




Heartburn From The Heartbleed Vulnerability

By: Keith Watson

CoC Information Security Manager

Georgia Tech College of Computing



What we will be talking about today

- What is Heartbleed Bug
- How do you fix it
- Systemic weaknesses uncovered by the bug
  - Is PKI broken?
  - Poor detection, how do you know your safe?
  - Challenges to the Linus's Law
  - Poor software development methodologies?
  - Responsible disclosure?

Georgia Tech College of Computing

How heartbleed ticks

- OpenSSL crypto library had a buffer over-read bug in their implementation of the TLS protocol heartbeat function
- Allowed an attacker to recover a web sites private key
- No logs are generated by the attack, IDS can't reliably see it
- Netcraft - 500,000 sites vulnerable or 17% of 2.9 million sites

Georgia Tech College of Computing

How to fix heartbleed

- EFF and Codenomicon published detailed information
  - Install patch
  - Revoke current certificates
  - Create new public/private key pair
  - Request new certificates
  - Install new certificates and restart services
  - Notify all users to change all passwords, keys and certificates they use on the your site

Georgia Tech College of Computing

Is PKI broken?

- Public key infrastructure (PKI) design assumptions that have problems
  - Certificates have short life spans
  - Browsers can check certificate revocation
    - Certificate Revocation Lists (CRL)
    - Online Certificate Status Protocol (OCSP)
  - Certificate revocation would be rare compared to the number issued (not checking is low risk)
  - The network will be available for revocation checks

Georgia Tech College of Computing

Is PKI broken? contd.

- Certificates life spans are typically 3 to 5 years but can be much longer (16 years)
- Certificates must remain in CRL/OCSP until they expire
- 500,000 certificates had to be revoked at the same time
- GlobalSign's CRL grew from 22KB to 4.9MB (1,492 certificates to 133,243)

Georgia Tech College of Computing

Is PKI broken? contd.

- Cisco estimates 12.5 billion Internet devices in 2010, 25 billion by 2015
- 12.5 billion x 4.9MB = 61.25 PB for just one of the certificate authorities
- OCSP has issues
  - Browsers had it off by default
  - When enabled default is soft fail (Wi-Fi hotspots can't authenticate until you login)
  - OCSP statement only valid for a few days
  - OCSP can be DDoSed

Georgia Tech College of Computing

How do you know your safe?

- Heartbleed didn't just affect web servers
  - Embedded devices like home routers
  - Commercial routers like Cisco and Juniper
  - Cell phones
  - Industrial control systems
  - Other software (including client software) that called OpenSSL libraries were affected
    - openvpn, freeradius, asterisk, curl, tor, and many more

Georgia Tech College of Computing

How do you know your safe? contd.

- Not everyone patched
  - June 21, 2014 - 300k vulnerable two months later
  - July 18 2014 - Industrial control systems
  - July 29 2014 - Only 3% of web servers in top corporations fully fixed
  - August 25 2014 - Only half of vulnerable sites are patched
- Hiding behind an IDS may not protect you

Georgia Tech College of Computing

How do you know your safe? contd.

- There are active attacks
  - Canadian Revenue Agency breach
  - Cupid spawns “evil” Wi-Fi networks
  - Community Health Systems breach 4.5 million patient records
  - Aviva Insurance pwnd via their iPhones

Georgia Tech College of Computing

How do you know your safe? contd.

- How to test if their patched
  - Testing a site for heartbleed may be a violation of the Computer Fraud and Abuse Act (CFAA)
  - Tools for testing for heartbleed
    - Filippo Valsorda's Heartbleed test
    - Qualys SSL Labs - SSL Server Test
    - CrowdStrike Heartbleed Scanner
    - DigiCert SSL Certificate Checker
    - More vulnerability testing services

How do you know your safe? contd.

- How to test if their patched contd.
  - Browser plugins/extensions for heartbleed
    - FireFox Heartbleed Notifier and Heartbleed Monitor
    - Chrome Heartbleed Check, Netcraft Extension, and Chromebleed
  - Google search to find a sites heartbleed notice
    - heartbleed site:example.com



Challenges to the Linus's Law

- Linus's Law
  - "given enough eyeballs, all bugs are shallow"; or more formally: "Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix will be obvious to someone."

