The Effects of HeartBleed on Certificate Change

Siyu Chen, Timothy Kelley, Zheng Dong and L. Jean Camp

Human and Technical Security Research Group
School of Informatics and Computing, Indiana University Bloomington

Introduction

A recent vulnerability called HeartBleed compromised a core security protocol of the web. HeartBleed enabled attackers to obtain the private key of X.509 certificates. The mitigation of this vulnerability required two steps. First, vulnerable parties needed to patch and upgrade to the next version of OpenSSL. Secondly, the vulnerable parties needed to obtain a new public key certificate with updated keys. Before and after HeartBleed we had thirteen PlanetLab certificate observatories that had been collecting certificates from the top million websites since 2012. Here we report on certificate changes for the two month period before and after the associated patches of HeartBleed were released.

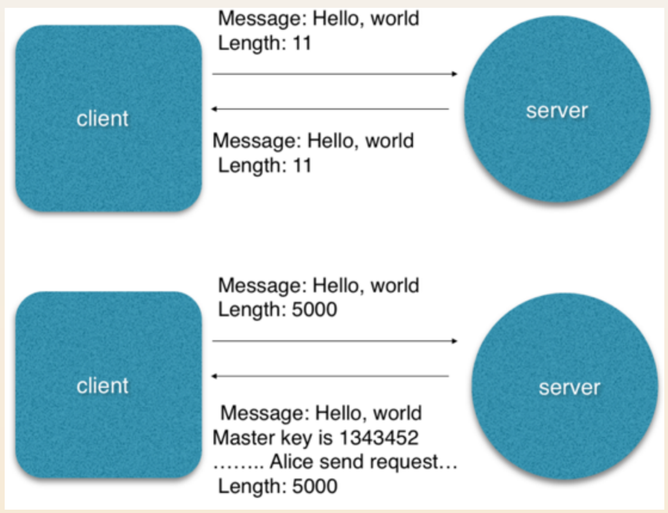

Fig.0 HeartBleed Attack

We find a significant increase in the rate of renewal. There were 246,776 unique certificate changes in 2014 (average 20,563 per month); 46,550 (23,275 per month) unique changes in last two months before HeartBleed and 82,011 (41,005 per month) changes in first two months after HeartBleed, which corresponds to a replacement of on the order of ten percent of the certificates effected. This was considered quite small given the scope of the vulnerability. The new certificates were significantly but not consistently cryptographically stronger than the ones replaced. We also examine the fields and extensions in the newly issued certificates and visualize notable changes.

Data Preparation

- Data Collection: We have a local server to download certificates of Alexa's Top 1 Million websites through port 443. We also use PlanetLab servers to help us cover more certificates all over the world.

