

KOLOKVARE

Lelelelegenda:

- SAD- [Security Association Database](#)
- SA - Security Association
- IPsec ponuja dva protokola za varovanje:
 - AH - [Authentication Header](#)
 - Zagotavlja avtentikacijo izvora in integriteto podatkov
 - Zagotavlja da glava in podatki ostanejo nespremenjeni
 - ESP - Encapsulation Security Payload
 - Poleg tega kar zagotavlja AH, ESP zagotavlja še zaupnost podatkov. Torej enkripcijo (simetrično, asimetrično)
- CA - Certificate Authority
- Syslog - Beleženje
 - sistem, ki bo beležil vsebino dogodkov ter kje in kdaj so se zgodili
 - Standard uporabljen za shranjevanje stanja nekega sporočila od pošiljatelja do prejemnika. Vsako sporočilo dobi posebno številko
- Izziv - je pri avtentikaciji, ker je avtentificira odjemalec od NAS-a
- SPI - Security Parameter Index
- LCC - logical link layer
- OTP Sistem - je avtentikacijski sistem v katerem se uporablja geslo, ki je veljavno le enkrat.
 - Sistem omogoča avtentikacijo, ki je varna proti pasivnim napadom, kot je napad s ponavljanjem (Replay attack - zajetje gesla iz omrežja za kasnejši dostop do sistema). Sistem ne preprečuje aktivnih napadov in socialnega inženiringa.
- RADIUS deluje na aplikacijski plasti. In spodaj seveda še obstajajo druge plasti.
 - Transportna npr., ki je pod njo je zadolžena za prenos. Ker hočemo z RADIUSOM zagotoviti avtentikacijo, avtorizacijo in beleženje, tukaj nočemo da pride do napak in zato uporabljamo TCP.
 - TCP pa zagotavlja vrstni red in varnost (šifriranje paketov).
 - **UDP** sicer je hitrejši vendar moramo povedati, kje ta hitrost nastopa. UDP potrebuje manj virov, drugače podatki na povezavi potujejo z enako hitrostjo. Razlika nastane ko 4. (transportna) Plast preda podatke 5. (aplikacijski). Transportni pomnilnik je manjši, ker ne potrebuje čakati na pakete

- NAS network access service deluje zato da spravi skupaj AAA. To ji pa omogoča RADIUS
- Napad s ponavljanjem
 - Oblika napada, v katerem napadalec prestreže šifriran promet in ga ponovno uporabi za dostop do oddaljenega sistema in ni treba, da pozna šifrirano vsebino.
- Avtentikacija
 - Ana (odjemalec) se avtenticira Borutu (strežnik)
- Vzajemna avtentikacije
 - Ana se avtenticira Borutu in Borut Ani
- EAP - Okvir za protokole (ni pravi protokol) - lahko vsebuje druge protokole kot npr. CHAP
- TLS - glavna naloga TLS protokola je, da zagotavlja varno povezavo in s tem prenos podatkov med dvema aplikacijama
- PAP - omogoča neposreden prenos gesla v čistopisu (ta protokol je zadnja možnost, če vse ostalo odpove in če smo še vedno pripravljeni to početi)
- LDAP - Lightweight Directory Access Protocol

[RFC 4514](#)

LDAP: Distinguished Names

String	X.500 AttributeType
-----	-----
CN	commonName (2.5.4.3)
L	localityName (2.5.4.7)
ST	stateOrProvinceName (2.5.4.8)
O	organizationName (2.5.4.10)
OU	organizationalUnitName (2.5.4.11)
C	countryName (2.5.4.6)
STREET	streetAddress (2.5.4.9)
DC	domainComponent (0.9.2342.19200300.100.1.25)
UID	userId (0.9.2342.19200300.100.1.1)

- These attribute types are described in [\[RFC4519\]](#).

Legenda:	0
Kolokvij 2019/20 KL02	3
1. naloga: Varnostni elementi. VPRAŠANJA :	3
2. Naloga AAA	5
3. naloga: Podatki za delovanje omrežja:	7
4. naloga: IEEE 802. VPRAŠANJA :	9
2018/19 Drugi kolokvij	12
1. naloga: Varnostni elementi.	12
2. naloga: AAA in RADIUS.:	13
3. naloga: Podatki za delovanje omrežja.	15
4. naloga: IEEE 802.:	17
2017/18 Drugi kolokvij	19
1. naloga: Varnostni elementi.:	19
2. naloga: AAA in RADIUS:	20
3. naloga:	21
4. naloga: IEEE 802.	22
2016/17 Drugi kolokvij	23
1. naloga: Varnostni elementi:	23
2. naloga: AAA in RADIUS.	24
3. naloga: Podatki za delovanje omrežja:	25
4. naloga: IEEE 802.	26
2015/16 Drugi kolokvij	27
Varnosti elementi	27
AAA in RADIUS.	28
Podatki za delovanje omrežja.	29
IEEE 802.	29
2014/15 Drugi kolokvij	31
1. naloga: AAA in RADIUS.	31
2. naloga: Imeniške strukture in LDAP.	31
3. naloga: Varnostni elementi.	32
4. naloga: Razno.	33

Kolokvij 2019/20 KL02

1. naloga: Varnostni elementi. VPRAŠANJA :

A) Eden od načinov za vzpostavitev VPN je uporaba protokola IPsec.

(i.) Pri IPsec se morata stranki vzajemno avtenticirati, za kar potrebujeta skupno skrivnost. Kje se hrani le-ta?

Usmerjevalnik ima bazo SAD, kjer hrani podatke o SA.

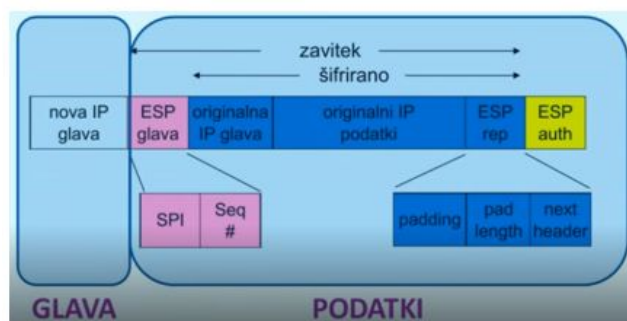
(ii.) ESP glava vsebuje dve polji. Kateri? čemu služi in kako se uporablja vsako od njih?

SPI- indeks SA, ki se ga uporabi za določanje nastavitev (vrednost uporabljena za identifikacijo SA)

Seq# - zaščita proti ponovitvi komunikacije

(iii.) IPsec datgram vsebuje tudi polnilo (padding). Ali lahko polnilo vedno uporabimo za prenos kakšnih dodatnih podatkov med članoma entitetnega para? Utemeljite odgovor.

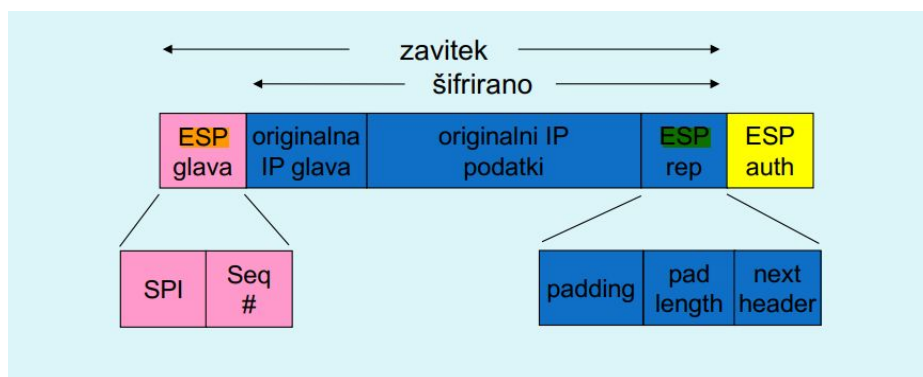
V ESP repu tudi shranimo št. Naslednje glave.



