Dallin Christensen

CS 465

HW 9 – Weak RSA Moduli Bug

Multiple researchers independently found a flaw with the way RSA public keys are generated that can expose the private keys. Due to low entropy in the random prime generators, it is possible to find a prime value p that was used in public key generation for multiple RSA keys. This p is found by taking the GCD of two or more susceptible RSA keys.

This is a major problem because it affects not just RSA, but all forms of cryptography that rely on random numbers. If randomly generated numbers can be predicted or derived, all of the cryptographic technologies that rely on that generator are essentially unsecure. Luckily this bug doesn’t really matter to websites that rely on certificates; they should be fine.

The most important lesson that I learned from this article is that our random number generators need to have true entropy. Specifically, CPUs should be built with hardware random number generators that have high entropy. I also learned that vulnerability in random number generation essentially destroys any amount of security that keys/certificates may claim to have.

After reading this article, my main questions were “How much does this security vulnerability matter in my life? Is any of my private data at risk?” Another question I had was “What can I do to prevent cryptographic vulnerabilities in the devices I use?”