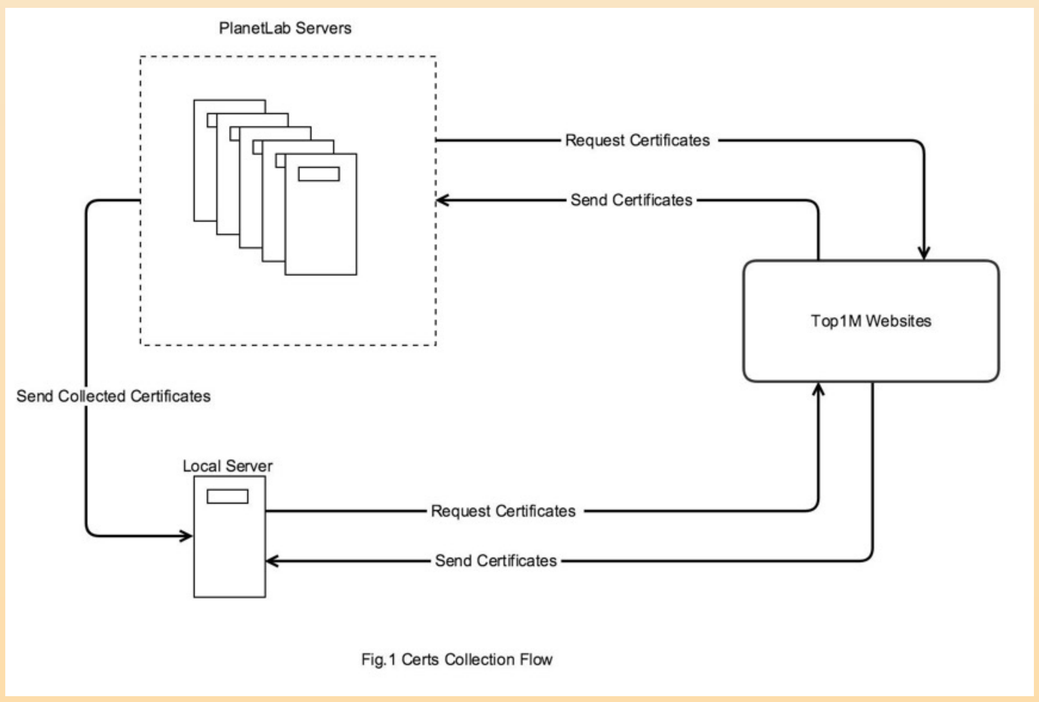

Fig.1 Certs Collection Flow

- We analyze the certificates mainly from two aspects:

1. Extracting all unique certificates during 02-07-2014 to 04-07-2014 and during 04-07-2014 to 06-07-2014. The two time periods are 60 days before and after HeartBleed disclosure. Then we compare the number of certificates for each X.509 field before and after.
2. Regarding server domain name and IP address as a pair. For each unique pair, if its certificate changed after 04-07-2014, we record both previous certificate and new certificate.

Results

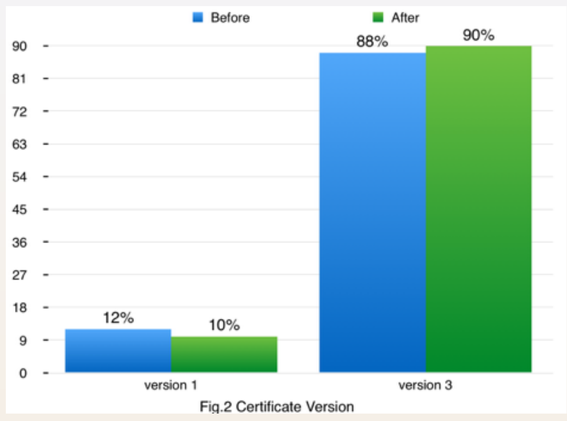

Fig.2 Certificate Version

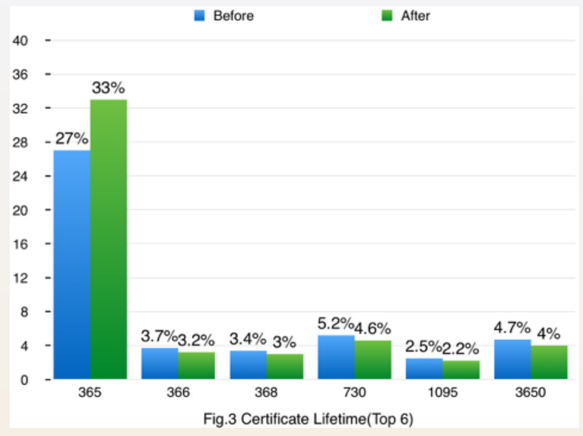

Fig.3 Certificate Lifetime(Top 6)