B) (i) Kako ESP preprečuje napade s ponavljanjem?

ESP preprečuje napade s ponavljanjem z zaporednimi številkami - seq (replay)

(ii) Utemeljite odgovor?



ESP preprečuje napade s ponavljanjem z zaporednimi številkami - seq (replay). Številke si shrani v tabelo (Anti-replay Window), tako da ko napadalec ponovno pošlje ta paket (replay) bo prejemnik pogledal v tabelo in bo ta številka v tabeli že prisotna. Tako bo ta paket zavgel.

[Vir za zgornje.](#)

C) Peter Zmeda želi postaviti navidezno zasebno omrežje s pomočjo OpenVPN. Namesto skupnega ključa želi uporabiti asimetrično kriptografijo in je zato postavil svojo certifikatno agencijo (CA). Odgovore na naslednja vprašanja tudi utemeljite.

(i.) Katere certifikate bo moral spraviti na OpenVPN strežnik? Za vsakega napišite, čemu je namenjen.

[Vir za spodnje.](#)

Najprej moramo postaviti PKI (public key infrastructure), ki je sestavljen iz:

- Ločenega certifikata (javni ključ) in zasebnega ključa za
 - Strežnik
 - Vsako stranko (client) in:
- Od glavne Certifikatne Avtoritete (Certificate Authority - CA - master key) certifikat in ključ, ki je uporabljen za podpisovanje strežnika in klientovega certifikata. Ta ni potreben, da je na strežniku ali na omrežju.

Strežnik potrebuje samo svoj certifikat/ključ - ne rabi poznati še certifikate strank.

Da dosežemo skupno zaupnost moramo narediti spodnje:

- Stranka (client) mora avtenticirati strežnikov certifikat
- In strežnik mora avtenticirati strankin certifikat

Tako kot strežnik in stranka morata avtenticirati drugega tako, da preverita ali je prisoten certifikat podpisan s strani glavne certifikatne avtoritete (CA).

(ii.) Katere certifikate bo moral spraviti na vsakega OpenVPN klienta? Za vsakega napišite, čemu je namenjen.

Potrebovali bi:

- certifikat strežnika - da lahko zaupamo strežniku, zaradi vzajemne avtentikacije
- certifikat glavne avtoritete (CA) - zato da vemo ali je strežnikov certifikat pravi

2. Naloga AAA

A) Storitev syslog je zabeležila:

Jan 17 10:07:27 AndyBook timed[133]:

settimeofday({0x5e21794f,0x436ca}) == 0

(i.) Kateri program je zahteval zabeležko? Utemeljite odgovor.

Timed, saj zraven vidimo PID, AndyBook je ime uporabnika, settimeofday pa ukaz.

(ii.) Kaj menite, da zabeležka pomeni.

Razlaga:

<https://cdn.discordapp.com/attachments/531132088007786509/802124108086902794/video-1588168110.mp4>

B) (i.) Opišite kako deluje napad vmesnega napadalca (man in the middle).

MitM počaka na napravo da vstopi v AP (authorization protocol) in dobi sporočilo. MitM vzpostavi tuneliran AP z authentication client-om. Ko je tunel vzpostavljen MitM začne posredovati sporočila od agenta do uporabnika.

(ii.) Ali je RADIUS protokol ranljiv na napad vmesnega napadalca (man in the middle)? Utemeljite odgovor.

RADIUS protokol je ranljiv za vmesnega napadalca takrat, ko nima skupnega gesla (skupne skrivnosti) z NAS-om. Če pa imata skupno skrivnost vzpostavljeno pa protokol postane varen.

Pri beleženju je ranljiv da napadalec prestreže sporočilo in ga večkrat pošlje.

PRI AVTENTIKACIJI: ranljiv, da lahko vprašanje, ki ga odjemalec pošlje NAS strežniku.

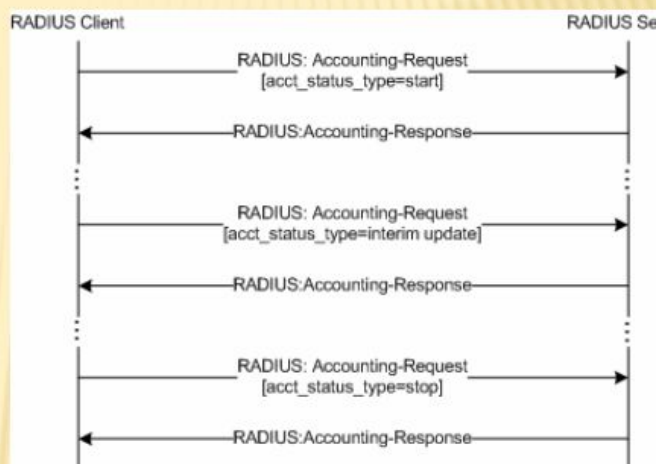
(iii.) Zakaj protokola CHAP ne bi mogli uporabiti ob uporabi RADIUS storitve, če bi bil protokol ranljiv na napad vmesnega napadalca? Utemeljite odgovor.

NAMIG: Razmislite kje in kako (arhitektura) se uporablja CHAP protokol pri RADIUS storitvi in kdo v tem primeru pozna skupno skrivnost ter za koga ne želimo, da jo pozna

Protokola CHAP ne bi morali uporabiti, ker bi problem postal na povezavni plati. Saj Radius sam po sebi ne omogoča zakrivanja, paketi niso šifrirani (pogovarjamo se v povezavi med NAS in RADIUS).

KOMUNIKACIJA NAS – RADIUS (..A)

- ✱ RADIUS protokol
 - + NAS pošlje: *Accounting Request*
 - + RADIUS odgovori: *Accounting Response*
 - + če ni odgovora v določenem času, se zahteva ponovno pošlje
- ✱ RADIUS lahko pošlje zahtevo naprej – *proxy*



Avtentikacije poteko od uporabnika proti radiusi (ker se NAS ne zna avtenticirati, radius pa)

RADIUS, imamo zato da NASu ni potrebno delati avtentikacije, ampak da to naredi RADIUS namesto njega

C) Kot rečeno, RADIUS storitev nudi Spela, ki v ta namen uporablja strežnik ~ *freeradius*.

(i.) Ali lahko Spela poskrbi, da bo RADIUS deloval tudi, če ji nekdo ugasne računalnik? Odgovor utemeljite.

(ii.) Spela želi uporabnike hraniti na način, kjer, če ji nekdo ukrade računalnik, ne bo mogoče razbrati gesel. Na predzadnjih vajah pri KPOV je slišala, da je to mogoče doseči z nekakšnimi moduli. Za kakšne module gre in kako jih uporabimo v *freeradius*?

Gre za freeradius module, ki se lahko uporabljajo za authentication, datastores, I/O, languages, policy, protocols

3. naloga: Podatki za delovanje omrežja:

A) Imeniška storitev je osnovana na standardu X.500.

(i.) Katere operacije definira standard?

Bind, read, list, search, compare, modify, add, delete, modifyRDN

(ii.) Kaj posamezna operacija naredi?

Tisto, zaradi česar je bila ustvarjena.

bind – želja po avtentikaciji ter ostalih možnih parametrih komunikacije (inačica, ...).

Seja je lahko tudi neavtentificirana.

unbind – zaključek komunikacije (seje).

Search – iskanje posameznih predmetov v bazi. Rezultat odvisen lahko odvisen od tega, ali je odjemalec avtentificiran ali ne.

compare – možnost primerjave vrednosti predmeta. Ni potrebno razkriti prave vrednosti predmeta, samo preverjamo enakost. Primerno za gesla in podobno.

