Digital Fingerprints

Kingston Armstrong

Computer Science 3

Mr. Ben-Yaakov

The internet is something we all use. We use it to play games, listen to music, talk to other people, and even manage our sensitive information. To do some of these things we need a Secure connection. One that will not let other people look at our Internet traffic. In the early days of the internet, HTTP (Hypertext Transfer Protocol) allowed anyone between you and the webserver to see your data. But in 1994 Netscape Communications created HTTPS. HTTPS is just HTTP but secure that is what the S on end stands for. The purpose of an HTTPS connection is to allow the transfer of data between the user and the webserver and encrypt that data so anyone between you and the webserver can't see your data. This is a good thing that has dramatically improved the security of the internet, but some organizations that love controlling everything that their users or employees do developed a technology called HTTPS Proxy Appliances. These devices can trick your browser into thinking it's securely connected to the remote site by creating a fake certificate, but in the real world, the person with the proxy can easily read all your internet traffic.

The person with the proxy is known as a MAN IN THE MIDDLE, aka MITM. This is risky because you don't know what that person in the middle is doing with your internet traffic. You are completely in the dark with your data that was thought to be secure. Right now you may be freaking out right now, not knowing if the internet is a safe place at all for any of your sensitive information, but it is ok because you can detect if your data is being intercepted with hashes. These proxy appliances are able to trick your browser with a fake certificate but they are not able to completely copy any website's certificate. When examining this certificate you can create a hash of it a.k.a a Digital fingerprint. A Hash is a bunch of "*complex mathematical*

algorithms which carefully process every single bit of what they "digest." They have the amazingly property that if even one bit inside the certificate is changed, an average of half of the fingerprint's hash bits will change in response!"(Steve Gibson) That means when you create this fingerprint of the fake certificate it will be nothing like the real one meaning you can detect when you have a MITM. A Certificate Authority (CA) is a trusted establishment that will sign the certificates of websites. This is something websites have to provide when the browser checks it. It checks the signature and compares it to many of the CAs it trusts to sign website identities. SSL interception is not something that you can turn off when connecting to a wifi network it is either there or it isn't. The only way to truly know is to check with fingerprints and only connect to trusted wifi networks. A false positive is when people think that there is a MITM while there isn't. This is due to big websites having a lot of security certificates and when people check them they might compare one valid one to a different valid one. A False negative would be when you have something in the middle and it somehow tells you there is not one. I don't think that schools or any organization have a right to eavesdrop on my communications. People have a right to privacy and As the Supreme Court wrote, students "do not shed their constitutional rights at the schoolhouse gate." So I believe that students have a right to privacy at school and everywhere. Many people say that the United States was built on having freedoms. Having someone able to read all your internet traffic isn't very free.'

References

Steve Gibson, G. I. B. S. O. N. R. E. S. E. A. R. C. H. C. O. R. P. O. R. A. T. I. O. N. (n.d.). *GRC : SSL TLS HTTPS web server certificate fingerprints*. GRC | SSL TLS HTTPS Web Server Certificate Fingerprints Retrieved September 18, 2022, from https://www.grc.com/fingerprints.htm#top