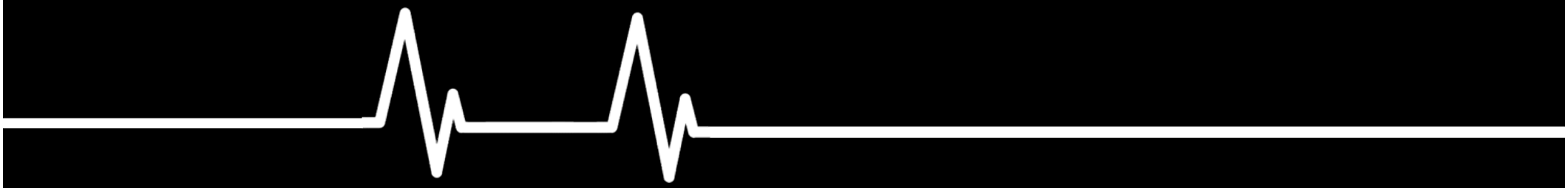
Heartbleed

Felipe Jorge Christine Tran Chelsea Waida



“We attacked ourselves,” Chartier says. The results freaked him out. The team realized they were able to access a user’s memory, encryption keys, usernames and passwords—”plus a lot of other stuff that we don’t want to mention,” Chartier says. “We saw how serious it was.”

- David Chartier
CEO of Codenomicon

What is Heartbleed?

- Found in April 2014
- An error in OpenSSL
  - length variable not checked
  - led to a buffer over-read
- Has been around since 2012
- Heartbleed was found by **Codenomicon security engineers**: Ossi Salmi, Ville Alatalo, Tuomo Untinen, Antti Karjalainen, and Ossi Herrela and **Google researcher** Neel Mehta
- Specifically in transport layer security (TLS) protocols' heartbeat extension
- Leaked usernames, passwords, financial and personal information, and encryption keys