Add - dodamo predmet v bazo

Delete - pobrišemo predmet iz baze

Modify - spremenimo vrednosti prilastkov predmeta

Modify DN - spremenimo ime predmeta(rename)

Start TLS - preklon na SSL način komunikacije

extended - generična možnost poljubnega dodatnega ukaza

(iii.) Izberite tri operacije in opišite scenarij, ko jih bi neka storitev uporabila.

Paket za upravljanje seje:

- Bind -> želja po avtentikaciji ter ostalih možnih parametrih komunikacije.
- Unbind -> zaključek komunikacije - seje

Paket za upravljanje poizvedbe:

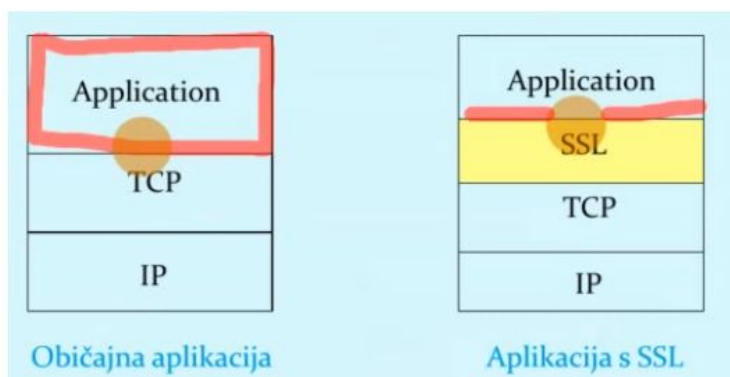
- Read
- List
- Search -> iskanje posameznih predmetov v bazi. Rezultat je odvisen od tega, ali je odjemalec avtentificiran ali ne
- Compare -> možnosti primerjave vrednosti predmeta. Primerno za gesla in podobno

B) (i) Katere načine varne komunikacije ponuja protokol LDAP?

Start TLS in LDAPS

(ii) Opišite njihovo delovanje.

- Start TLS preklopi na TSL/SSL način komunikacije ter doda SSL plast. SSL deluje samo na TCP povezavi.



- LDAPS namestitev strežnika na drugih vratih za izvajanje celotne komunikacije prek SSL protokola

Primer delovana:

<https://cdn.discordapp.com/attachments/772193271140319232/799766252033671228/video-1610748513.mp4>

C) Peter uporablja LDAP. V bazo je vnesel tudi podatke o sebi:

```
dn: cn=si,ou=users,dc=butale,dc=si
objectClass: inetOrgPerson
objectClass: person
cn: si
sn: Zmeda
gn: Peter
```

(i) Razložite, kaj pomenijo *dn*, *cn*, *ou* in *dc* v prvi vrstici.

- Dn: Določi različno ime za vnos
- Cn: common_name: Določa splošno ime osebe, ki je polno ime, ki ga oseba pogosto uporablja
- Ou: organization_unit_name - Določa atribut, ki vsebuje ime organizacijske enote. (profesorji, študenti)
- Dc: organization (fakulteta)

(ii) Ker se je poročil s prelepo Rozamundo, bi sedaj rad imel dva priimka - Zmeda in Turjaški. Kako naj popravi svoj vnos v bazi?

Uporabi ukaz modify nad sn.

4. naloga: IEEE 802. VPRAŠANJA :

1. (i) Katera tehnika je ena izmed ključnih pri povečanju hitrosti brezžičnega prenosa od 802.11g do 802.11n?

Povečanje moči signala z uporabo večjega števila anten.

(ii) Zakaj oziroma kako omogoča povečanje hitrosti?

Večjo hitrost omogoča zaradi možnosti oddajanja s 5GHz

2. Ethernet okvir ima določeno obliko.

(i.) V primeru, da je okvir uporabljen za EAPOL protokol, se kje v okvirju nahaja ta podatek?

Nahaja se v "type".

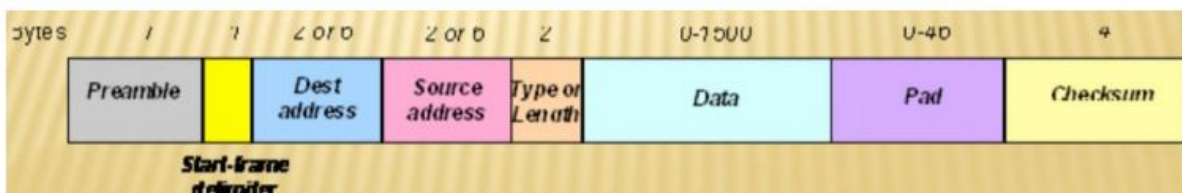
(ii.) Kakšna je vrednost, ki se uporablja, za označevanje EAPOL protokola?

Vrednost, ki se uporablja za označevanje EAPOL protokola je 0x888E.

(iii.) Kako to polje vpliva na delovanje mostičkov? Utemeljite odgovor.


3. Peter ima težavo - ponudnik interneta mu je „zaklenil“ usmerjevalnik tako, da deluje samo z njegovim starim računalnikom, ki bi ga sedaj rad zamenjal.

- ✦ standard IEEE 802.1x definira EAP na povezavni plasti – EAP over LAN -> EAPOL
 - ✦ kasneje je bil EAPOL uporabljen še v drugih pod-družinah IEEE 802.1x:
 - ✦ 802.1ae: varnost na MAC plasti
 - ✦ 802.1ar: varno identificiranje enot
- ✦ EAPOL je definiran tako, da se njegova vsebina prenaša neposredno v Ethernet okvirjih z vsebinsko značko 0x888E (type):
 - ✦ Preamble (7-bytes) Start Frame Delimiter (1-byte)
 - ✦ Dest. MAC Address (6-bytes) Source MAC Address (6-bytes)
 - ✦ **Length / Type (2-bytes)**
 - ✦ MAC Client Data (0-n bytes)
 - ✦ Pad(0-p bytes) Frame Check Sequence (4-bytes)



(i.) Na osnovi katerega podatka, vezanega na računalnik, lahko ponudnik to zaklepanje izvaja? Utemeljite odgovor.

Če je Petrov računalnik avtoriziran. Na osnovi podatka o pravicah Petrovega računalnika.



(ii.) Recimo, da ima Peter na računalniku prav Vaš najljubši operacijski sistem. Opišite, kateri ukaz naj izvede ali kam naj klikne, da bo prišel do tega podatka. syslog?

(iii.) Poleg zaklepanja na računalnik ponudnik interneta zahteva še, da se Peter prijavi z uporabniškim imenom in geslom. Ali v ta namen ponudnik lahko uporabi isti standard (802.1x) kot za avtentikacijo na brezžična omrežja? Če ne, zakaj? Če da, katera oprema mora standard podpirati?

YEAAAAHHHH

2018/19 Drugi kolokvij

1. naloga: Varnostni elementi.

A) Za uspešno vzpostavitev zasebnega navideznega omrežja so ključni podatki, ki jih vsebuje SA zapis

(i.) Naštejte pet elementov, ki jih SA zapis hrani ter za vsakega od njih kako (oziroma za kaj) se uporablja.

- 32 bitni ID SA, imenovan SPI (Security Parameter Index)
- Izvorni in ponorni IP SA
- Vrsta enkripcije (npr. 3DES) in ključ
- Vrsta preverjanja integritete (npr. HMAC-MD5, HMAC-SHA1, ...)
- Ključ za avtentikacijo (potrebujemo ga zato, da lahko pošiljatelj dokaže svojo istovetnost prejemniku)

(ii.) Zakaj en SA zapis vsebuje samo podatke za vzpostavitev enosmerne povezave?

