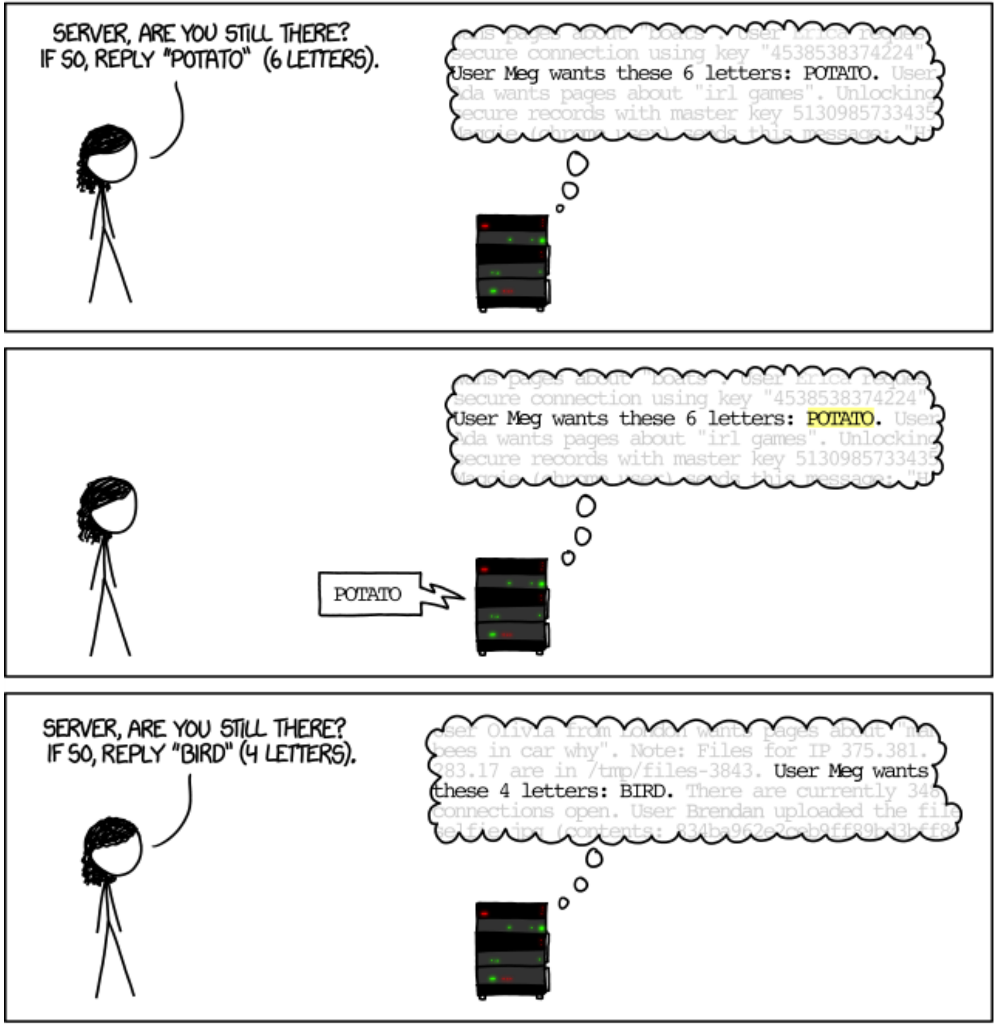
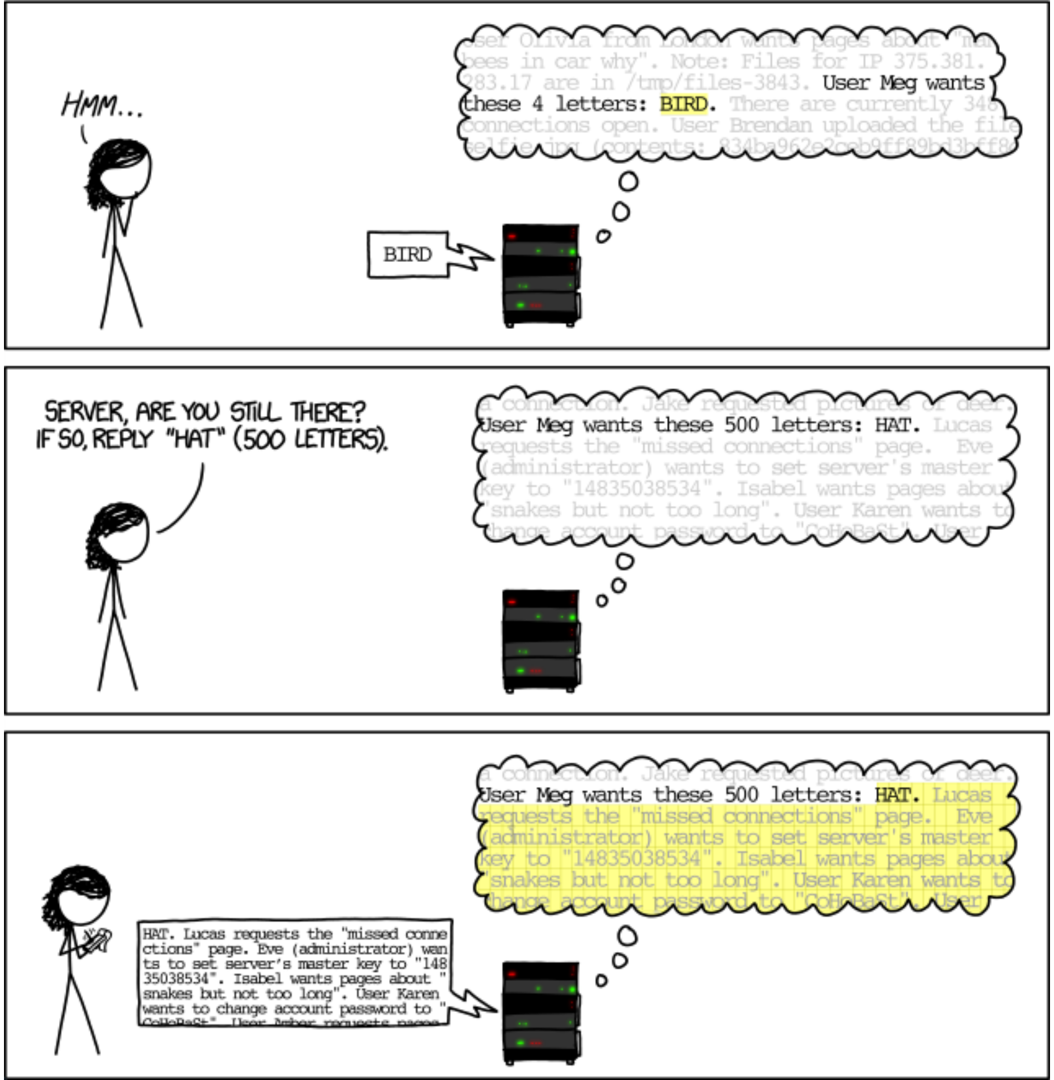
HOW THE HEARTBLEED BUG WORKS:


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
ans pages about "boats". User Erica reques secure connection using key "4538538374224" User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435 Maggie (chrome user) sends this message: "H
ans pages about "boats". User Erica reques secure connection using key "4538538374224" User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435 Maggie (chrome user) sends this message: "H
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8


HMM...
User Olivia from London wants pages about "ma
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 346
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
"snakes but not too long". User Karen wants to
change account password to "CoHoBaSt". User
a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
"snakes but not too long". User Karen wants to
change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed conne
ctions" page. Eve (administrator) wan
ts to set server's master key to "148
35038534". Isabel wants pages about "
snakes but not too long". User Karen
wants to change account password to "
CoHoBaSt". User Amber requests pages

But what is heartbeat exactly?

- Contains a payload(data) and the size of that payload
- For keeping a TLS connection alive, if there is a communication-gap
- “Heartbeat”-packets == a way of saying:”Are you there?” to the server
- Is intended for use over UDP(or other connectionless protocol) == no guarantee that the packet won’t be lost
- Arbitrarily-sized payload == too much flexibility for most users

The good news

Implementation error

Not an error by design

The bug

- Programmer forgot to check the payload size
- Returns up to 64kb of additional RAM-data
- Etc. send payload of 1b, with size of 60.000b, rinse and repeat
- That could be:
    - Database information
    - Server side code
    - Privat encryption keys
    - Basically anything in the RAM

Demonstration

```
$ python hb-test.py localhost
```

Affected versions

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Vulnerable for almost 2 years