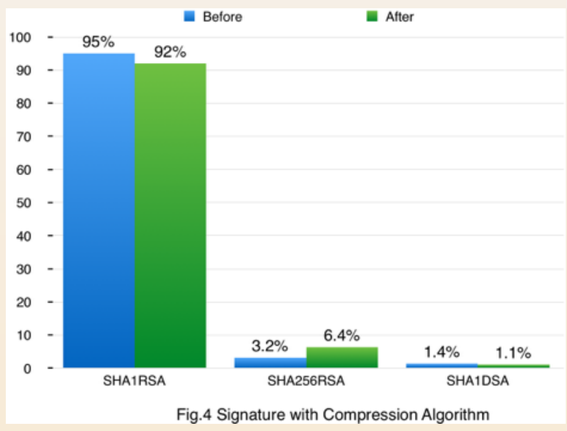

Fig.4 Signature with Compression Algorithm

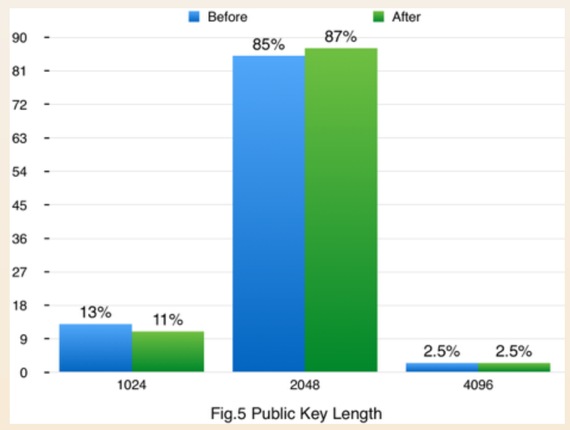

Fig.5 Public Key Length

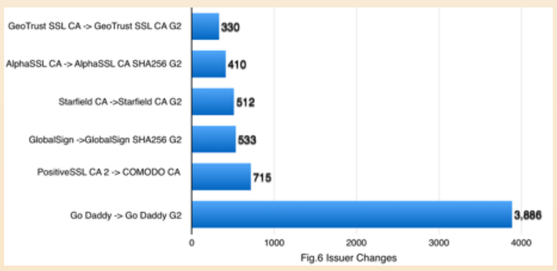

Fig.6 Issuer Changes

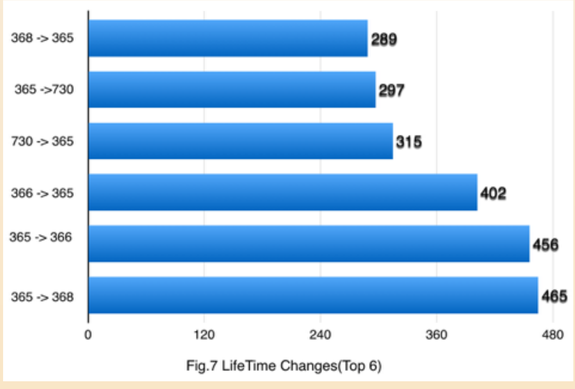

Fig.7 LifeTime Changes(Top 6)

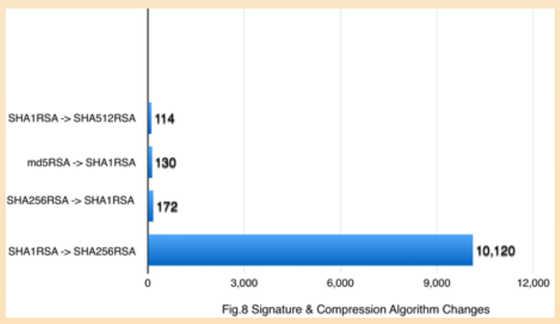

Fig.8 Signature & Compression Algorithm Changes

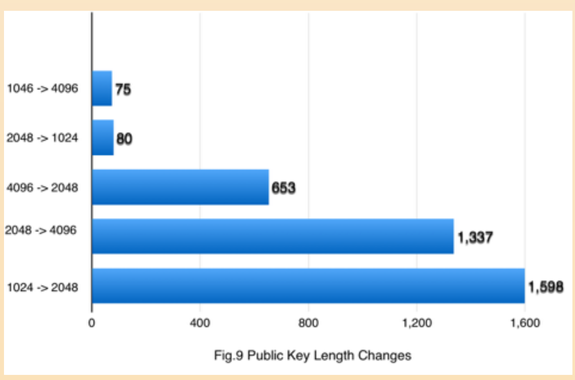

Fig.9 Public Key Length Changes

Conclusion

Within sites that updated their certificates in light of HeartBleed, the data demonstrate specific patterns that define the changes in the two months after HeartBleed. More certificates updated to version 3 certificates, and a majority of certificates increased the size of the public key. Renewed certificates set their new lifetime to 365 days. And while SHA1 certificates continued to be released, the use of SHA256-based certificates increased. Another notable change is issuer changes. Most issuers changed their name to G2 to indicate they have switched to SHA256.

Acknowledgements

Cyber Security CRA W911NF-13-2-0045 (ARL); DHS Contract N66001-12-C-0137, unrestricted research funds from Cisco, and Google. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies or views, either expressed or implied, of the DHS, ARL, DoD, Google, Cisco, IU, or the U. S. Government.