
http://www.hallaminternet.com/2015/migrating-website-http-https/

[26] Good Math -- Bad software, Cryptography: The Heartbleed Bug
http://www.goodmath.org/blog/2014/04/08/the-heartbleed-bug/

References

[27] Krystal -- The OpenSSL Heartbleed bug simplified

https://krystal.co.uk/blog/2014/04/the-openssl-heartbleed-bug-simplified/

Question 1

1. Why is Heartbleed so devastating?
    a. Highly confidential information available without any privileged information required
    b. Affected 0.5 million machines, some still unpatched to this day

Question 2

2. What are the most known Heartbleed exploits?
   a. 900 SIN numbers stolen from the CRA
   b. 4.5 million patient records compromised from Community Health Systems

Question 3

3. How long did it take for the Heartbleed bug to be identified?
    a. Introduced in March 14, 2012
    b. Identified in March 21, 2014, more than two years after introduction