

i. Ta se hrani na disku pri obeh straneh.

ii. - SPI - Indeks SA, ki se uporablja za določanje nastavitev

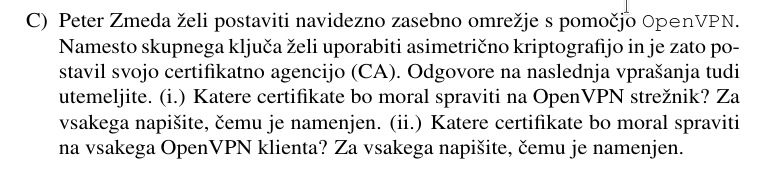
- Seq# - Zaščita proti napadu s ponovitvijo (reply attack)

iii. Če kot polnilo mislite padding v ESP repu, potem je odgovor ne. Padding se namreč uporablja za bločno šifriranje. Sicer bi lahko verjetno s kombinacijo originalnih IP podatkov in polnila, le to uporabili kot neke dodatne podatke, vendar bi morala biti uporaba predefinirana, kar ni ravno smotrno, ker potem ne bi sovpadal povsem z ESP standardom.



Z Seq#, ki je v ESP glavi. Ta zagotovi, da so paketi dekapsulirani le enkrat. Seveda lahko paketi zaradi omrežja pridejo v drugačnem zaporedju, zato dekapsulator vzdržuje Anti-replay Window, ki sledi prejemnemu statusu fiksnega števila prejšnjih sekvenčnih številk.

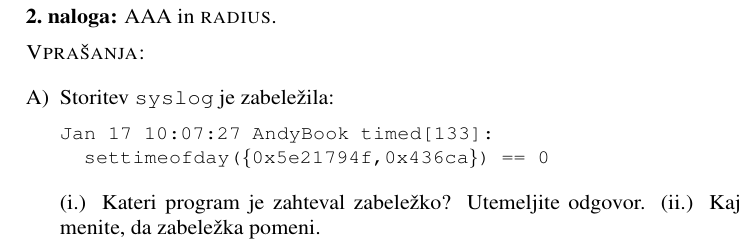
Še daljša razlaga: https://mr.gy/blog/snabb-esp.html



i. Samo generirana certifikat in ključ za strežnik, ter Diffie Hellman parametri . CA master key, ta ni nujno da je sploh na strežniku ali na omrežju. Ključe in certifikate od klientov tudi ne rabimo, saj bo strežnik dal dostop le tistim klientom, ki so bili podpisani z CA master keyem ali pa s strani strežnika.

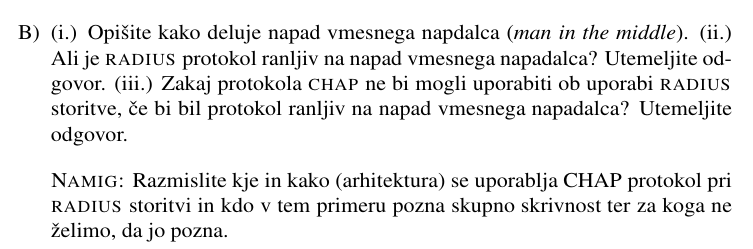
ii. Master CA certifikat, potreben za vzpostavitev, in pa certifikat in ključ klienta. Tadva sta potrebna za avtentikacijo.

Več: https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/



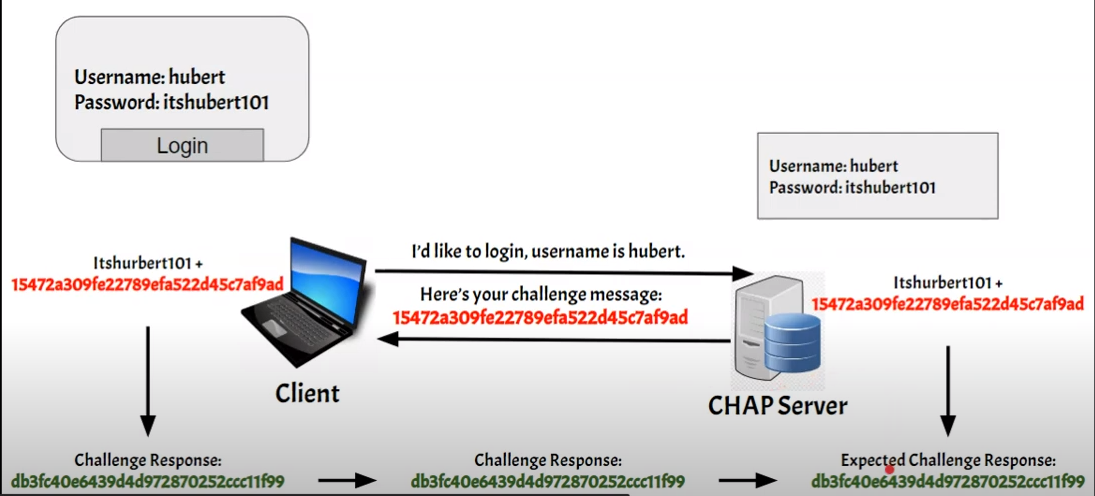
i. zabeleško je zahteval program timed, saj zraven vidimo njegov PID, AndyBook je ime uporabnika, settimeofday pa ukaz.

ii. Ukaz settimeofday je ukaz za nastavljanje časa, torej je čas nastavil na 00:00 oz. polnoč.

