CS50 Cybersecurity

Overview

The Internet is full of security threats. One significant threat is the threat of **cyberattacks**, where hackers attempt to target computer systems and networks for malicious purposes. **Cybersecurity** refers to systems and practices that web sites and users can employ in order to better protect themselves against cyber threats. Users can help to protect themselves against cyber threats through a variety of means, including choosing more secure passwords and being mindful of spam email.

Key Terms

- cyberattacks
- cybersecurity
- phishing
- two-factor authentication
- SSL
- TLS

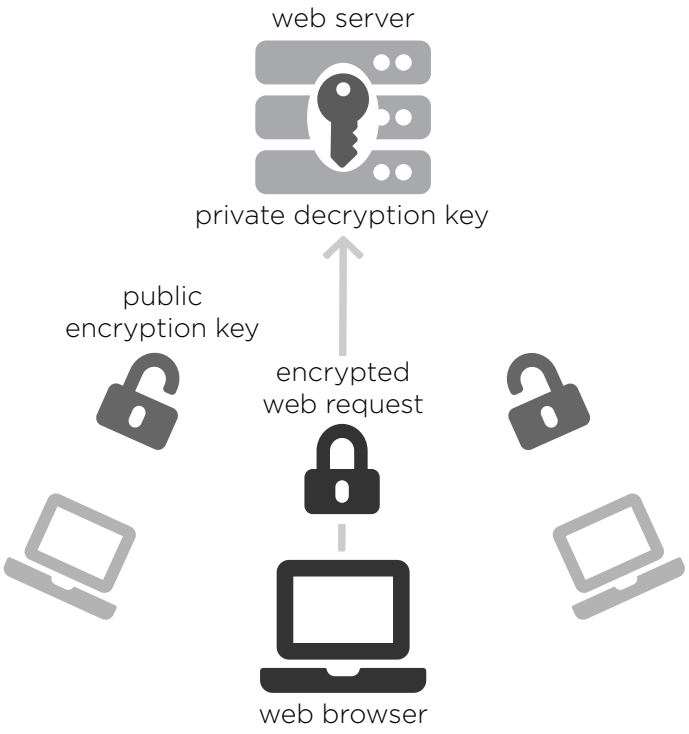
Passwords

Hackers can attempt to obtain passwords in various ways. One way is to try submitting millions of possible username and password combinations until one is successful. This is why choosing a longer and harder to predict password can improve security. Hackers may also attempt **phishing** attacks, where they send emails to users pretending to be a legitimate company and ask users to click on a link that asks for a password or other sensitive information.

Some services (including Google and Facebook) offer **two-factor authentication** as a means of combating possible password theft. Two-factor authentication requires two types of authentication that are inherently different, one factor would be a username and password, while the other factor can take the form a verification code sent via text to your phone or a security question or SecurID, which was a physical device that would generate a random 6-digit integer. Thus a user needs both their password and a secondary device in order to be able to login successfully. However, there is a tradeoff in convenience: if your phone is lost, or do not have access to your phone then you may be unable to access your account.

Website Security

HTTPS (with the "S" standing for "Secure") is a protocol for communication across the internet that combines HTTP and a technology called Secure Sockets Layer (**SSL**). Websites that use SSL each have a certificate, which is distributed to users who are trying to access the website. The certificate secures the connection between the server and the individual and also contains a public encryption key, which tells web browsers how to encrypt requests that are sent to the web server. The web server has another key, the private key, which can decrypt the encrypted requests. As a result, when a user sends an encrypted request to a web server using SSL, the information is more secure. You can generally tell which websites are using this technology by noting whether or not their URLs begin with `https://`



Today, a technology called Transport Layer Security (**TLS**) is more commonly used, but it is just an updated and improved version of SSL.

Other Cyberattacks

Hackers use several other techniques to perform cyberattacks. In a man-in-the-middle attack, a malicious piece of equipment (like a router or DNS server) in between a user and a web server can replace any occurence of `https://` with `http://` in links and redirects. The result is that an adversary can return pages to a user that look like the correct website, but actually are not.

Session hijacking is another cyberattack technique, wherein an adversary monitors network traffic for cookies, and uses the cookie in the adversary's own HTTP headers, tricking a web server into thinking that the adversary is someone else.