The discovery

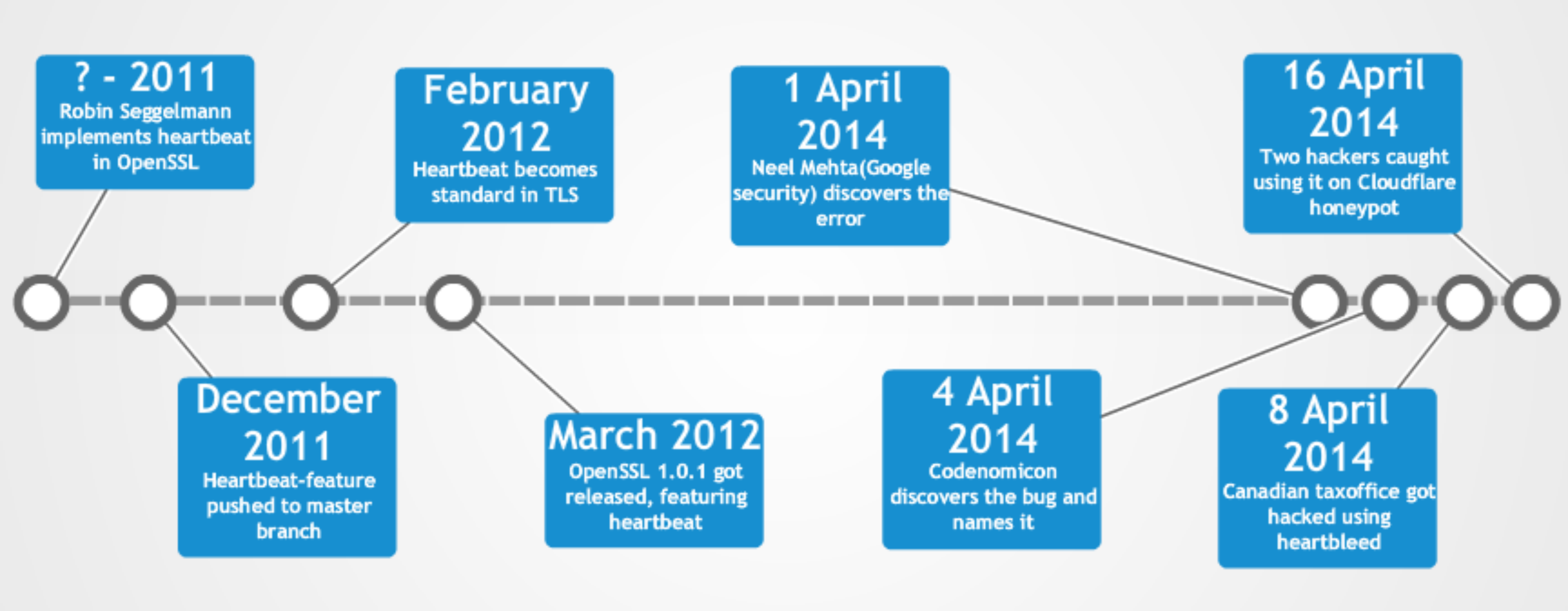
Discovered independently by:

- Codenomicon(security team consisting of 3 people)
- Neel Mehta(Google security)

Reported to OpenSSL

Analyzed and verified by “The National Cyber Security Centre Finland”

Timeline



? - 2011
Robin Seggelmann implements heartbeat in OpenSSL

December 2011
Heartbeat-feature pushed to master branch

February 2012
Heartbeat becomes standard in TLS

March 2012
OpenSSL 1.0.1 got released, featuring heartbeat

1 April 2014
Neel Mehta(Google security) discovers the error

4 April 2014
Codenomicon discovers the bug and names it

8 April 2014
Canadian taxoffice got hacked using heartbleed

16 April 2014
Two hackers caught using it on Cloudflare honeypot

Scale and Impact

- Shutdown costs caused by Heartbleed are estimated to be 500 million US dollars
- Many major websites, such as fx. GitHub, Pinterest, Reddit, SourceForge and Tumblr were affected
- Android v 4.1.1 is still susceptible to Heartbleed. There is 50 million devices still using that version

How could it happen?

- OpenSSL was operating solely on donations totalling $841
- OpenSSL defied the standards of OpenBSD and programmed their own memory management
- OpenSSL is maintained by a single full-time worker and a tiny number of volunteers
- Because of lack of funding OpenSSL never had proper security audits. Nobody checked if Heartbleed was there

The Future

- Experts predict more vulnerabilities like Heartbleed will be found
- The Linux Foundation has started a multi-million dollar project to fund initiatives such as OpenSSL