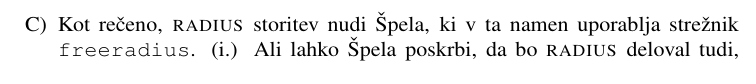


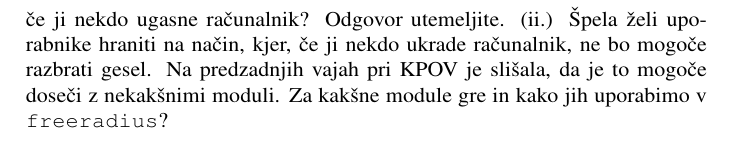
i. Napadalec prestreže komunikacijo in se obnaša, kot da je ciljni sistem (pri uporabi certifikatov lahko žrtev uporablja tudi javni ključ od napadalca).

ii. RADIUS je ranljiv na napad Man in the middle. Podpis je uporabljen kot avtentikacija odgovora in ne ščiti zahteve odjemalca. Za preprečitev tega bi uporabil CHAP.



iii. Ker RADIUS potem ne bi mogel opravljati svoje funkcije suvereno, torej ne bi mogel zagotavljati avtentikacije.



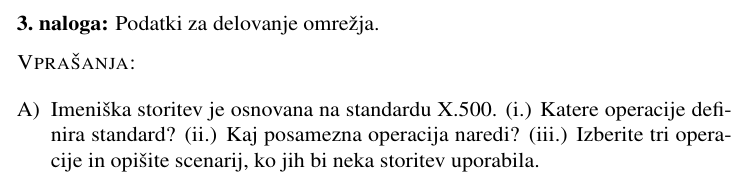


i. Da, lahko uporabi medstrežnike ali gostovanje (roaming).

Mislim, da je tudi možna rešitev Radius in cloud, tako bo vedno delovou. Tudi to bi šlo.

ii. Gre za module, ki jih lahko dodamo freeradius-u, da dodamo funkcionalnost.

Dodamo jih tako da jih inštaliramo in omogočimo z npr: a2enmod auth\_raduis



i. – operacije nad strukturo

ii. Bind (želja po avtentikaciji ter ostalih možnih parametrih komunikacije (inačica, ...). Seja je lahko tudi neavtenticirana.),

unbind (zaključek komunikacije (seje)),

Read,

List,

Search (iskanje posameznih predmetov v bazi),

Compare (možnost primerjave vrednosti

predmeta. Ni potrebno razkriti prave vrednosti

predmeta, samo preverjamo enakost. Primerno za

gesla in podobno),

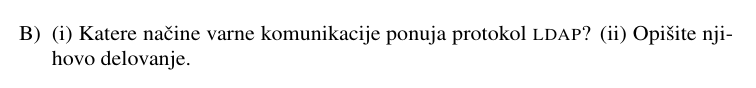
Modify (spremenimo predmet v bazi spremenimo vrednosti prilastkov predmeta),

Add (dodamo predmet v bazo),

Delete (pobrišemo predmet iz baze),

Modify DN (spremenimo ime predmeta (rename)).

iii. Od zgoraj.

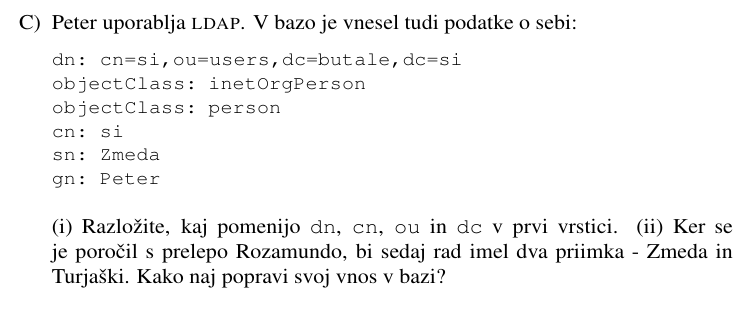


i. - start TLS

- ldaps

ii. - start TLS – preklop na TSL/SSL način komunikacije

- druga možnost je namestitev strežnika na drugih vratih in izvajanje celotne komunikacije prek SSL protokola – ldaps (depricated)