En SA zapis vsebuje samo podatke za vzpostavitev enosmerne povezave zato, ker povezavo v drugo smer vzpostavi druga naprava.

Za vzpostavitev SA uporabljamo IP protokol oz. njegovo nadgrajeno verzijo IPsec. Ker je IP promet enosmeren, moramo za povratno komunikacijo vzpostaviti novo povezavo. Za vsako povezavo potrebujemo $2 + 2n$ povezav.

B) Kateri od naslednjih opisov najbolje opisuje pojem tunneling:

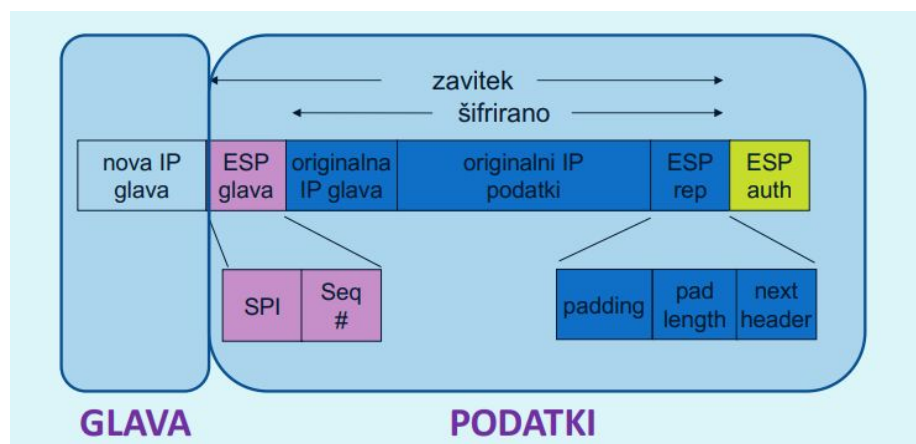
(a) sistem za zaznavo napak v paketu pri prenosu preko omrežja;

(b) način šifriranja paketa, tako da se šifrira podatke in glavo;

(c) sistem za detekcijo vdorov v omrežje; ali

(d) način šifriranja paketa, tako da se šifrira samo podatke. Utemeljite odgovor, oziroma opišite postopek.

Pojem tunneling najbolj opisuje b).



C) Peter Zmeda želi postaviti navidezno zasebno omrežje s pomočjo OpenVPN. Namesto skupnega ključa želi uporabiti asimetrično kriptografijo in je zato postavil svojo certifikatno agencijo (CA). odgovore na naslednja vprašanja tudi utemeljite.

(i.) Ali mora biti CA postavljena na računalniku znotraj navideznega omrežja?

Ne, saj imamo lahko katerokoli certifikatno agencijo. Potrebujemo CA, samo da nam ključke enkrat potrdi

(ii.) Na računalniku s CA se je pokvaril disk, zaradi česar so izgubljeni vsi podatki. Se lahko uporabniki še zmeraj povežejo v navidezno omrežje?

Da, saj imajo ključke že shranjene na svojih računalnikih.

(iii.) Kaj morajo narediti uporabniki, preden bodo lahko začeli uporabljati novo CA?

Ponovno dobiti potrdilo od strežnika na katerem je CA.

2. naloga: AAA in RADIUS.:

A) Storitve syslog je zabeležila:

```
Jan 1 21:38:22 svarun dhcpd: uid lease 192.168.127.137
for client 10:9a:dd:a6:dd:38 is duplicate on 192.168.127.0/24
```

Kateri od naslednjih programov je zahteval zabeležko:

a.) *lease*;

b.) *svarun*;

c.) *uid*; ali

č.) *dhcpcd*.

Utemeljite odgovor.

Zabeležko je zahteval program *dhcpcd* (ime programa, ki zahteva zabeležko je napisano pred dvopičjem).

B) Peter želi ponuditi novo storitev in sicer tiskanje nalepk. Razumljivo, tiskanje ni dovoljeno kar vsakomur in zato želi uporabiti RADIUS storitev, ki jo ponuja Špela.

(i.) Narišite sliko arhitekture Špeline in Petrove storitve ter kje je uporabnik Petrove storitve. Označite kakšen protokol je uporabljen med posameznimi elementi arhitekture.

Špela je avtentikacijski strežnik

Peter je strežnik

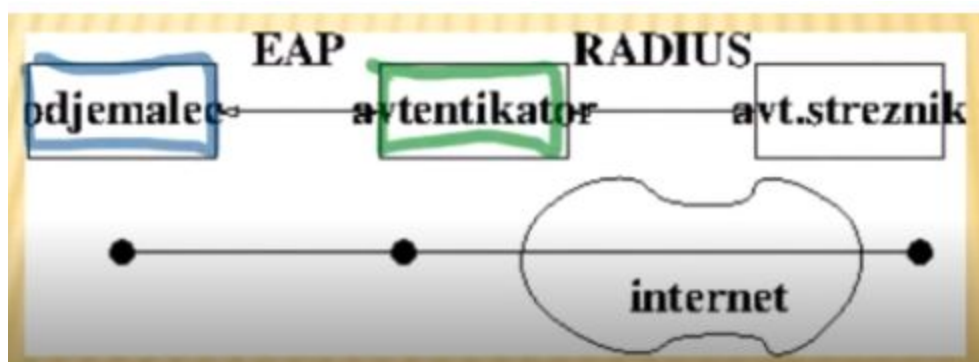
Luka je pa uporabnik.

Med Luko in Petrom teče EAP ali oa CHAP(starejši?) protokol.

Med Špelo in Petrom pa RADIUS protokol

Tri udeležene stranke:

- **uporabnik** neke storitve
- **ponudnik storitve** - ponudnik storitve (NAS → je hkrati **RADIUS** odjemalec)
- **RADIUS strežnik** → je lahko vmesni člen pri dostopu do drugega **RADIUS** strežnika



(ii.) Luka Kratkohlačnica je uporabnik, ki želi uporabiti Petrovo storitev. Čim podrobneje opišite, kako poteka avtentikacija in avtorizacija, pri čemer se naj uporablja CHAP protokol.

NAMIG: Kakšni podaki (čistopis ali šifrirani in kako šifrirani) se prenašajo med elementi vaše arhitekture.

1. Luka pošlje Petru vprašanje če se lahko pridruži (Access Request)
2. Peter, ga vpraša kdo si ti. Ter mu Luka odgovori z: jaz sem Luka.
3. Peter pošlje Špeli vprašanje: Ali poznaš Luko?
4. Špela lahko odgovori z Da (Acces-Accept), Ne (Acces-Reject) ali pa potrdi mi, če je Luka res Luka (**Acces-Challenge**):
5. Peter pošlje Luki nato izziv, da se potrdi. Luka pošlje Petru upravljen izziv in nato Peter Špeli, ki se bo sedaj lahko odločila, ali je pravi ali ne.

(iii.) Opišite, kako lahko Cefizelj izvede vmesni (MITM, man in the middle) napad na CHAP protokol. Za lažje odgovarjanje, vam ni potrebno upoštevati RADIUS protokola; se pravi Ana bi rad avtenticirala Braneta in Cefizelj izvaja MITM napad. Cefizelj stoji med Branetom in Ano. Ter ko Ana pošlje vprašanje *kdo si ti* bi ji Cefizelj odgovoril *Jaz sem Ana*. Tako in nato naprej Cefizelj vstavi svoje geslo na odgovor na izziv in bo dobil potrjeno, da je Cefizelj res Ana.

C) Kot rečeno, RADIUS storitev nudi Špela, ki v ta namen uporablja strežnik *freeradius*.

(i.) Na koga oziroma kaj se nanašajo vnosi v datoteki `/etc/freeradius/3.0/clients.conf`?

Nanašajo se na uporabnike.

