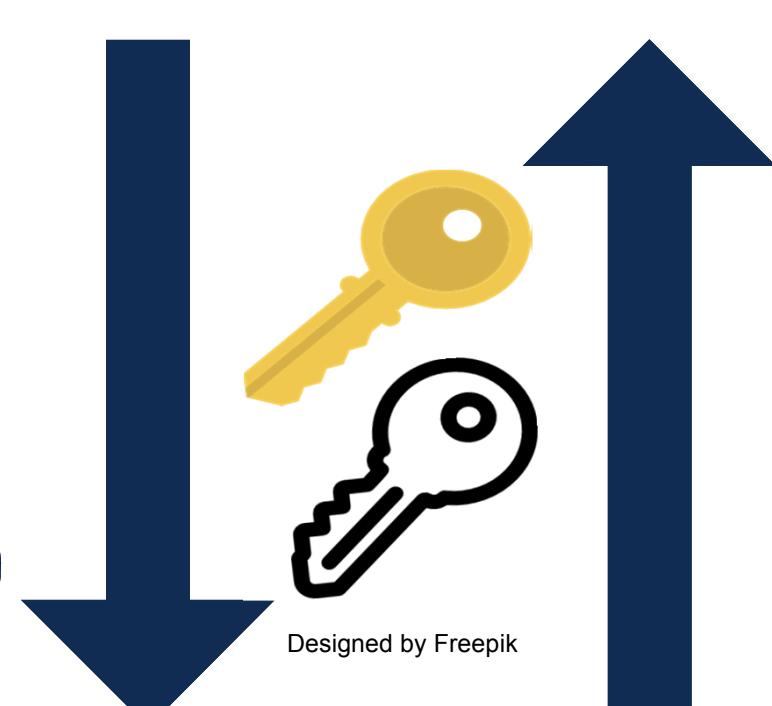
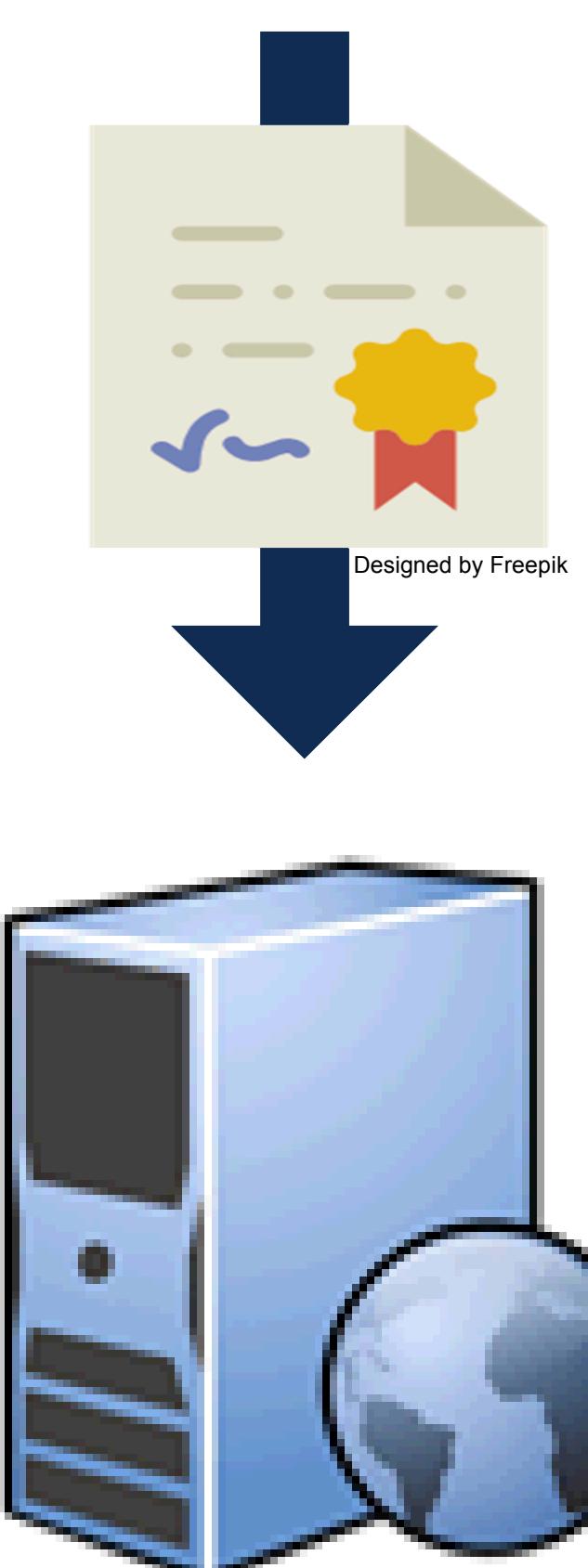


SSL Certificate Blacklisting

Armisha Roberts, Howard University
Kristen Beneduce and Margot Kimura, Sandia National Laboratories



What are SSL (Secure Sockets Layer) certificates?

SSL certificates are a mechanism that allows a user to leverage authentication to ensure that the site one is visiting is the site it is believed to be. SSL certificates are issued by Certificate Authorities (CAs).

How do SSL Certificates work?

Sensitive information is encrypted through the use of public and private keys. The user's browser and the website's server engage in an "SSL Handshake" to ensure security and establish a connection.

What is SSL certificate blacklisting?

Hackers have discovered ways to circumvent, alter, or abuse SSL certificates. One preventative measure to protect users against hackers is to use SSL blacklisting. An SSL certificate blacklist is a list of untrustworthy SSL certificates that have been created and can potentially harm users. SSL Blacklisting stores a living list of certificates that have been compromised or fictitiously created. Blacklisting allows for potential malicious connections to be prohibited which protects your day to day user, you.

