Scott Christensen

10/21/16

C.S. 465

H.W. #9: Weak RSA Moduli bug

For what I got out of the article, there was a supposed vulnerability in RSA, independently found by Arjen Lenstra and James P. Hughes, and Nadia Heninger. Should their original claim have been the whole story, we would all be in BIG trouble. However, they later posted results that this bug had made itself manifest only because of poor public key design. That is how attacks were successful. These attacks went under the assumption that the RSA private key was shared between two public keys. The researchers then assured the public that there was nothing wrong with any website on the internet.

The article went on to explain how the researchers found this fact out by explaining the basics of RSA, then to explain how they compared each RSA key against every other RSA key on the Internet. It was a staggeringly large number, but their algorithm was able to do all of the comparisons simultaneously.

Lastly, the lesson/ message of the article was shared. The article explained that the real problem did not have root in RSA itself, but in the expired certificates and bad public keys that brought about this phenomenon. The real problem was in fact basic key management. If public keys are not enrolled into the global PKI managed by the Certificate Authorities, there is going to be more problems than just this obscure weak RSA moduli bug. Most any data can be compromised if the parties involved do not use proper certificate and key distribution, which is usually the common case of nearly all security breaches.