Georgia Tech College of Computing

Challenges to the Linus's Law contd.

- Some have never believed - Do “Many eyeballs make all bugs shallow”?
- Some believe heartbleed finally disproves Linus’s Law
  - Heartbleed - There Are Not Enough Eyeballs
  - Popular Android apps inherit bugs from recycled code

Challenges to the Linus's Law contd.

- Some believe heartbleed proves Linus's Law
  - Does Heartbleed Disprove 'Open Source is Safer'?
  - Eric S. Raymond - Does the Heartbleed bug refute Linus's Law?

Challenges to the Linus's Law contd.

- Some see both sides
  - Did open source matter for Heartbleed?
  - Heartbleed: Open source's worst hour
  - Heartbleed and misconceptions about Open Source
- Does Linus's Law =
  - Bug free code?
  - Code audit?
  - Bugs get fixed quickly?


Software development

- OpenSSL software development has problems
  - RT Backlog
  - Incomplete/incorrect documentation
  - Library complexity
  - Inconsistent coding style
  - No clear release plan
  - No clear platform strategy
  - No published security strategy

Georgia Tech College of Computing

Software development contd.

- Because OpenSSL open source there are options not available to closed source
  - Linux Foundation to fund security audit and two full-time developers for OpenSSL
  - Core Infrastructure Initiative - Linux Foundation and corporations “to fund open source projects that are in the critical path for core computing functions”



Software development contd.

- Open source options contd.
  - Funded forks of OpenSSL
    - OpenBSD LibreSSL
    - Google BoringSSL

Georgia Tech College of Computing

Responsible disclosure?

- Some say yes
  - Forbes - Was The Heartbleed Bug Disclosed Responsibly?
  - Bruce Schneier - More on Heartbleed
  - CloudFlare - Staying ahead of OpenSSL vulnerabilities
  - Nagios - Heartbleed: One Bug to Rule Them All

Responsible disclosure? contd.

- Some say no
  - eWeek - Heartbleed SSL Flaw Angst Aggravated by Broken Disclosure Process
  - Arbor Networks - The Heartburn Over Heartbleed: OpenSSL Memory Leak Burns Slowly

Responsible disclosure? contd.

- Controversial enough that the Sydney Morning Herald published a time line
  - 3/21/2014 - Neel Mehta of Google Security discovers Heartbleed
  - 3/21/2014 – Google patches their systems
  - 3/31/2014 – someone notifies CloudFlare and they patch
  - 4/1/2014 – Google notifies OpenSSL
  - 4/2/2014 Codenomicon discovers heartbleed

Irresponsible disclosure? contd.

- 4/3/2014 - Codenomicon notifies National Cyber Security Centre Finland (NCSC-FI)
- 4/4/2014 - Akamai notified by anonymous member of OpenSSL community, patches
- 4/6/2014 - NCSC-FI asks U.S. CERT to create a CVE for OpenSSL but provides no details
- 4/6/2014 - Mark Cox of OpenSSL notifies Red Hat and authorizes them to tell other Linux distributors

Irresponsible disclosure? contd.

- 4/6/2014 - Red Hat notifies private Linux distro list only says to contact them directly
- 4/7/2014 - SuSE, Debian, FreeBSD, AltLinux respond and are provided details
- 4/7/2014 - Facebook “finds out” and patches
- 4/7/2014 - OpenSSL publishes advisory and patch
- 4/7/2014 - World finds our via Codenomicon web site, patches are published within days

- What do you think?

Georgia Tech College of Computing



Where to get more information

- This Presentation

  http://www.cc.gatech.edu/~krwatson
- Heartbleed

  https://en.wikipedia.org/wiki/Heartbleed
- How heartbleed ticks

  http://www.theregister.co.uk/2014/04/09/heartbleed_explained/

Georgia Tech College of Computing

Where to get more information contd.