i. dn - distinguishedName

cn - commonName

ou - organizationalUnit

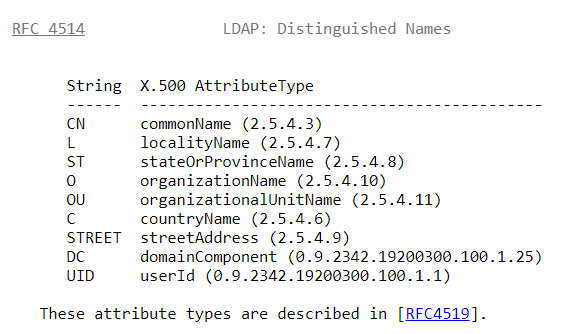
dc - domainComponent

gn - givenName

sn - surname

<https://www.cryptosys.net/pki/manpki/pki_distnames.html>

<https://docs.bmc.com/docs/fpsc121/ldap-attributes-and-associated-fields-495323340.html>



ii. Credit goes to @veso266

Najprej nardimo nek (.ldif datoteko, to je tk k ena .sql skripta)

grem-po-strik-andy-prit-na-pogrep.ldif

tole damo notr

*dn: cn=si,ou=users,dc=butale,dc=si*

*changetype: modify*

*replace: sn*

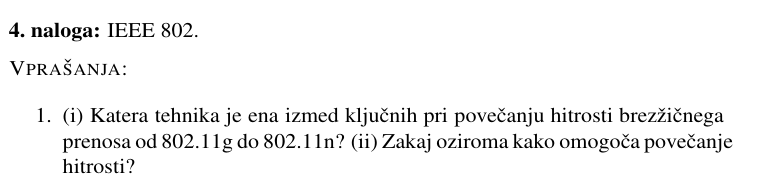
*sn: Zmeda Turjaski*

po pa na ldap strežnik s tem orodjem gor spravmo:

*ldapmodify -x -h ldap://localhost -D cn=si,ou=users,dc=butale,dc=si -W -f grem-po-strik-andy-prit-na-pogrep.ldif*

če ni -f lohka kr direkt ukaze pišemo notr tk k v mysql konzolo

Edin nvm če maš lohka 2x sn (verjetn ne). Duplicirani atributi niso podprti in bo javilo napako.

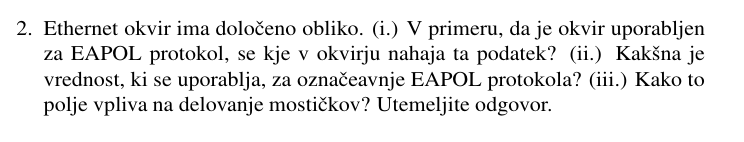


i. Uporaba večjega števila antem (MIMO).

ii. "MIMO" pomeni "Multiple-Input, Multiple-Output", in se nanaša na način, kako usmerjevalnik razčlenjuje pasovno širino in potisne na posamezne naprave. Večina sodobnih usmerjevalnikov uporablja "SU-MIMO" ali "Single User, Multiple-Input, Multiple-Output". S temi usmerjevalniki lahko le ena naprava prejme podatke v določenem času.

Na drugi strani pa usmerjevalniki "MU-MIMO" ("večkratni uporabnik, večkratni vhod, večkratni izhod") lahko razširijo to pasovno širino v ločene posamezne tokove, ki jih vsakdo enakomerno poveže s povezavo, ne glede na aplikacijo. MU-MIMO usmerjevalniki so na voljo v treh okusih: 2 × 2, 3 × 3 in 4 × 4, ki se nanašajo na število tokov, ki jih lahko ustvarijo za vsako napravo v vašem gospodinjstvu. Na ta način lahko vrtalni stroj MU-MIMO istočasno pošlje Pezu v štiri smeri hkrati. Če ne preveč tehnično, je to, kot da vsaka naprava dobi lasten "zasebni" usmerjevalnik, do štirih skupaj v 4 × 4 MU-MIMO nakladanja.

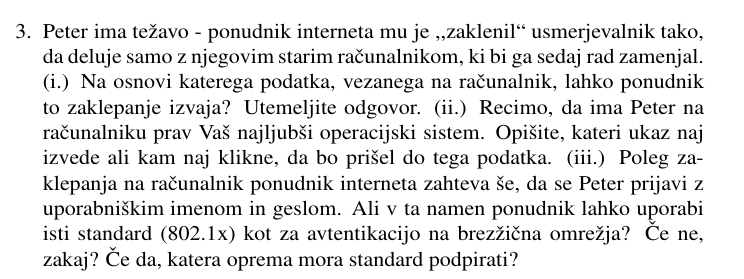
<https://sl.play-and-more.com/4724-what-is-mu-mimo-and-do-i-need-it-on-my-router>



i. in ii. EAPOL je definiran tako, da se njegova vsebina prenaša neposredno v

Ethernet okvirjih z vsebinsko značko 0x888E (type).

iii. ?



i. Na podlagi MAC naslova. Samo to se ne spremeni.

ii. V terminal vpiše: ip a/ ipconfig -> odvisno od sistema

iii. ?