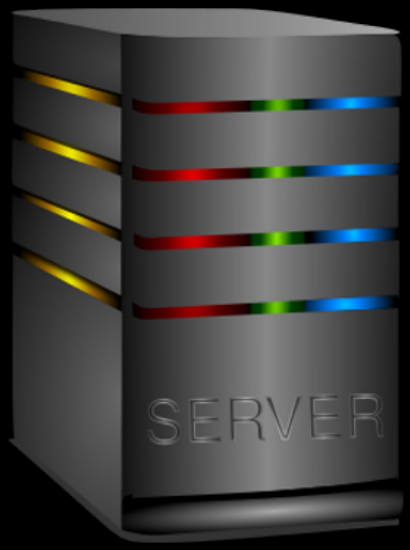
How SSL Works

Prove Identity + $$$

Certified Public Key

Trusted Third Party Company

- Verisign
- Thawte



Certified Public Key

Encrypted Secret Key Generated

Communication under Symmetric Encryption begins

User

Trusted Third Party Public Key

The Heartbleed Exploitation

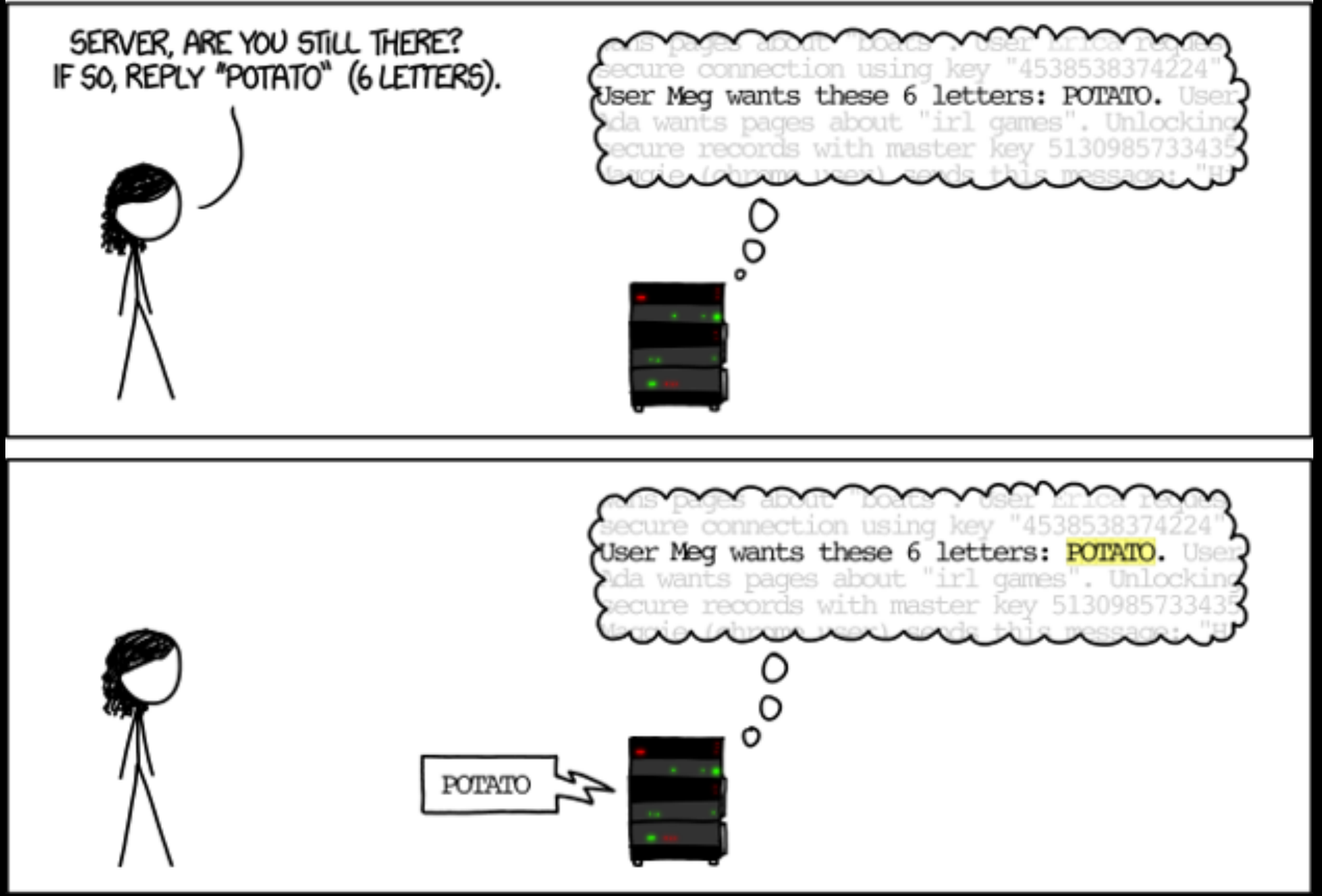
