A Summary of ‘Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices’

Ally Smith

due April 28, 2022

This paper was quite interesting. I found it very impressive that they analyzed the entire public IPv4 space and collected tens of millions of TLS certificates and SSH keys. I was shocked at the number of private keys for the TLS and SSH they were able to compute. It seems as if they conducted a comprehensive study as to the vulnerabilities that enabled them to compute these keys. One of the vulnerabilities that I found most interesting was the repeated keys due to low system entropy. It makes sense that small embedded devices have a limited entropy pool, due to the lack of user interaction. However, many of these devices still require accessing `/dev/urandom` and therefore run into issues. I am interested to see the presentation during class to see if they cover any possible solutions to this problem. Overall, I think that the methodology that they used to scan and analyze the keys is very promising for future research. As mentioned in the paper, by scanning the keys that actually exist in the world, researchers can find vulnerable keys far faster than previously possible. In the past, individual hardware systems were reverse engineered or flaws were observed and recorded by a user. I hope that the presenters in class discuss some potential uses for this methodology.