HTTP, HTTPS and HSTS

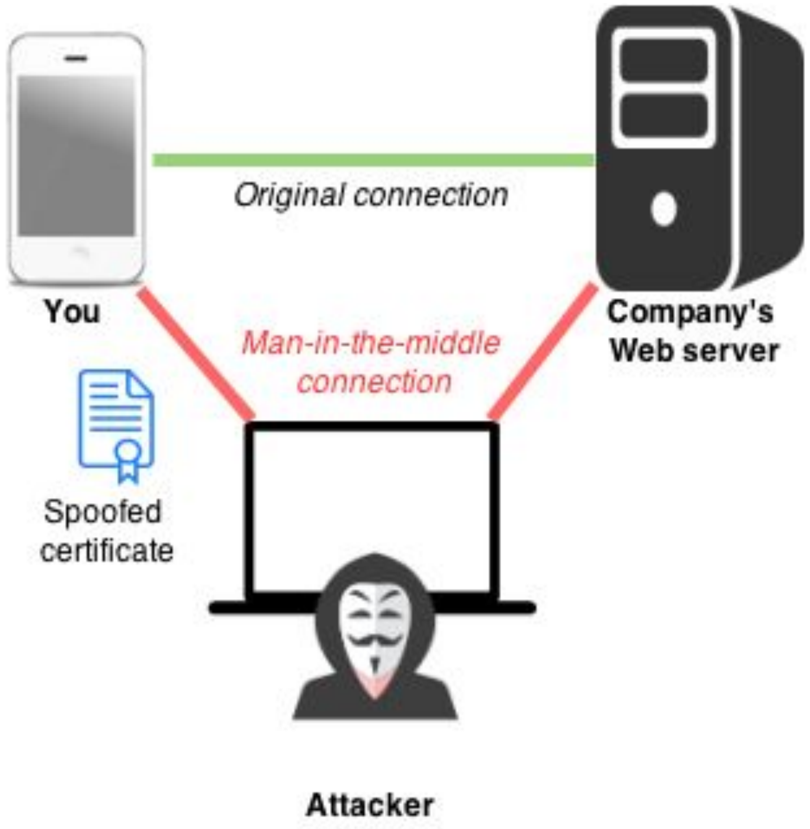
- **HTTP** communicates in clear-text and is vulnerable.
- **HTTPS** (HTTP Secure) uses TLS for encryption and is secure.
- **HSTS** (HTTP Strict Transport Security) enforces only authentic HTTPS connection with domains that are in a preload list. https://hstspreload.org/

Attacks on HTTPS (both of type MITM):

- SSL Sniffing
- SSL Stripping

Hacking HTTPS: SSL Sniffing

- **SSL Sniffing** means performing a man-in-the-middle (MITM) attack on SSL/TLS traffic.
- **The hacker dynamically (on the fly) generates certificates** for the domains that are being accessed and use those spoofed certificates for the part of the connection between him and the victim. All traffic will be sniffed and seen in clear-text.



- The victim's **browser will recognize that the certificate is not authentic** because it's not signed by an authority the browser trusts and will display a security warning.
- The attack will not work on HSTS domains.

Hacking HTTPS: SSL Stripping (HTTPS Downgrade)

- **SSL Stripping** (MITM) will try to downgrade HTTPS connections to their HTTP or unencrypted counterpart.
- In an SSL Stripping attack the hacker will manipulate the redirects and send the victim to the HTTP, unencrypted site. Now the user is still on your site, interacting as he normally would, but every bit of data he transmits is in plaintext.
- SSL Stripping does not convert already established HTTPS connections to HTTP. It only does this in the sense that URLs are rewritten from **https://** to **http://**.
- The attack will not work on HSTS domains.