Heartbeat extension

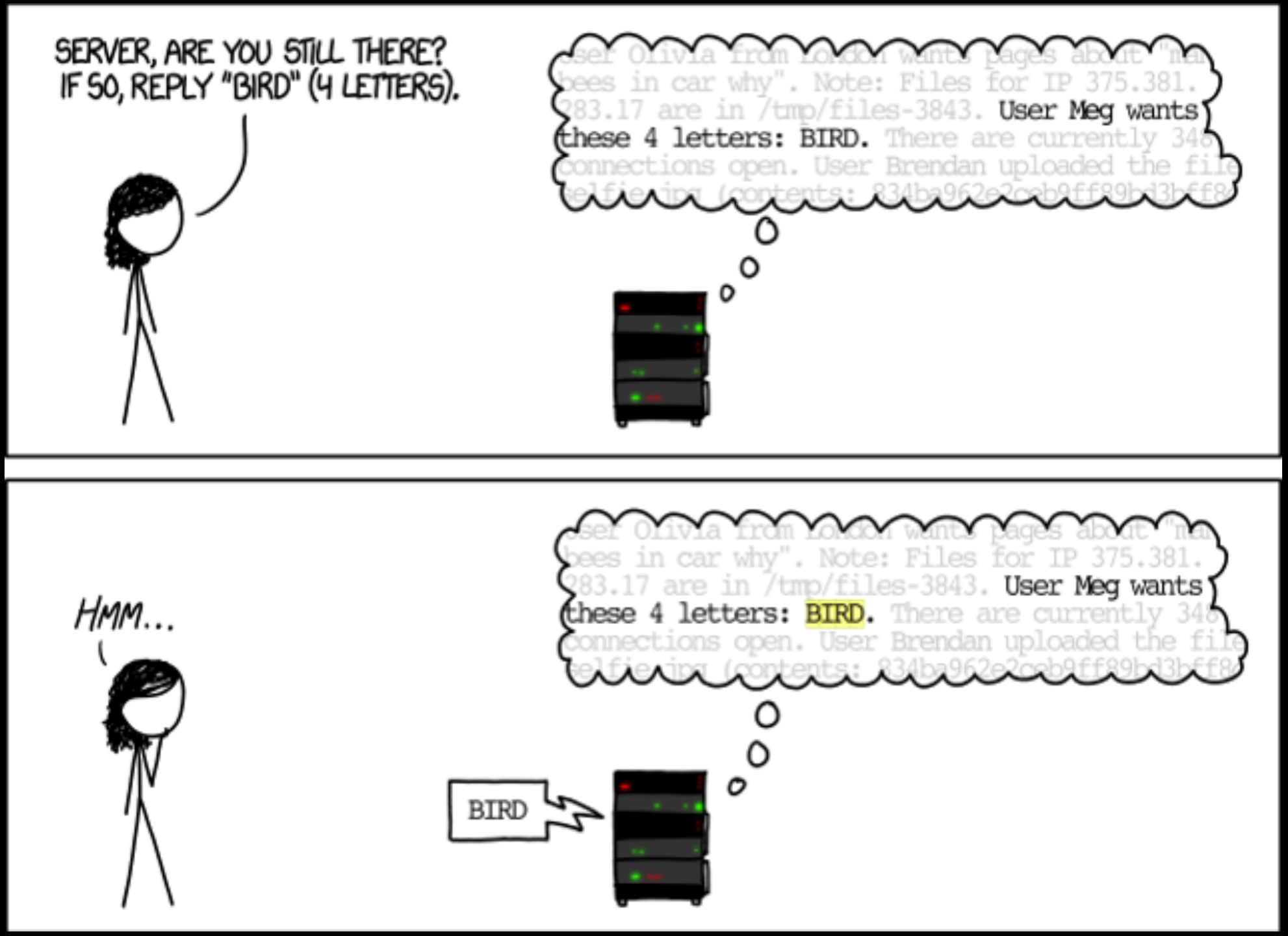
- Provides a way for computer and server to check if they are still connected.
- Some internet routers will drop connection if idle for too long
- **Heartbeat requires 3 parts:**
  1) request for acknowledgment
  2) a short, random message
  3) the number of characters in the message