- OpenSSL

  https://en.wikipedia.org/wiki/OpenSSL
- Cryptography

  https://en.wikipedia.org/wiki/Cryptography
- Buffer over-read

  https://en.wikipedia.org/wiki/Buffer_over-read
- Transport Layer Security (TLS)

  https://en.wikipedia.org/wiki/Transport_Layer_Security

Georgia Tech College of Computing

Where to get more information contd.

- Heartbeat

  https://en.wikipedia.org/wiki/Heartbeat_(computing)
- Private key

  https://en.wikipedia.org/wiki/Private_key
- Intrusion Detection System (IDS)

  https://en.wikipedia.org/wiki/Intrusion_detection_system

Georgia Tech College of Computing

Where to get more information contd.

- Evading IDS with heartbleed attack

  http://blog.erratasec.com/2014/04/fun-with-ids-funtime-3-heartbleed.html

- Netcraft - Half a million widely trusted websites vulnerable to Heartbleed bug

  http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

Georgia Tech College of Computing

Where to get more information contd.

- Electronic Frontier Foundation (EFF) - Heartbleed Recovery for System Administrators

  https://www.eff.org/deeplinks/2014/04/bleeding-hearts-club-heartbleed-recovery-system-administrators

- Codenomicon heartbleed site

  http://heartbleed.com/

Georgia Tech College of Computing

Where to get more information contd.

- CVE-2014-0160 - heartbleed vulnerability

  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

- Public key certificate

  https://en.wikipedia.org/wiki/Public_key_certificate

- Public/private key pair

  https://en.wikipedia.org/wiki/Public-key_cryptography

Georgia Tech College of Computing

Where to get more information contd.

- Certificate Signing Request (CSR)

  https://en.wikipedia.org/wiki/Certificate_signing_request
- Public key infrastructure (PKI)

  https://en.wikipedia.org/wiki/Public_key_infrastructure
- Public key certificate

  https://en.wikipedia.org/wiki/Public_key_certificate

Georgia Tech College of Computing

Where to get more information contd.

- Certificate Revocation List (CRL)

  https://en.wikipedia.org/wiki/Revocation_list
- Online Certificate Status Protocol (OCSP)

  https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol
- Federal Agency Best Practices for Device Certificates

  https://www.idmanagement.gov/sites/default/files/documents/AgencyBestPracticesDeviceCerts.pdf

Georgia Tech College of Computing

Where to get more information contd.

- Microsoft recommendations on certificate expiration based on key length

  http://blogs.technet.com/b/configmgrteam/archive/2009/06/12/recommendations-for-pki-key-lengths-and-validity-periods-with-configuration-manager.aspx

- GlobalSign's CRL - Heartbleed Bug Sends Bandwidth Costs Skyrocketing

  http://www.wired.com/2014/04/cost-of-heartbleed/

Georgia Tech College of Computing

Where to get more information contd.

- Cisco report estimating number of Internet connected devices

  http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

- Certificate authority

  https://en.wikipedia.org/wiki/Certificate_authority

- Online Certificate Status Protocol (OCSP) Vulnerabilities Analysis

  https://www.imperialviolet.org/2014/04/19/revchecking.html

Georgia Tech College of Computing

Where to get more information contd.

- Wi-Fi hotspots

  https://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)
- Distributed denial-of-service attack

  https://en.wikipedia.org/wiki/Ddos#Distributed_attack
- Heartbleed on Embedded hardware

  http://www.embedded.com/design/safety-and-security/4430090/Heartbleed-and-its-impact-on-embedded-security

Georgia Tech College of Computing

Where to get more information contd.

- Home routers vulnerable to heartbleed

  http://www.dd-wrt.com/site/content/heartbleed-dd-wrtdd-wrt-online-services

- Cisco and Juniper network devices vulnerable to heartbleed

  http://www.huffingtonpost.com/2014/04/11/heartbleed-routers_n_5132306.html

Georgia Tech College of Computing



Where to get more information contd.

- Aviva attacked via heartbleed vulnerable cell phones

  http://www.theregister.co.uk/2014/06/23/aviva_heartbleed_hack/

- Industrial control systems

  https://en.wikipedia.org/wiki/Industrial_control_system

- openvpn vulnerable to heartbleed

  https://community.openvpn.net/openvpn/wiki/heartbleed

Georgia Tech College of Computing

Where to get more information contd.

