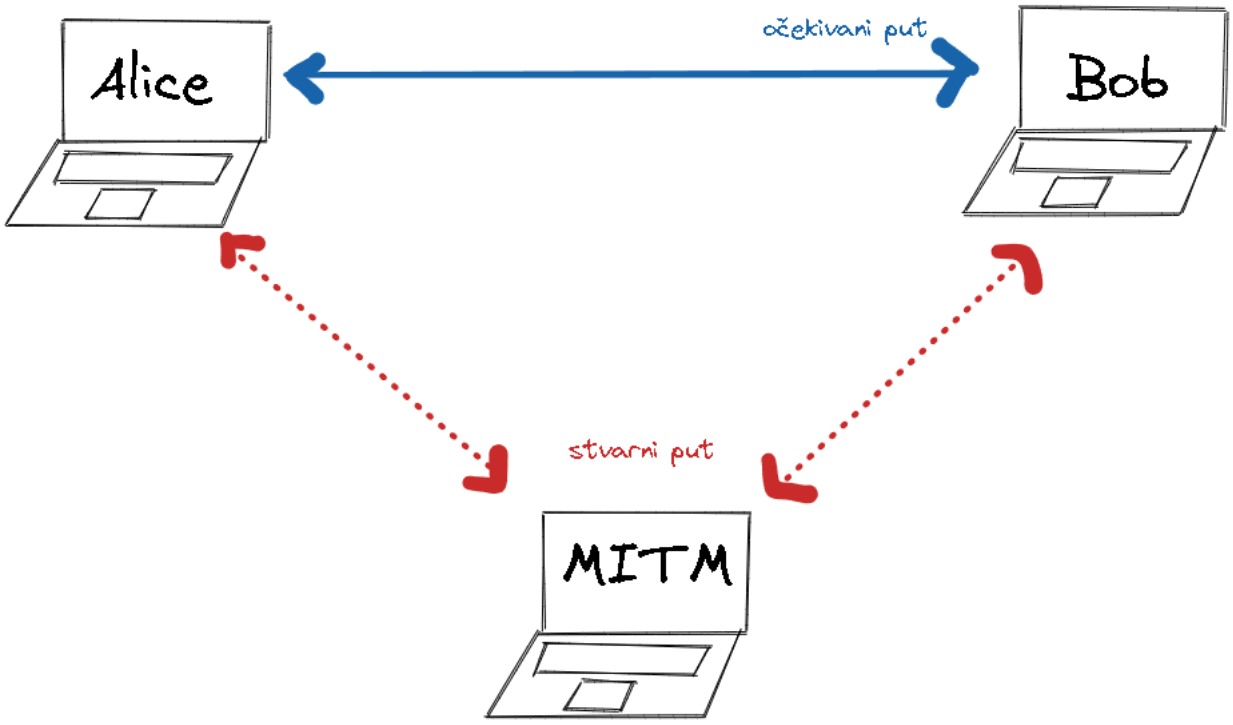
Izvještaj iz 1. laboratorijskih vježbi /SRP/

Man-in-the-Middle Attack [ARP spoofing]

> 💡 ARP (Address Resolution Protocol) je protokol kojim se dobiva fizička adresa na **lokalnoj mreži** iz poznate **mrežne adrese**. IP adrese se povezuju s MAC adresama.

U situaciji kada imamo dvoje kolega, koji su bili zbunjeni predavanjima iz kolegija “Sigurnost računala i podataka”, nek’ se zovu Alice i Bob, koji pokušavaju jedno drugome razjasniti spomenute zbunjoze (važno je za spomenuti da se razgovor vrši preko računala, koji su spojeni na istu lokalnu mrežu, nećemo ulaziti u to zašto ne komuniciraju verbalno…), može se dogoditi da postoji neka osoba koja bi htjela prisluškivati njihov razgovor.

Ta osoba koristeći mane ARP protokola, može ostvariti to da bude “man-in-the-middle”, tj. on postaje dio komunikacijskog kanala i da sav promet prolazi kroz njegovo računalo, gdje ih on može ili pročitati, ili spriječiti da dođu do svog odredišta (denial-of-service). Ovime se narušava **integritet** mreže!



Alice i Bob uopće ne mogu znati da se njihov razgovor prisluškuje jer s njihove strane sve izgleda potpuno normalno. No, naš man-in-the-middle zna da kad kad Alice pošalje poruku Bobu, da ARP protokol znajući Bobovu IP-adresu, zatraži njegovu MAC adresu, i on će tu upasti u priču i odgovoriti na taj zahtjev sa svojom MAC adresom. Zato Alice misli da njene poruke idu Bobu, no zapravo baš i neće.

Docker

Što se tiče konkretnih detalja laboratorijske vježbe, koristeći fizička računala riskiramo integritet mreže zbog toga što je jako puno računala spojeno na tu istu mrežu, pa smo na vježbi koristili virtualno okruženje koristeći **Docker** tehnologiju.

Docker kontejnerima smo simulirali **3 računala** i **lokalnu mrežu** na našem računalu i u tom okruženju smo izvršili demonstraciju “ARP spoofinga”.

Računala su nazvana “**Alice”, “Bob”** i “**Man-In-The-Middle”**. Na početku smo postavili Bobovo računalo kao server, Aliceino računalo kao klijenta i uspostavili smo komunikacijski kanal između njih koristeći ***netcat*** naredbu.

Zatim, na računalu “**Man-In-The-Middle”** palimo skriptu ***arpspoof***. Tu se događa sva čarolija, i sada kada koristimo naredbu ***tcpdump*** možemo presresti sve poruke koje Alice šalje Bobu i obrnuto.

Zaključak

Ono što možemo zaključiti, da ovakve stvari je trivijalno izvesti, i da se ove stvari mogu i hoće događati u stvarnosti. Stoga, naša dužnost je potruditi se obraniti od ovakvih napada, na način da gradimo obranu protiv njih na slojevit način. Prvo bismo se morali osigurati protiv neovlaštenog pristupa mreži, pa bi trebali enkriptirati podatke koje šaljemo mrežom koristeći principe javnih i privatnih ključeva (**Diffie-Hellman key exchange**).