Overview of the Year In Security

Kevin Hill
OSG Security Team

OpenSSL - Recent

- New OpenSSL vulnerabilities announced last week.
- Important security flaws in 1.0.2 branch. RHEL and SL don't use this branch.
- After much speculation, turned out to be mainly vulnerable to denial of service attacks.
- Malformed certificates can crash a client or a server.
- 3/20/15

OpenSSL- Freak

- Many clients and servers were able to be tricked into accepting weak “export” grade RSA keys.
- Man in the middle attack possible.
- Was rated “medium”, but upgraded to “high” once it was discovered just how many sites still accepted the weak export grade keys.
- Export restrictions lifted 10 years ago.
- 3/3/15

OpenSSL - POODLE

- Attackers could set up a man-in-the-middle attack and cause connections to fall back to older SSLv3 encryption.
- Padding Oracle attack was possible against SSLv3 to determine encrypted data with repeated request to the victim server.
- Somewhat limited impact due to needing network access to get m-i-t-m set up.
- 10/14/14

Heartbleed

- Announced during OSG AHM 2014.
- Really perfected the art of branding security vulnerabilities.
- Flaw in OpenSSL's implementation of the heartbeat TLS extension.
- Did result in some SSL servers being compromised, including leaks of 4.5 million patient records of a large hospital chain.
- 4/7/14

Open Science Grid

Glibc “Ghost”

- Flaw in name resolution routines of glibc could potentially result in remote code execution.
- Depends on IPv4 specific routines that generally aren’t used by default anymore.
- Depends on apps accepting user generated hostnames to look up.
- Turns out main issue only with certain mail servers.

Open Science Grid

ShellShock

- A flaw in Bash allowed code to be executed in specially formatted environment variables.
- Many web apps using CGI vulnerable, some DHCP clients and other system affected as well.
- Quickly exploited. Several Bot nets popped up within the first day.
- New version of Bash quickly released, turned out first fix was not perfect.
- 10/24/14

Open Science Grid

BadUSB

- Researchers discovered that some USB devices firmware could be modified maliciously.
- Keyboards, flash drives could be used as attack vector and evade anti-malware software.
- Could infect BIOS, even infecting air-gapped systems.
- 7/14

Open Science Grid

Twitch

- Twitch video game video streaming service notified users that their personal info may have been compromised.
- Users requested to reset passwords and re-connect accounts with Facebook, Youtube, etc.
- No details yet on who broke in or how they got in.
- 3/23/15

Lenovo Superfish

- Lenovo shipped laptops for the past year or so with Adware called Superfish.
- Superfish inserted its own ads into webpages.
- To be able to do this on https sites, it set up a man-in-the-middle attack.
- It also used an easily guessable password for the mitm keys.
- Lenovo produced an uninstall tool.
- 2/15

Sony Attack

- Believed launched by North Korea.
- Hack resulted in massive data breach, including internal emails and unreleased Movies.
- Resulted in unparalleled publicity for the movie *The Interview*.
- Hackers claimed to have taken over 100TB of data, and installed malware to wipe Sony's systems.
- 11/24/14

JPMorgan

- Tens of millions of Chase customers had credit card info leaked.
- Did not appear to affect bank data.
- Said to affect over 80 million US households and 7 million small to medium businesses.
- FBI investigation continuing.
- May have been caused by an old server not being upgraded to require 2 factor authentication.
- 6/14

Open Science Grid

iCloud

- Celebrity photos and other info posted to various websites.
- Apple claimed no break ins.
- Appears to be work of guessing/brute-forcing passwords.
- Apple added enhanced security including two-factor auth.
- 8/31/14

US Postal Service

- USPS networks hacked, employee info leaked.
- Attacks traced to China.
- News broke while US and Chinese leaders were meeting to discuss cybersecurity among other things.
- 11/10/14

Target Breach

- Cleanup from Target's 2013 breach continued into 2013
- Total cost estimated at $110 million.
- Proposed settlement for $10 million.
- 40 million credit/debit cards may have been impacted.
- 12/13

Home Depot

- Over 53 million email addresses and 56 million credit cards stolen.
- Third party vendor at fault, allowing hackers to spread through the network to POS terminals.
- 4/14

Open Science Grid

Conclusions

- Some common themes emerge.
- Most break-ins took advantage of old vulnerabilities.
- Two factor auth would have helped in several cases. Stealing passwords not enough.
- Configuration management/verification needed. Two factor auth only helps if all systems require it.

Open Science Grid

Links

- http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/
- https://en.wikipedia.org/wiki/Heartbleed
- http://www.wired.com/2014/07/usb-security/
- http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/