(ii.) Špela želi uporabnike hraniti v podatkovni bazi mysql. Ali naj bo strežnik mysql na istem računalniku kot freeradius? Zapišite po eno prednost za uporabo ločenega in za uporabo istega stroja za obe storitvi.

Če bo strežnik mysql na istem računalniku kot freeradius bo povezava hitrejša ampak manj varna. Zaradi varnosti bi bilo bolje postaviti mysql strežnik na drugem računalniku.

3. naloga: Podatki za delovanje omrežja.

A) Peter za hranjenje podatkov uporablja storitev LDAP, ki jo nudi Simona. Ker Peter ni zahteval nobenih posebnosti, je Simona doslej ponujala LDAP.V2, sedaj pa mora nadgraditi storitev na LDAP.V3.

(i.) Kaj je zahteval Peter, da Simona ni mogla tega zagotoviti s starejšo inačico storitve?

Organization name.

Poleg tega LDAPv2 ne zagotavlja ustreznih varnostnih funkcij za uporaba na internetu. LDAPv2 ne zagotavlja nobenega mehanizma za podatke celovitost ali zaupnost. LDAPv2 ne podpira sodobnega avtentikacijskega mehanizma, kot so tisti, ki temeljijo na DIGEST-MD5, Kerberos V in X.509 javnih ključev.

(ii.) Poleg tega je Peter našel na sistemu ukaz *ldapcompare* z naslednjim opisom:
ldapcompare opens a connection to an LDAP server, binds, and performs a compare using specified parameters. The DN should be a distinguished name in the directory. Attr should be a known attribute. If followed by one colon, the assertion value should be provided as a string. If followed by two colons, the base64 encoding of the value is provided. The result code of the compare is provided as the exit code and, unless ran with -z, the program prints TRUE, FALSE, or UNDEFINED on standard output.

Zakaj vrne opisane rezultate? Utemeljite odговор in primer uporabe.

Ker nočemo da proizvedovalec dobi geslo, niti v šifrirani obliki. Zato imamo parameter *compare*, ki vrne ali je geslo pravilno ali napačno.

Undefined je če tega nemore storiti?

B) Peter Zmeda je doma v Butalah na Glavni ulici #5 in dela na Občini Butale.

Njegov e-naslov je peter.zmeda@gov.bu. Kakšno je razločevalno ime, ki ga najbolje določa glede na opis v RFC 4514:

(a) *CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob.*

Butale,DC=gov,DC=bu

(b) *CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob.*

Butale,DC=gov+DC=bu

(c) *CN=Peter Zmeda,C=Butale,STREET=Glavna ulica #5,O=Ob.*

Butale,DC=gov+DC=bu

(d) *CN=Peter Zmeda C=Butale STREET=Glavna ulica #5 O=Ob. Butale DC=gov DC=bu*

Utemeljite odgovor.

a) Ga najbolje določa

[Vir.](#)

C) Kaj in kam moramo v sistemih Unix zapisati, da se bo za razreševanje internetnih imen uporabljal DNS strežnik z naslovom 193.2.1.66? Utemeljite odgovor.

4. naloga: IEEE 802.:

1. Peter Zmeda je slišal, da postaja internet stvari (IoT - Internet of Things) stvarnost. Zato se je odločil, da bo definiral svojo obliko okvirjev v protokolu IEEE802. Izberite eno od kombinacij polj v okvirju, ki jih mora definirati, da bodo njegovi okviri še vedno nemoteno potovali in da jih nihče drug pomotoma ne bo obdeloval:

- a.) ciljni naslov in podatke;
- b.) izvorni naslov in podatke;
- c.) samo podatke; ali
- č.) polje *ethertype*?

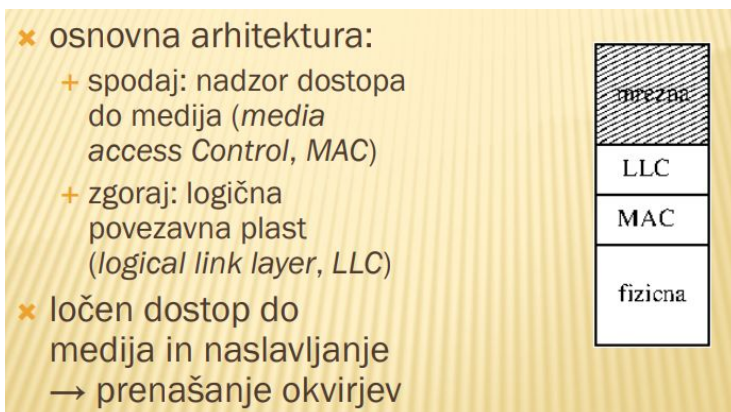
Utemeljite odgovor.

č) polje *ethertype*. V polju *ethertype* je definirano kateri od protokolov je enkapsuliran.

2. Povezavna plast, ki je implementirana z IEEE.802 protokolom je običajno razdeljena na dve podplasti.

(i.) Kateri sta ti podplasti?

- LLC(zgornja)
- MAC(spodnja)



(ii.) V kateri podplasti delujejo mostički (bridge)? Utemeljite odgovor.

Mostički delujejo v LLC, ker MAC pove na kateri način (koliko voltov, kapaciteta, kakšne led diode)

LLC pa kam, ker mostički znajo pošiljati pakete, takrat ko je to zahtevano.

(iii.) Usmerjanje (routing) in premoščanje (bridging) sta zelo podobni storitvi.

Katera od njiju zahteva več virov za enako število ciljnih vozlišč in zakaj?

Več virov zahteva premoščanje, saj moramo priti do točno določenega MAC naslova. (Pri IP lahko moramo priti samo do pravega podomrežja).

3. Peter ima slab spomin in si nikakor ne more zapomniti MAC naslova omrežnega vmesnika v svojem računalniku. Rad bi namreč poskrbel, da bi njegov računalnik ob priklopu v domače omrežje vedno dobil isti naslov.

(i.) Kako lahko ugotovi kakšen je MAC naslov njegovega računalnika?

To lahko ugotovi z ukazom `ifconfig`.

(ii.) Kako lahko poskrbi, da bo njegov računalnik dobil isti naslov? Seveda, ročno nastavljanje IP naslova ne pride v poštev.

Za to lahko poskrbi na DHCP strežniku. Tam spremeni nastavitve tako, da za njegov DHCP strežnik vedno dodeli isti IP naslov.

(iii.) Zakaj uporaba DHCP storitve ne omogoča zaščite omrežja pred priklopom nepovabljenih gostov?

NAMIG: Opišite napad.

Ker ne pregleduje kdo se prijavlja, ampak ko se naprava prijavi, bo DHCP dodelil IP naslov. Lahko bi napadalec napadel strežnik, tako da bi se prijavil tolikokrat da bi DHCP pool bil čisto poln.

2017/18 Drugi kolokvij

1. naloga: Varnostni elementi.:

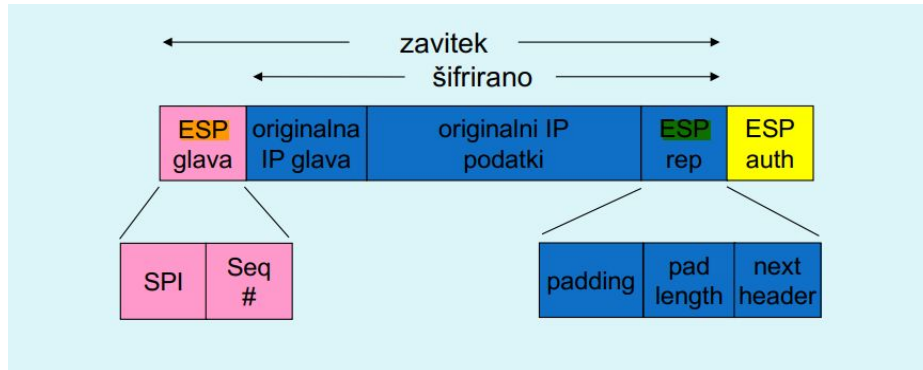
A) Peter sumi, da se nekdo poigrava z njegovimi paketi, ki potujejo med dvema njegovima računalnikoma. Kako naj ugotovi, če je to res – ne kako naj to prepreči, če je res. Podrobno opišite postopek preverjanja.

