HTTPS Connections and Fingerprints

Jishnu Devarapalli
Allen High School, STEAM Campus
Computer Science II
Mr. Ben-Yakov
September 21, 2022

HTTPS

The primary purposes of a secure HTTPS connection are to ensure that all data coming and going from the site is encrypted and also to make sure that the user is on an authentic site. An HTTPS Proxy Appliance is a way that an organization such as a school or company monitors the data of their students or employees using a fake authenticator in order to trick the browser into thinking that the site is secure. This allows the organization to view or manage or set restrictions on data.

MITM

A MITM is a man-in-the-middle attack which is when someone intercepts your data. This presents the risk of someone stealing your data when it is coming or going.

Hash

A hash is a mathematical algorithm that digests an SSL certificate's contents even if there is a small change in the certificate the hash will be drastically changed.

Certificate Authority

A certificate authority is an entity that signs and issues certificates to websites that they think are trusted. Essentially a certificate authority puts their stamp of approval on websites that they believe to be legitimate; they essentially stake their reputation on the fact that the website is trustworthy.

SSL interception

An SSL interception cannot be prevented but it can be detected because it is very difficult to fool a security certificate. An SSL interception can be detected by looking at the fingerprint, if the website is fraudulent the fingerprint will be different.

False Positives and Negatives

A false positive is when it seems like the certificate is unauthentic but in actuality the sites, although they are from the same company, may use different certificates.

Another way to get a false positive is when the user accidentally compares the wrong certificate. A false negative is when it seems like there was no interception but there actually was. One case where that can happen is when the user verifies a certificate and it seems to be authentic but actually, that connection was specifically ignored and other connections are being intercepted.

Does your school/government / ISP have a right to eavesdrop on your communications?

I think that organizations shouldn't be able to eavesdrop on communications as it is a breach of privacy. Additionally, it causes people to distrust the organization

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 August 24, 2022, from https://www.grc.com/fingerprints.htm#top

What is MITM (man in the middle) attack: Imperva. Learning Center. (2019, December 29). Retrieved September 17, 2022, from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/