University of Windsor

SAC2022

Invited Talk:

On the passive compromise of TLS keys and other cryptanalytic adventures

Nadia Heninger

Abstract: It is well known in the cryptographic literature that the most common digital signature schemes used in practice can fail catastrophically in the presence of faults during computation. I will discuss recent joint work using passive and active network measurements to analyze organically-occuring faults in billions of digital signatures generated by tens of millions of hosts. We find that a persistent rate of apparent hardware faults in unprotected implementations has resulted in compromised certificate RSA private keys for years. Finally, we will put this work in the context of other cryptographic flaws that can be exploited in the wild.