A Summary of 'Analyzing Forged SSL Certificates in the Wild'

Ally Smith

due April 28, 2022

This paper was quite interesting to me, as I have done research in the past on issues with PKI and forged certificates. This paper helped me get a better grasp of just how many systems are affected by the things I was researching. In particular, I found the idea that users who skip SSL certificate warnings are extremely susceptible to man-in-the-middle attacks using self-signed certificates. Frequently, I will run into websites that have expired certificates, and will ignore the warning if I need to access the website. After reading this paper, however, I will think twice before continuing to the sites. One thing I found quite shocking is that browsers do not have direct access to the certificates of the sites you visit. Instead, the researchers had to use Flash to access these elements. This seems like a large oversight on the part of the browsers' developers. However, it is possible that providing access to this could be used maliciously. Additionally, I found it the fact that 0.2% of real-world connections are forged to be surprisingly low. Perhaps it is because the connections that are forged get marked as revoked upon discovery, but I thought that the vulnerabilities of forged certificates would be a higher risk.