Frederick Brehm

6/4/2024

CS 305

SNHU

Certificate Authorities help secure the internet for organizations and users. The goal of a CA is to verify that a website, domain, and organization are authentic so users can be certain that they are communicating safely and whether that specific entity can be trusted with their data. SSL or Secure Sockets Layer is a communication protocol or set of rules that creates a secure connection between devices on a network. TLS or Transport Layer Security is an upgraded version of SSL that has fixed SSL’s vulnerabilities. TLS uses SSL certificates to encrypt and authenticate data for HTTPS. HTTP is layered on top of TLS to create HTTPS. HTTPS is critical in providing enhanced protection for applications and websites requiring high security and privacy such as banking, taxes, and online access to payments and personal information. CAs are responsible for maintaining the security of infrastructure and issuing certificates in compliance with industry standards and best practices.

Symantec/Verisign and Comodo are a few examples of CA’s. They can sign cryptographic certificates that are on servers. When a client connects to the server, the server then sends a certificate to the client. If the client trusts the CA that signed the certificate, the client can then trust the server after verifying authenticity. Verification is made possible by public key cryptography which is based off TLS. Once trust has been established between CA, client, and server, a secure channel has been established.

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

References

*What is the role of certificate authorities (CAS)?*. Fortanix. (n.d.). https://www.fortanix.com/faq/public-key-infrastructure/what-is-the-role-of-certificate-authorities-cas

Manico, J., & Detlefsen, A. (n.d.). *Iron-clad Java*. O’Reilly Online Learning. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch06.html#ch06lev1sec1