



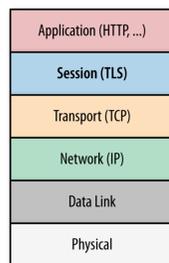
Computer Security Matters: An Exploration of the Heartbleed Exploit

Erin Davis, '14



Background of Heartbeats

What is TLS?



Who uses OpenSSL?

Apache and nginx both use OpenSSL, and those two open source web servers run 66% of the Internet's active sites.

What is OpenSSL?

An open-source, free implementation of TLS/SSL. You can find more information about it at <https://www.openssl.org/>

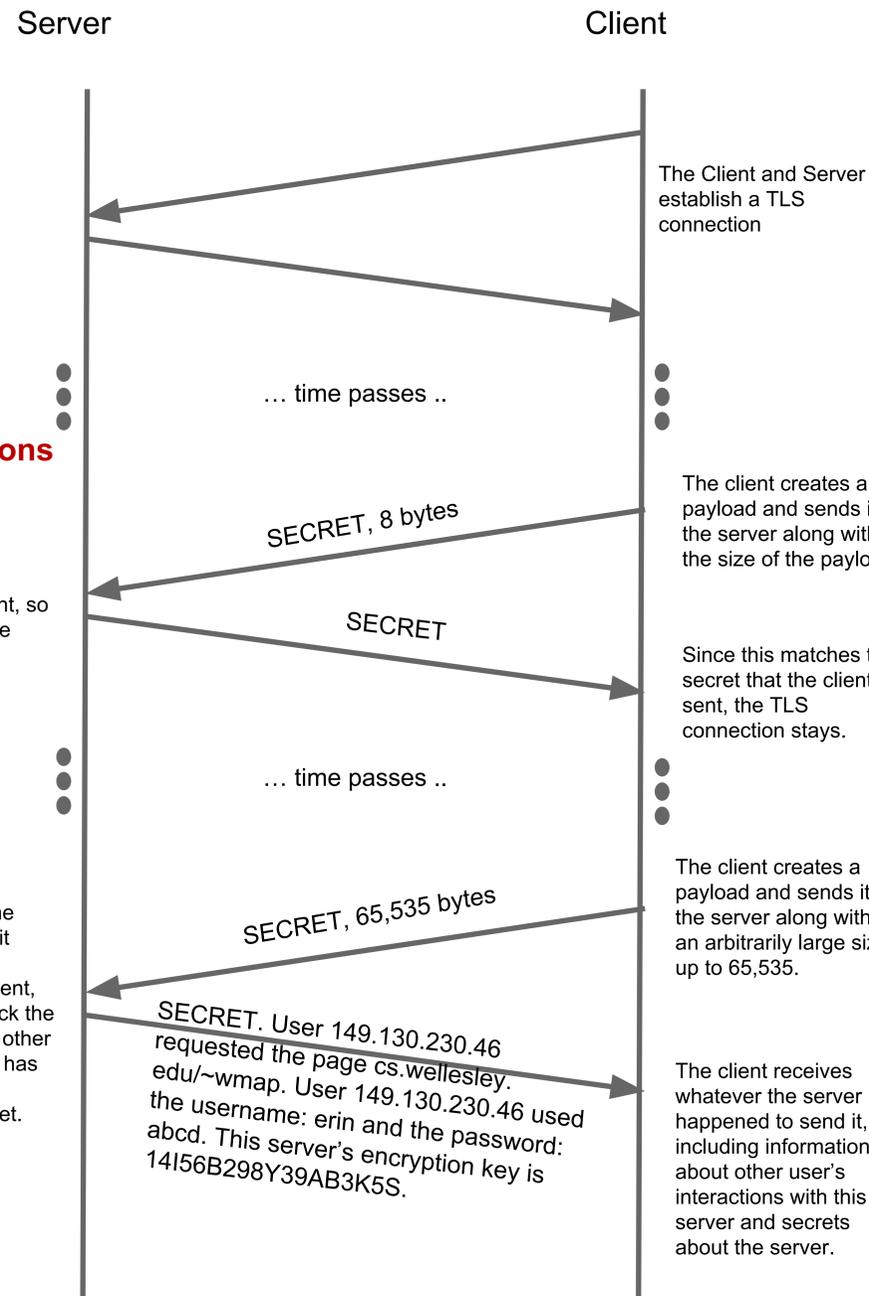
What is the heartbeat? How does it work?

Initiating a TLS connection takes a long time, but once you have a connection established, continuing it should not take as long. The heartbeat is a way to minimize OpenSSL traffic and time costs by sending a keep-alive message periodically. To confirm that the server and client still have a solid connection, the client sends a random set of bytes, and the server responds with the same set of bytes. After those bytes are confirmed to be the same, the connection remains. This decreases the overhead of repeating the TLS handshake.

How long has it been around?

The heartbeat was first introduced in the version of OpenSSL from December 31, 2011.

How does the Heartbeat become a Heartbleed?



HEARTBEAT Under Normal Conditions

The server receives the payload, decides that it wants to continue its connection with the client, so sends the client back the clients secret.

HEARTBEAT Being Exploited

The server receives the payload, decides that it wants to continue its connection with the client, so sends the client back the clients secret plus the other information the server has stored in the 64KB of memory after the secret.

The Extent of Devastation

What information can a hacker steal?

"We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials we were able to steal from ourselves the secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication." [1] Anything stored in memory with the TLS process on the server is possible to retrieve.

How much information can a hacker steal?

A hacker can get up to 64KB of data at once, but can repeat this exploitation multiple times. 64 KB is the largest amount of data whose size can be encoded in 2 bytes.

How much has been infected?

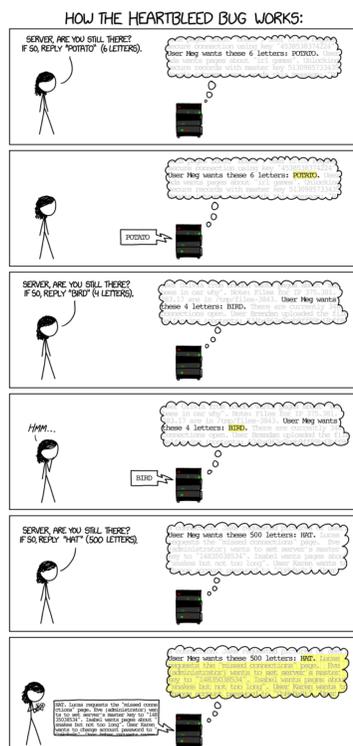
Any server running a version of OpenSSL from 2012 or later has this bug. This is about 66% of the Internet's active sites.

But how do you know if this has been exploited?

That's the scary thing: you can't. "The attack can be performed anonymously in an undetectable manner for typical web server configurations" [2].

So you have no idea if it's been exploited and how much?
Yes.

XKCD's Explanation



Computer Security is Everywhere



Hacker holds key to free flights

Xbox password flaw exposed by five-year-old boy

lifehacker

PSA: Teach Your Friends and Family About "Tech Support" Scams

Massive Security Bug In OpenSSL Could Affect A Huge Chunk Of The Internet

Posted Apr 7, 2014 by Greg Kumparak (@grg)

SECURITY
The Target Credit Card Breach: What You Should Know

40 million shoppers could be at risk for credit and debit card fraud.