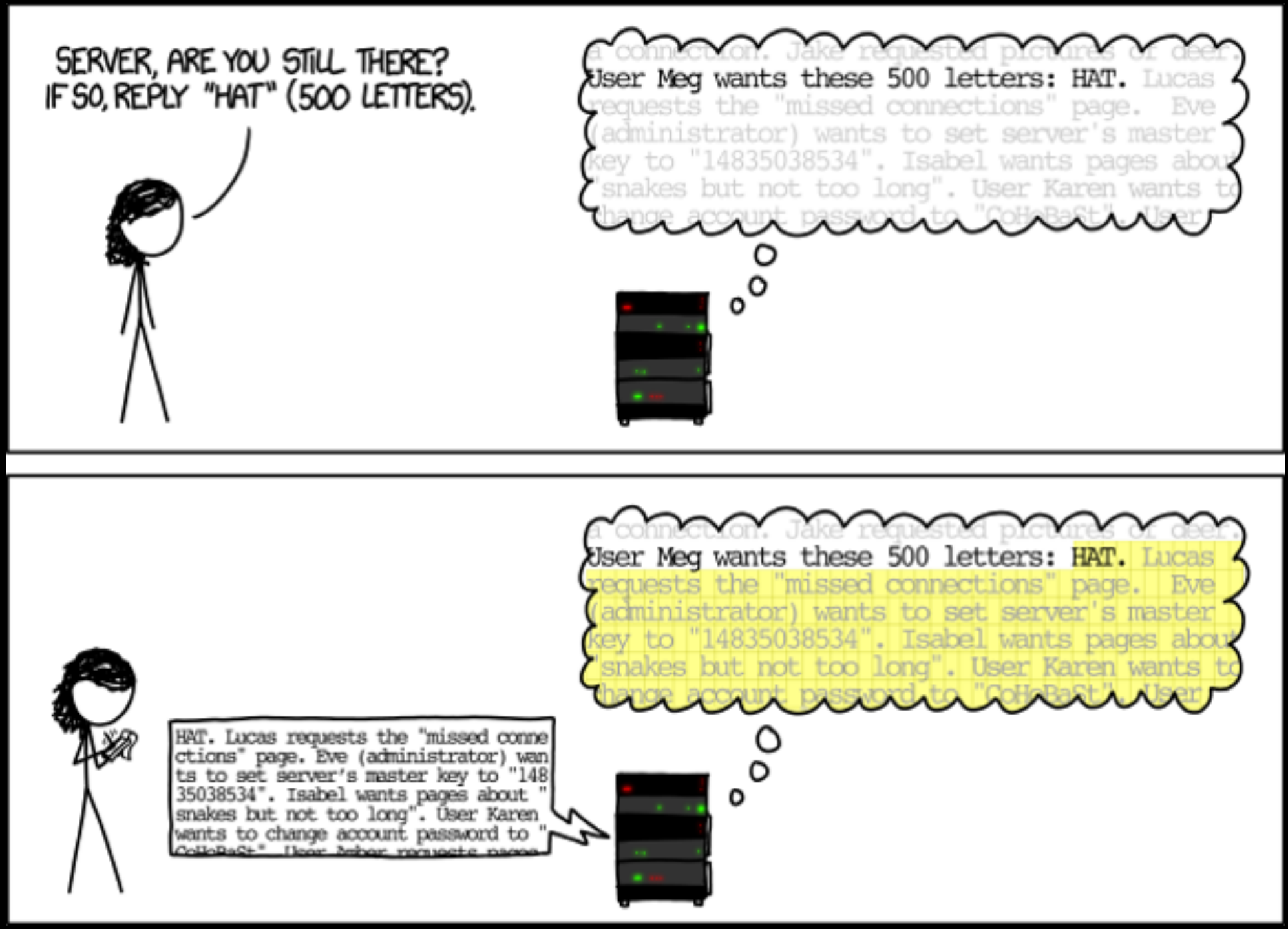
Heartbleed

- The attacker can take advantage of heartbeat by sending requests and instead of asking for the correct length of the message, it asks for 64kb.
- The server doesn't check if the message and the length match, and therefore will send whatever is stored in memory at the time.