Ugotovi tako, da primerja paket poslan iz računalnika A in dobljen paket iz računalnika B.

Vzpostavimo SA(Security Association) in usmerjevalnik postavimo kot SAD, na katerem bo hranil podatke o njunem SA, ki prav tako hrani izvorni in ponorni IP in s tem bomo preprečili.

Lahko bi postavili tudi ESP

B) Kako ESP preprečuje napade s ponavljanjem? Utemeljite (opišite) kako vaš odgovor v resnici preprečuje napade s ponavljanjem. Lažje bo, če narišete strukturo paketa.



ESP preprečuje napade s ponavljanjem z zaporednimi številkami - seq (replay). Številke si shrani v tabelo (Anti-replay Window), tako da ko napadalec ponovno pošlje ta paket (replay) bo prejemnik pogledal v tabelo in bo ta številka v tabeli že prisotna. Tako bo ta paket zavgel.

[Vir za zgornje.](#)

C) Peter Zmeda se je odločil, da bo postavil navidezno omrežje med s pomočjo OpenVPN. Spisal je takole nastavitveno datoteko, s katero se povezava vzpostavi:

remote 212.235.189.164 dev tap secret static.key

i.) Kakšen IP naslov ima na strežnik na vpn? Utemeljite odgovor.

212.235.189.164, ker ko nastavljamo clientov key, mu moramo povedati javni IP naslov od tega strežnika

ii.) Kje / kako lahko to preberemo?

ifconfig

iii.) Kako ga lahko spremeni?

V datoteki networks na strežniku

2. naloga: AAA in RADIUS:**A) OTP (One-time password) iz RFC 2289 je podoben (odgovor utemeljite):**

- (a) protokoloma SRTP in CHAP,
- (b) protokoloma TSL in EAP,
- (c) protokoloma SRTP in EAP ali
- (d) protokoloma IPsec in CHAP.

B) Protokol Radius nudi nekaj varnostnih elementov.**i.) Ali nudi zakrivanje ali celovitost sporočila in kako?**

Radius sam po sebi ne nudi zakrivanja. Celovitost se zagotavlja z MD5(Besedilo * Skrivnost * token)

ii.) Opišite podrobno varovanje česa omogoča ter zakaj ostalega ne.

Nudi:

- Med uporabnikom in NAS-om (preden se avtentificira) lahko uporabljamo PPP
 - PPP sam po sebi nima zaščite, vendar ga lahko tuleniramo v drug protokol. Če pri tem zagotavljamo TCP povezavo, zagotovimo tudi varno uporabo tega protokola (SSL)
- Med NAS in RADIUS
 - NAS ne ponuja avtentikacije, ampak namesto njega to počne RADIUS.
 - Med NAS-om in Radiusom je lahko prodlem ponavljanje izziva, ki ga lahko pošlje man in the middle, a to preprečimo če imamo vzpostavljeno skupno skrivnost (geslo)

NAMIG: Lažje bo, če opišete (narišete) paket in smer komunikacije.

C) Peter poizkuša postaviti svoj strežnik Radius. V ta namen uporablja ukaz *radtest*. V dokumentaciji piše, da se ukaz uporablja takole:

radtest <username> <password> <hostname> <NAS port> <secret>

i.) Kakšno vrednost naj uporabi za NAS port in zakaj? Kaj ta parameter sploh pomeni?

[Vir.](#)

Je številka med 0 in n^{32} in ni pomembno kaj tukaj damo. 10 bo v redu

ii.) Če bo vnesel napačno geslo (password), kakšen odgovor lahko pričakuje? Kaj pa, če bo vnesel napačno skrivnost (secret)?

3. naloga:

Peter Zmeda je doma v Butalah na Glavni #5 in dela na Občini Butale. Njegov e-naslov je peter@gov.bu. Razmislimo o naslednjih razločevalnih imenih:

1. CN=Peter,C=Butale,STREET=Glavna #5,O=Ob. Butale,DC=gov+DC=bu
2. CN=Peter,C=Butale,STREET=Glavna \#5,O=Ob. Butale,DC=gov+DC=bu
3. CN=Peter,C=Butale,STREET=Glavna \#5,O=Ob. Butale,DC=gov,DC=bu
4. CN=Peter C=Butale STREET=Glavna #5 O=Ob. Butale DC=gov DC=bu

A) Katero od naštetih razločevalnih imen, določeno glede na opis v RFC 4514, je pravilno in zakaj. Zakaj so ostala napačna?

!polž

B) Peter se je odločil, da bo s prijatelji vzpostavil navidezno zasebno omrežje. Za avtentikacijo so se odločili, da uporabijo certifikate, ustvarjene s pomočjo easy-rsa, ki so ga dobili poleg OpenVPN.

i.) Ali bi lahko certifikate za OpenVPN ustvarili kako drugače? Če da, kako; če ne, zakaj ne?

ii.) V datoteki ~ vars je vsak nastavil svoj KEY CN. Bi lahko vsi uporabili istega? Odgovor utemeljite.

iii.) Ko je Peter nastavil spremenljivke v datoteki vars, ukazi, kot so build-key, build-req in sign-req, niso delovali. Kaj je pozabil? Kako skripte, ki sestavljajo easy-rsa preberejo nastavitve?

C) V sistemu DNS korenski strežnik preusmerja poizvedbe, na katere ne zna odgovoriti, na DNS poizvedbe naslednjim strežnikom.

i.) Kako lahko napademo ta sistem in kako se lahko branimo pred takšnim napadom?

ii.) Kaj je lažje izvesti pri poizvedbah proti DNS strežnikom – varovanje celovitosti sporočil ali zakrivanje. Utemeljite odgovor.

4. naloga: IEEE 802.

1. EAPOL (EAP over LAN) omogoča avtentikacijo uporabnika za uporabo storitve priklop na mrežo. Ali obstaja v EAPOL tudi paket, ki sporoči strežniku, da uporabnik ne potrebuje več te storitve? Izberite najboljši odgovor in ga utemeljite:

(a) Ne, saj se odklop zgodi samodejno, če v predoločenem času ni nobenega prometa.

(b) Ne, saj avtentikacija je druga storitev kot priklop na mrežo.

(c) Ne, saj ni potrebno, ker je ponudnik obeh storitev ista naprava.

(d) Da, imenuje se Logoff.

2. Pri protokolu IEEE 802.1x nastopajo tri entitete.

i.) Katere in kakšna je vloga posamezne od njih?

ii.) Paroma se neposredno pogovarjata po dve entiteti. Kateri in kakšen protokol se uporablja pri tem? Na kateri plasti je ta protokol? Utemeljite odgovor.

3. Peter si je doma postavil brezžično omrežje tako, da je kupil običajno brezžično dostopno točko (wireless access point). Sedaj bi rad do omrežja omejil dostop, pri čemer bi vsakemu uporabniku dodelil svoje ime in geslo.

i.) Katero vrsto avtentikacije mora iskati v nastavitvah?

ii.) Ali kaj takega sploh lahko naredi z običajno brezžično točko, namenjeno domačim uporabnikom, ne pa večjim podjetjem? Utemeljite odgovor.

iii.) Poleg nastavitve na brezžični dostopni točki, kaj bo moral še postaviti na omrežje – kje bodo podatki o uporabnikih?

