



NASA IV&V and the Heartbleed Vulnerability

Presented by Rick Hess
Sept 10, 2014



- What is OpenSSL
 - OpenSSL Heartbeat
 - From Heartbeat to Heartbleed
 - Example use of the Heartbleed Vulnerability
 - From a Low Level
- What versions of OpenSSL were effected
 - Maintenance Concerns
- How can NASA Protect Against This Type of Issue
- Results
- What has happened since...
- Takeaways
- Special Thanks
- Questions



- According to Google, “OpenSSL is an open-source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols”
 - The core library, written in the C programming language, implements the basic cryptographic functions and provides various utility functions
 - Wrappers allowing the use of the OpenSSL library in a variety of computer languages are available
 - It’s free
 - **As of 2014, 2 out of 3 Web Servers use OpenSSL**

Reference (<http://en.wikipedia.org/wiki/OpenSSL>)



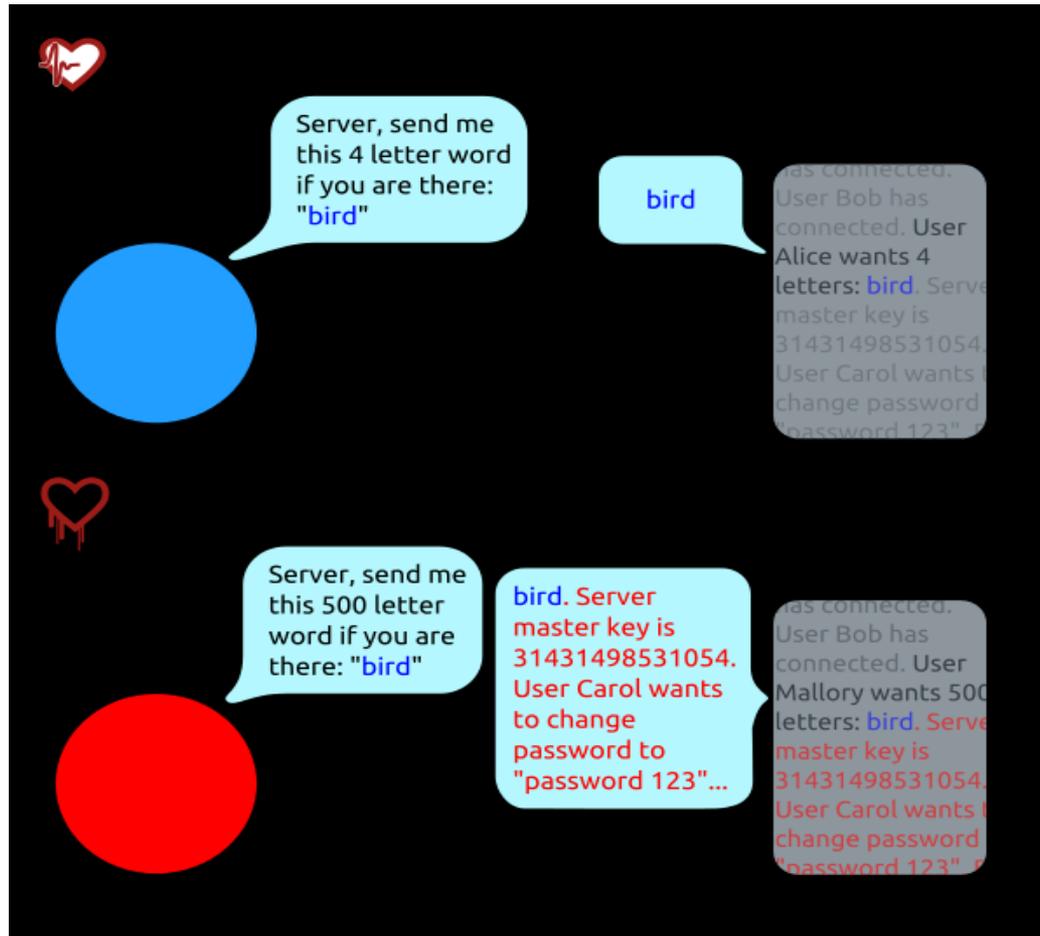
- The Heartbeat Extension for the TLS and Datagram Transport Layer Security (DTLS) protocols
- It provides a way to test and keep alive secure communication links without the need to renegotiate the connection each time



- According to Mark J. Cox of OpenSSL, Google's security team reported Heartbleed on April 1, 2014
 - This defect could be used to reveal up to 64 kilobytes of the application's memory with every heartbeat
- The affected versions of OpenSSL allocate a memory buffer for the message to be returned based on the length field in the requesting message, without regard to the size of actual payload in that message



Example use of the Heartbleed Vulnerability



Reference (<http://en.wikipedia.org/wiki/Heartbleed>)



- **Memcpy(bp, pl, payload)** copied the data from the buffer to the data being sent out
- The variable 'payload' is used to store the size
 - It begins uninitialized and is specified per the user, not by the system
 - It is a 4 byte array, unsigned



What Versions of OpenSSL Were Effected

- The Heartbleed “Bug” was introduced to OpenSSL in December 2011 and has been out in the “wild” since OpenSSL release 1.0.1 on 14th of March 2012
- **OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug**
 - OpenSSL 1.0.1g is NOT vulnerable (it was fixed in this version)
 - OpenSSL 1.0.0 branch is NOT vulnerable (Vulnerability was not introduced yet)
 - OpenSSL 0.9.8 branch is NOT vulnerable (Vulnerability was not introduced yet)



Maintenance Concerns for OpenSSL

- According to ZDNet.com
 - Steve Marquess, OpenSSL Software Foundation president, said that even if the small donations arrived at the same rate indefinitely, **it would not be enough for the project**
 - "It is nowhere near enough to properly sustain the manpower levels needed to support such a complex and critical software product"
 - Marquess said that the project needed half a dozen full-time employees, at least, for the project to be better managed, and that a special personality was needed to work with current funding
 - Striking out at comments that OpenSSL made a sloppy mistake that broke the internet, Marquess said that it wasn't a mystery that overworked OpenSSL volunteers missed the bug, **but that it hadn't happened more often.**
 - "Given the widespread use of OpenSSL over many years it still has an excellent track record"
 - "Two years passed before Google with its impressive technical resources and talent (and shortly thereafter Codenomicon) found this issue"



How can NASA Protect Against This Type of Issue

- A request was sent out to determine if tools exist to find the Heartbleed issue
- A quick turnaround effort was created between SCAWG and SWAT to answer this request



- After working with multiple tools on this idea, at least one of these tools was able to be used to find the defect out of the box, in addition to the Analyst's knowledge on Static Code Analysis
- We have added the Heartbleed Defect to our list of checks within our Tool Capabilities Matrix
- **Question:** Since we were able to use SCA tools to detect this issue, could there be more defects?



What has happened since...

- A collaboration of different companies (Linux, Google, IBM, Microsoft, etc.) has come together to support Critical Open Source Projects, called the **Core Infrastructure Initiative**.
- The Core Infrastructure Initiative website claims “The steering group will work with an advisory board of esteemed open source developers to identify and fund open source projects in need”
- <http://www.linuxfoundation.org/programs/core-infrastructure-initiative>



- It is OK to question 3rd party libraries
 - We can't always assume that they have been fully tested at the level of detail that we expect
- You just can't assume adequate testing has always been performed
- If you would like more information, please contact the Static Code Analysis Working Group (SCAWG) or the Software Assurance Tools team (SWAT).



Special Thanks

- Jerry Williams
- Chris Williams
- Marcus Fisher
- Rich Brockway



Questions?