HOW THE HEARTBLEED BUG WORKS:




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).
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
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 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 "

Affected Sites

Social Networks:

- Facebook
- Instagram
- Pintrest
- Tumblr

Entertainment:

- Flickr
- Minecraft
- Netflix
- Youtube

Email:

- Gmail
- Yahoo Mail

Companies:

- Google
- Yahoo

Financial:

- American Funds
- Venmo

Stores & Commerce:

- Amazon Web Services
- Etsy
- GoDaddy

Government & Taxes:

- Healthcare.gov
- USAA

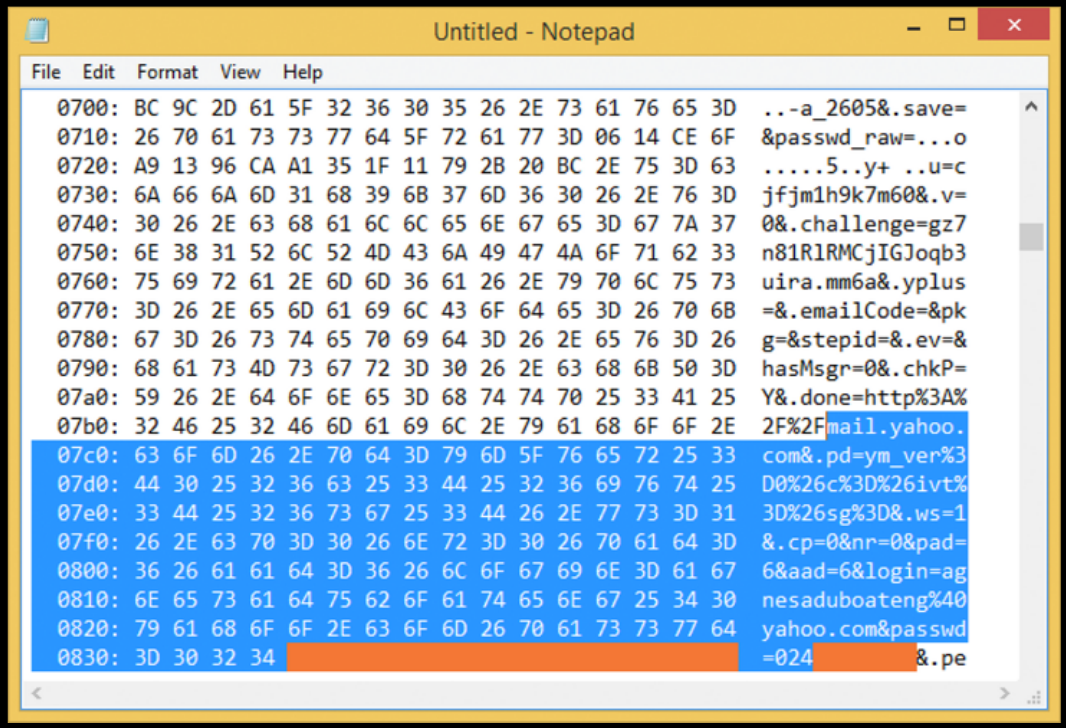
Other:

- GitHub
- Dropbox
- IFTTT
- Wikipedia
- Wordpress

The Heartbleed Patch

```
hbtype = *p++;
n2s(p, payload);
 if (1 + 2 + payload + 16 > s->s3->rrec.length)
        return 0; /* silently discard per RFC 6520 sec. 4 */
pl = p;
```

- ✓ OpenSSL 1.0.1g patch
- ✓ Patches the bug in OpenSSL's implementation of the TLS Heartbeat extension
- ✓ A bounds check using the correct length of the incoming Heartbeat message
- ✓ Every company affected had to install the updated/patched version of SSL



Did the NSA Exploit Heartbleed?