- freeradius vulnerable to heartbleed

  http://freeradius.org/security.html
- asterisk vulnerable to heartbleed

  http://blogs.digium.com/2014/04/11/asterisk-heartbleed/
- curl vulnerable to heartbleed

  http://curl.haxx.se/mail/lib-2014-04/0109.html

Georgia Tech College of Computing

Where to get more information contd.

- tor vulnerable to heartbleed

  https://blog.torproject.org/blog/openssl-bug-cve-2014-0160

- More things vulnerable to heartbleed

  https://en.wikipedia.org/wiki/Heartbleed#Specific_systems_affected

- June 21, 2014 - 300k vulnerable to Heartbleed two months later

  http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html

Georgia Tech College of Computing

Where to get more information contd.

- July 18 2014 - Critical industrial control systems remain vulnerable to Heartbleed exploits
- http://arstechnica.com/security/2014/07/critical-industrial-control-systems-remain-vulnerable-to-heartbleed-exploits/

Georgia Tech College of Computing

Where to get more information contd.

- July 29 2014 - Only '3% of web servers in top corporations fully patched for Heartbleed

  http://www.theregister.co.uk/2014/07/29/only_3_of_top_firms_fully_patched_against_heartbleed_flaw/

Where to get more information contd.

- August 25 2014 - Only half of vulnerable sites are patched

  http://arstechnica.com/security/2014/08/heartbleed-is-the-gift-that-keeps-on-giving-as-servers-remain-unpatched/

- Canada Revenue Agency breached using heartbleed

  http://globalnews.ca/news/1274997/hacker-charged-in-cra-heartbleed-breach/

Georgia Tech College of Computing

Where to get more information contd.

- Cupid spawns evil Wi-Fi network that exploits heartbleed

  http://arstechnica.com/security/2014/06/meet-cupid-the-heartbleed-attack-spawns-evil-wi-fi-networks/

- Community Health Systems breached using heartbleed

  http://www.csoonline.com/article/2466726/data-protection/heartbleed-to-blame-for-community-health-systems-breach.html

Georgia Tech College of Computing

Where to get more information contd.

- Scanning for heartbleed may be a violation of the Computer Fraud and Abuse Act (CFAA)

  http://www.theregister.co.uk/2014/04/11/heartbleed_health_checking_services_may_be_illegal/

- Computer Fraud and Abuse Act (CFAA)

  https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Georgia Tech College of Computing

Where to get more information contd.

- Heartbleed test

  https://filippo.io/Heartbleed/
- SSL Server Test

  https://www.ssllabs.com/ssltest/
- Heartbleed Scanner

  http://www.crowdstrike.com/community-tools/
- SSL Certificate Checker

  http://www.digicert.com/help/

Georgia Tech College of Computing

Where to get more information contd.

- Heartbleed vulnerability testing services

  https://en.wikipedia.org/wiki/Heartbleed#Vulnerability_testing_services
- FireFox plugin Heartbleed Notifier

  https://addons.mozilla.org/en-US/firefox/addon/heartbleed-notifier/
- FireFox plugin Heartbleed Monitor

  https://addons.mozilla.org/en-US/firefox/addon/heartbleed_monitor/

Georgia Tech College of Computing

Where to get more information contd.

- Chrome extension Heartbleed Check

  https://chrome.google.com/webstore/detail/heartbleed-check/ionodkjccdnnaibdmcfilldkdigfnhdg

- Chrome extension Netcraft Extension

  https://chrome.google.com/webstore/detail/netcraft-extension/bmejphbfclcpmpohkggcjeibfilpamia

- Chrome extension Chromebleed

  https://chrome.google.com/webstore/detail/chromebleed/eeoekjnjgppnaegdjbcafdggilajhpic

Georgia Tech College of Computing

Where to get more information contd.

- RFC6761 - Special-Use Domain Names (example.com)

  http://tools.ietf.org/html/rfc6761
- Linus's Law

  https://en.wikipedia.org/wiki/Linus's_Law
- Do "Many eyeballs make all bugs shallow"?

  http://www.easterbrook.ca/steve/2009/12/do-many-eyes-make-all-bugs-shallow/

Georgia Tech College of Computing

Where to get more information contd.