2016/17 Drugi kolokvij

1. naloga: Varnostni elementi:

A) Sol je v Butalah močno cenjena dobrina in zato je Peter Zmeda za občino Butale izdelal aplikacijo za naročilo semena soli. Aplikacijo je moč uporabljati tudi preko spleta in sicer jo je Peter postavil v demilitizirano območje (demilitarized zone). Dostop je možen preko vrat 2017 ob uporabi TCP prenosnega protokola. Zaradi varnostnih zahtev želi Peter Cefizlju preprečiti dostop kaj šele uporabo aplikacije. S kakšnim načinom filtriranja lahko to doseže? Utemeljite odgovor.

Firewall?

B) Pri IPsec poznamo dva načina komunikacije: tunelski in transportni.

(i.) Zapišite primer, kjer je prvi boljši od drugega, in primer, kjer je drugi primernejši od prvega. Oba primera utemeljite.

Transportni način je boljši, ker komunikacija teče neposredno med pošiljateljem in odjemalcem (deluje hitreje).

Tunelski način:

- Paket od pošiljatelja in svojega ruterja potuje odprt
- Od ruterja do ruterja prejemnika, je paket zaščiten
- Od prejemnikovega ruterja pa je znova odprt

Slabost tunelskega načina je, da karkoli se dogaja izven ruterjev je lahko ogroženo

NAMIG: Za utemeljitev razmislite kaj lahko naredimo z enim in ne moremo z drugim načinom komunikacije.

(ii.) Pri IPsec imajo paketi lahko ESP ali AH glavo. Ali je za AH glavo tudi potreben vpis v SAD? Utemeljite odgovor.

Da je potreben vpis, saj ena izmed stvari, ki jo AH (Authentication Header) zagotavlja je, da je glava nespremenjena. Ter glava vsebuje ponorni in izvorni IP, ki ga prav tako hranimo v SAD.

NAMIG: Najlažje bo, če opišete funkcionalnost, ki jo nudi AH glava ter dele IP paketa, ki ima AH glavo.

C) V Butalah so postavili navidezno lokalno IP omrežje, za kar so uporabili OpenVPN. Tip naprave so nastavili na *tap*. V Tepanjah imajo podobno omrežje, prav tako

zgrajeno okrog OpenVPN. Sedaj bi v imenu boljših medsosedskih odnosov vasi radi omrežji združili, za kar bodo prav tako uporabili OpenVPN.

(i.) Na kakšne težave lahko naletijo in kako jih rešiti (navedite vsaj eno)?

<https://cdn.discordapp.com/attachments/370216420199628802/801902695899987968/ummsasa.mp4>

(ii.) Kako naj nastavijo usmerjevalne tabele?

(iii.) Ali omrežje lahko deluje, ne da bi imeli v usmerjevalni tabeli vsaj en prehod? Utemeljite odgovor.

2. naloga: AAA in RADIUS.

A) Kako protokol CHAP preprečuje napade s ponavljanjem? Utemeljite odgovor.

Ker vsakič, ko se mora zgoditi avtentikacija dobi stranka izziv in, ker se izziv menja, je protokol CHAP težko napasti s ponavljanjem.

B) Eden od načinov avtentikacije posameznikov je avtentikacija z biometričnimi podatki (prstni odtis, retina, ...). Peter Zmeda bi rad v svoji novi aplikaciji uporabil takšno avtentikacijo, a se ne more odločiti kako. Pri tem seveda predpostavlja, da ima uporabnik na voljo enoto, ki prebere biometrični podatek, ter ga odda kot enoličen (glede na posameznika) niz 512 bitov. Razmišljal je o uporabi protokola CHAP. Opišite kako bi ga uporabili in implementirali celoten postopek avtentikacije.

NAMIG: Pri opisovanju rešitve posebej pazite na zaupanje posameznim elementom oziroma sestavnim delom rešitve in kako se izogniti možnosti napada. Morda bo potrebno kaj tudi narediti z napravo za branje biometričnih podatkov, da bo niz bitov, ki ga odda ter ga nato uporabimo, bolj zaupanja vreden.

C) Peter je postavil strežnik RADIUS in ustvaril nekaj uporabnikov. Nato je prišel naokrog Cefizelj, prebral /etc/freeradius/users in pokradel gesla vseh uporabnikov.

(i.) Kako bi Peter lahko preprečil tako krajo v prihodnosti?

Ustreli cefizla

set auth_goodpass = no

(ii.) Kako lahko poskrbi, da gesla ne bodo shranjena na strežniku RADIUS v tekstovni obliki? Opišite vsaj 2 načina.

Lahko jih shrani v SQL podatkovno bazo, ker freeRADIUS vključuje modul za upravljanje z SQL podatkovnimi bazami.

Druga možnost je storitev LDAP. LDAP storitev hrani opise, podatke o uporabnikih (uporabniško ime, geslo, ...).

3. naloga: Podatki za delovanje omrežja:

A) V imeniku so shranjeni predmeti.

(i.) S čem je opisan posamezen predmet? Navedite primer.

Razločevalno ime (Distinguished Name) je opisan z

- DC

(ii.) Kaj je to shema in kaj določa? Navedite primer.

Schema združuje različne predmete in prilastke

Prilastki opisujejo lastnost

(iii.) Kaj novega je prinesel LDAPv3 v primerjavi z LDAPv2? Naštejte vsaj tri (konkretne) dopolnitve in opišite njihovo funkcionalnost.

- Certificate authentication in storitve za varstvo podatkov,
- Internacionalizacija z uporabo Unicode (UTF-8),
- Polje SupportedControl, da je lahko LDAP protokol podaljšan.

B) Včasih želimo najti objekte na osnovi bolj zapletenih poizvedb. Lahko bi na primer iskali vse ljudi iz Butal, ki jim je ime Francot ali Kozmijan. Vprašanje je, ali poizvedbeni jezik, s katerim dobivamo podatke iz baze LDAP, kaj takega sploh podpira? Utemeljite odgovor.

Da, poizvedbeni jezik to podpira. Uporabimo ldapsearch in filtriramo podatke po želji.

C) Peter bi rad vsem Butalcem omogočil, da bi se prijavljali na vse računalnike v vasi. Podatke o uporabnikih bo spravil v podatkovno bazo LDAP.

(i.) Kaj bo moral na računalnikih nastaviti, da se bodo uporabniki lahko avtenticirali? Dovolj bo, če poveste, nastavitve katere knjižnice bo spreminjal.

(ii.) Kaj bo moral nastaviti, da bo sistem ob prijavi znal prevesti uporabniška imena v številke uporabnikov?

(iii.) Peter je prebral, da bo za testiranje lahko uporabil ukaz:

```
ldapsearch -H ldapi:/// \ -D cn=peter,ou=people,dc=butale,dc=si\ -W -b  
ou=people,dc=butale,dc=si
```

Kaj predstavlja niz za stikalom -D in kaj niz za stikalom -b? Kaj pa niz za stikalom -H?

4. naloga: IEEE 802.

1. Pri protokolu IEEE 802.1X smo omenjali uporabo protokola EAPOL.

(i.) Čemu je namenjen?

Namenjen je avtentificiranju pri avtentikatorju na LAN omrežju

(ii.) Prenosni protokol zanj je na Ethernet protokol na drugi plasti. Zakaj ni to IP protokol na tretji plasti? Utemeljite odgovor.

EAPOL vsebuje samo MAC naslov, ki deluje na drugi plasti.

2. Peter Zmeda je slišal, da postaja internet stvari (IoT – Internet of Things) stvarnost. Zato se je odločil, da bo definiral svojo obliko okvirjev v protokolu IEEE802. Kaj vse mora definirati, da bodo njegovi okviri še vedno nemoteno potovali in da jih nihče drug pomotoma ne bo obdeloval? Utemeljite odgovor.