Photographer: Paul J. Richards/AFP via Getty Images

"The U.S. National Security Agency knew for at least two years about [Heartbleed] ... and regularly used it to gather critical intelligence"

-Bloomberg News

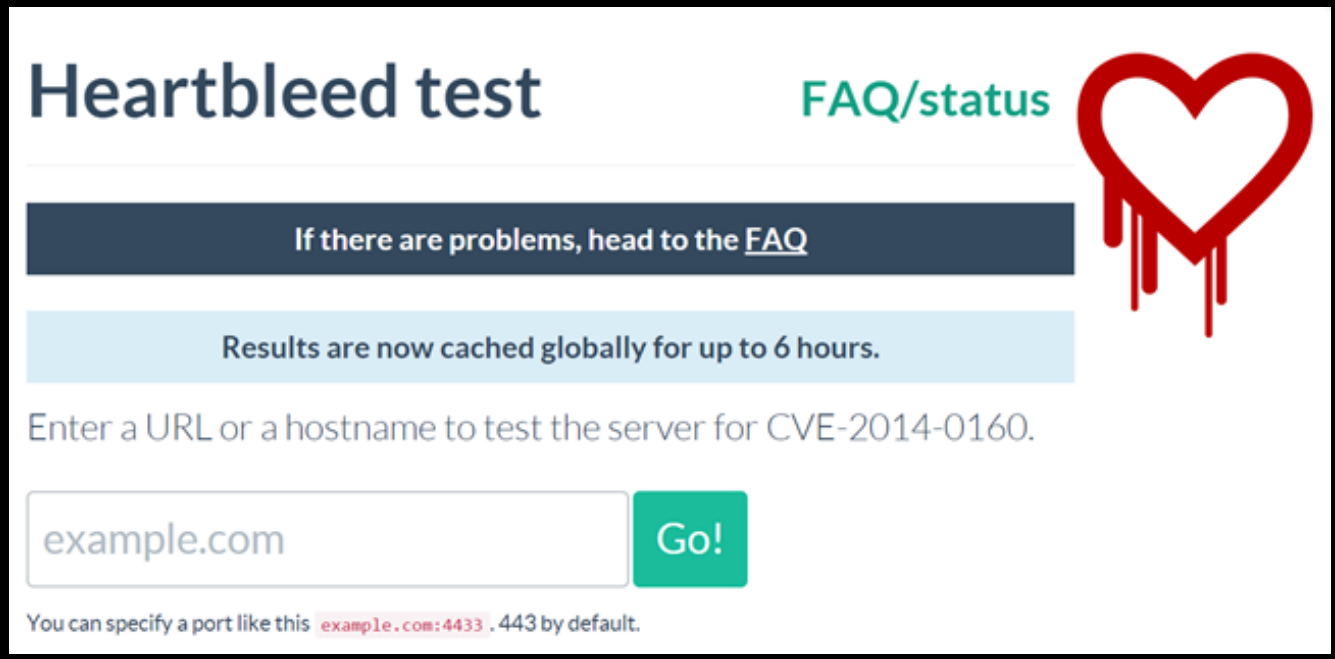
- Headlines reported NSA was exploiting Heartbleed
- Mike Rogers, director of the NSA, denies having known about the bug before it was publicly announced
- No proof apart from the two anonymous sources "familiar with the matter"

NSA's Arsenal of Vulnerabilities

- Gains computer vulnerabilities from "Black Market"
- Often keeps these vulnerabilities out of the public eye
- Will not disclose to public if:
  - "No one but us" can find the vulnerability
  - The intelligence to be gained is necessary
  - Not much harm would be done if an adversary found the vulnerability

Consequences & Countermeasures

- Attacks and exploitations do not leave a trace
- Attacks do not have a limit
- Can attack again and again until payload gives critical information
  - Password
  - Security Questions & Answers
- Sites and companies recommend:
  - Change passwords after a patch has been confirmed



Citations

- Official Heartbleed Site
- xkcd Explanation of Heartbleed
- Heartbleed Wikipedia Page
- Bloomberg Article on NSA Exploitation Of Heartbleed
- NSA's Tracking of Bugs
- Details of How Heartbleed Works
- How SSL Works
- NSA's Hoarding of Vulnerabilities
- Criteria of Disclosing Cyber Vulnerabilities
- Discovery Heartbleed
- How Heartbleed was Found
- Explanation of Heartbleed Code
- Heartbleed Test Site

Thank you for listening!