- Heartbleed - There Are Not Enough Eyeballs

  https://timboudreau.com/blog/eyeballs/read

- Popular Android apps inherit bugs from recycled code

  http://www.itnews.com.au/News/390365,popular-android-apps-inherit-bugs-from-recycled-code.aspx

Georgia Tech College of Computing

Where to get more information contd.

- Does Heartbleed Disprove 'Open Source is Safer'?

  http://www.datamation.com/open-source/does-heartbleed-disprove-open-source-is-safer-1.html

- Does the Heartbleed bug refute Linus's Law?

  http://esr.ibiblio.org/?p=5665

Georgia Tech College of Computing

Where to get more information contd.

- Did open source matter for Heartbleed?

  http://www.zdnet.com/did-open-source-matter-for-heartbleed-7000028378/

- Heartbleed: Open source's worst hour

  http://www.zdnet.com/heartbleed-open-sources-worst-hour-7000028420/

Georgia Tech College of Computing

Where to get more information contd.

- Heartbleed and misconceptions about Open Source

  http://www.binpress.com/blog/2014/04/12/heartbleed-misconceptions-open-source/

- OpenSSL Project Roadmap (analysis of project issues)

  https://www.openssl.org/about/roadmap.html

- Open source

  https://en.wikipedia.org/wiki/Open_source

Georgia Tech College of Computing

Where to get more information contd.

- Closed source

  https://en.wikipedia.org/wiki/Proprietary_software
- Linux Foundation announces new backers

  http://www.linuxfoundation.org/news-media/announcements/2014/05/core-infrastructure-initiative-announces-new-backers

Georgia Tech College of Computing

Where to get more information contd.

- OpenSSL to get a security audit and two full-time developers

  http://arstechnica.com/information-technology/2014/05/openssl-to-get-a-security-audit-and-two-full-time-developers/

- Core Infrastructure Initiative

  http://www.linuxfoundation.org/programs/core-infrastructure-initiative

Georgia Tech College of Computing

Where to get more information contd.

- Forking software

  https://en.wikipedia.org/wiki/Fork_(software_development)
- LibreSSL (OpenSSL replacement)

  http://www.libressl.org/
- BoringSSL (OpenSSL replacement)

  http://arstechnica.com/security/2014/06/google-unveils-independent-fork-of-openssl-called-boringssl/

Georgia Tech College of Computing

Where to get more information contd.

- Responsible disclosure
  - https://en.wikipedia.org/wiki/Responsible_disclosure
- Was The Heartbleed Bug Disclosed Responsibly?

  http://www.forbes.com/sites/richardstiennon/2014/04/16/was-the-heartbleed-bug-disclosed-responsibly/

Georgia Tech College of Computing

Where to get more information contd.

- More on Heartbleed (responsible disclosure)

  https://www.schneier.com/blog/archives/2014/04/more_on_heartbl.html

- Staying ahead of OpenSSL vulnerabilities (responsible disclosure)

  http://blog.cloudflare.com/staying-ahead-of-openssl-vulnerabilities

Georgia Tech College of Computing

Where to get more information contd.

- Heartbleed: One Bug to Rule Them All (responsible disclosure)

  http://labs.nagios.com/2014/04/10/heartbleed-one-bug-to-rule-them-all/

- Heartbleed SSL Flaw Angst Aggravated by Broken Disclosure Process

  http://www.eweek.com/security/heartbleed-ssl-flaw-angst-aggravated-by-broken-disclosure-process.html

Georgia Tech College of Computing

Where to get more information contd.

- The Heartburn Over Heartbleed: OpenSSL Memory Leak Burns Slowly (responsible disclosure)

  http://www.arbornetworks.com/asert/2014/04/heartbleed/

- Sydney Morning Herald heartbleed time line (responsible disclosure)

  http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html

Georgia Tech College of Computing



Where to get more information contd.

- U.S. CERT

  http://www.cert.org/

Georgia Tech College of Computing