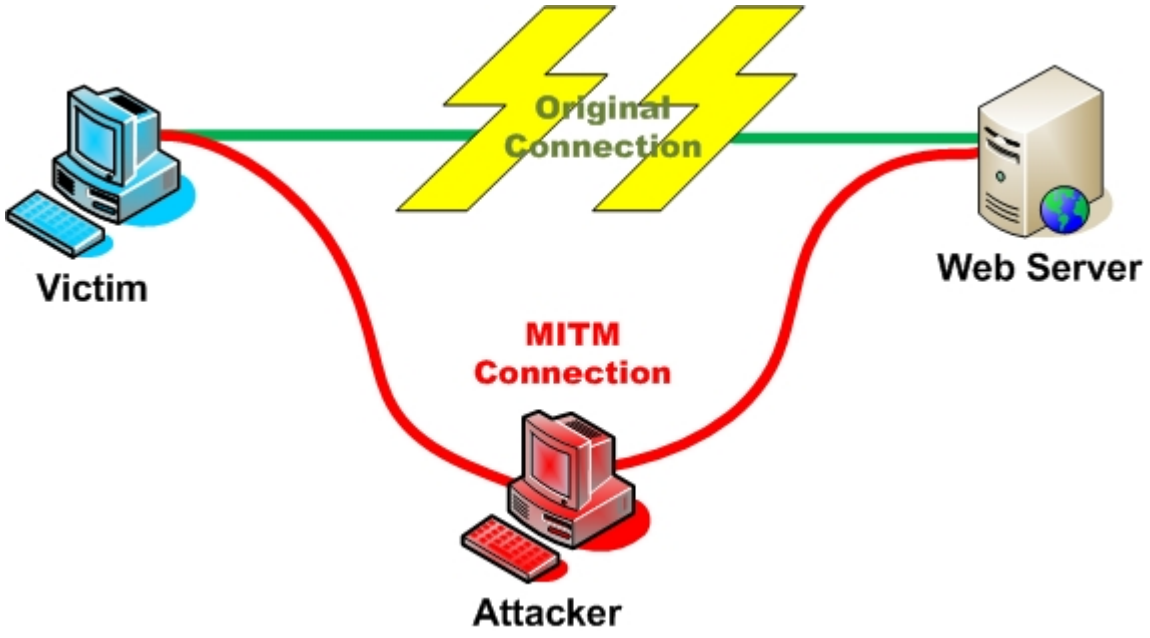
Uzbrukumi bezvadu tīklu klientiem izmantojot MITM (man in the middle) metodi.

Kas ir MITM?

- MITM ir datu plūsmas novirzīšana cauri uzbrucēja iekārtai.
- Upuris par to var neko neuzzināt.



Kas nepieciešams?

- Uzbrucējam jābūt pieejai pie tīkla, caur ko tiek vadīti upura dati.

Kā nokļūt vienā tīklā?

- Publiskie WiFi
- WEP PSK
- WPA/WPA2 PSK – dictionary attack
- WiFI ar ieslēgtu WPS PIN autorizāciju
- Izmānīt paroli

Datu lasīšana

- Wireshark
- Tcpdump

Datu izmainīšana

- ARP spoofing
- WiFi roaming
- Privoxy (http proxy serveris ar filtriem, kas ļauj veikt izmaiņas)
- SSLstrip (nomaina https uz http un kalpo kā https klients)

Iespējamais pielietojums

- Paroļu iegūšana.
- Iefiltrēšanās lietotāja datorā, tā pakļaušana.
- Privātas informācijas iegūšana.
- Naudas zādzības caur internetbanku.

- Veikt uzbrukumus ir vienkārši un lēti.
- To var izdarīt jebkurš (arī 8. klases skolnieki (kaut vai “prikola” pēc)).
- Uzbrucēji jūtas drošāk, jo domā, ka nav redzami un ir nenotverami.

Kā aizsargāties?

- Publiskos tīklos censties lietot https://
- Pārliecināties, ka https sertifikāts ir derīgs, un nelietot lapu, kas lieto neuzticamu sertifikātu.
- HTTPS Everywhere pārlūka spraudnis.

- Uz rūteriem nelietot WEP šifrēšanu.
- Izmantot grūtāk uzminamas paroles.
- Izslēgt WPS (ja to nevar izslēgt – mainīt rūteri).
- Fiziski aizsargāt tīkla iekārtas.

- Būt uzmanīgam.