- a.) ciljni naslov in podatke,
- b.) izvorni naslov in podatke,
- c.) payload,
- č.) ethertype.

3. Peter je malce len in na vseh svojih elektronskih napravah uporablja isto geslo. Sedaj bi doma rad zavaroval svoje brezžično omrežje, obenem pa svoji sestri noče povedati svojega gesla – raje bi imel ločena uporabniška imena in gesla. Kako naj nastavi svojo brezžično dostopno točko? Kaj bo moral še postaviti / nastaviti?

2015/16 Drugi kolokvij

1. Varnosti elementi

A) Na govornilni uri je nekdo postavil vprašanje, ali se pri IPsec v paketu vidi izvorna in ponorna vrata? Kaj menite, se vidijo? Utemeljite odgovor.

Ne, saj IPsec zagotavlja tudi zakrivanje, sepravi se tega ne vidi. Zato imamo ESP glavo in AH

B) Peter bi rad s svojim prijateljem Konradom igral prastaro igrico – Warcraft II. Igrica za igranje preko omrežja uporablja protokol IPX. Peter in Konrad živita na različnih koncih mesta in uporabljata takšne konfiguracije za OpenVPN:

Peter	Konrad
proto tcp	proto tcp
remote vpn.prijateljkonrad.net	dev tun
dev tun	secret skrivnost.txt
secret skrivnost.txt	

(i) Kdo bo za igrico postavil strežnik – Peter ali Konrad? Utemeljite odgovor.

Strežnik bo postavil Konrad.

```

30
31 server.conf:
32     proto tcp-server
33     dev tun
34     secret mybestsecret.key
35     ifconfig 10.40.0.1 10.40.0.2
36
37 client.conf:
38     remote 192.168.1.34
39     proto tcp-client
40     dev tun
41     secret mysecondsecret.key
42     ifconfig 10.40.0.2 10.40.0.1
43

```

(ii) Veselo sta odigrala nekaj partij openra (Open Red Alert) prek svojega navideznega omrežja. Warcraft II vseeno ne deluje. Kaj menite, da je razlog? Kako naj težavo odpravita?

C) Peter Zmeda se je odločil zasoliti shranjena in zgoščena gesla, da bi ne bila ranljiva na mavrični napad. Zal je vrednost soli izgubil. Je to pomembno? Utemeljite odgovor.

Ne, saj soli ne vnašamo z geslom, ampak se tako samo shranijo v bazi. Ko bo pa pozabil še geslo bo pa geslo ponovno zasolil z novo vrednostjo soli.

2. AAA in RADIUS.

A) Eden od protokolov za avtentikacijo se imenuje CHAP.

(i) Opišite, kako deluje.

1. Ana (strežnik) pošlje izziv
2. Borut (odjemalec) izziv združi z geslom in ga vrne šifriranega z enosmerno razpršilno funkcijo (žeton)
3. Ana preveri pravilnost odgovora

(ii) Posebna lastnost protokola CHAP je, da preprečuje napad s ponavljanjem. Kako?

Izziv, ki se pošilja odjemalcu je vedno drugačni.

B) Zgoraj smo zapisali, da je CHAP protokol za avtenkacijo.

(i) Ali omogoča vzajemno avtentikacijo?

Ne, saj "Navaden" CHAP protokol ne omogoča vzajemne avtentikacije.

Jo pa zagotavlja MS-CHAP.

(ii) Če da, kako; in če ne, kako bi ga nadgradili, da bi jo omogočal? NAMIG: Če menite, da CHAP ne omogoča vzajemne avtentikacije, lahko definirate svojo novo inačico CHAP protokola.

CHAP ne omogoča vzajemne avtentikacije, zato je Microsoft razvil svojo različico, ki se imenuje MS-Chap in omogoča vzajemno avtentikacijo.

Nadgraditi ga moramo tako, da se bo še strežnik avtetniciral odjemalcu. Tukaj pride potreba po novi certifikatni agenciji (CA), katera bi odjemalcem in strežniku zagotavljala, da je drugi res bil podpisan pri CA in je pravi.

C) Peter Zmeda je našel v sistemski zabeležki naslednjo vrstico:

```
Jan 18 06:30:45 svarun saslauthd[52023]:
do auth: auth failure: [user=pzmeda] [service=smtp]
[realm=] [mech=pam] [reason=PAM auth error]
```

(i) Kateri program je zahteval zabeležko?

saslauthd - SASL authentication server.

(ii) Kaj pravzaprav pravi zabeležka in ali bi Peter moral biti zaskrbljen? Utemeljite odgovor.

3. Podatki za delovanje omrežja.

A) Osnovni protokol za nudenje podatkov za delovanje, ki smo ga spoznali, je LDAP. Opišite tri bistveno različne načine kako lahko promet protokola LDAP zakrijemo. Za vsakega od njih opišite, kdaj bi ga izbrali namesto drugih dveh. Utemeljite odgovor.

NAMIG: Vaš odgovor mora za vsakega od načinov vsebovati situacijo (in utemeljitev), ko je ta način primernejši od drugih dveh.

B) Peter Zmeda za shranjevanje uporabnikov uporablja LDAP. Njegova domena je *butale.si*. Vsi njegovi uporabniki so del organizacije trg. Sedaj je po sili razmer prisiljen ustvariti uporabnika *cefizelj*, ki bo v organizacijski enoti *lopovi*. Kakšno bo razpoznavno ime (distinguished name) objekta v imeniku LDAP, ki opisuje Cefizlja? Utemeljite odgovor.

dc=trg, ou=lopovi, uid=cefizelj

C) Pri SSL/TLS rokovanju odjemalec pošlje strežniku seznam podprtih šifrirnih algoritmov. Kako lahko SSL/TLS prepreči izbris močnejših algoritmov s seznama podprtih? Utemeljite odgovor.

kpov » Forumi » Pogovori o predmetu / Course discussion »
Prijava na izpit



Re: Zadeva: Prijava na izpit
od Andrej Brodnik - torek, 19 januar 2021, 12:05

Počasi, počasi, prosim!
Najprej hvala tako Azri za vpršanje kot Aljažu za pojasnilo. To je vse, kar vidim zapisanega.

Lep dan in ne pozabite se prijaviti, če boste pisali.

Lep dan in LPA
[Pokaži starša](#) | [Odgovor](#)
[Oglej si objavo v kontekstu](#)

4. IEEE 802.

1. (i) Na kateri plasti govori odjemalec s ponudnikom priklopa na lokalno mrežo?

Na omrežni plasti?

(ii) Peter je slišal da protokol IEEE 802.1x uporablja RADIUS. Glede na odgovor na prvi del vprašanja, ali bo Petru uspelo spraviti RADIUS promet do odjemalca, ki bi se rad priključil na lokalno mrežo z uporabo protokola IEEE 802.1x? Utemeljite odgovor.

2. Peter je postavil strežnik Freeradius. Sedaj bi ga rad uporabil za avtentikacijo na več dostopnih točkah.

(i) Ali lahko na vseh uporabi isto skrivnost? Recimo, da imam Peter nastavitveno datoteko z naslednjo vsebino:

```
client dostopna
secret = secret
shortname = localhost
nastype = other
ipaddr = 192.168.1.1
require message authenticator = no
```

(ii) Pomagajte mu jo dopolnite tako, da bosta strežnik lahko uporabljali še dve dostopni točki na isti mreži kot že nastavljena. Privzamete lahko, da gre za sodobno dostopno točko, ki deluje v skladu z RFC5080.

Kateri izmed naslednjih izrazov je najbolj primeren za izračun naključne VLAN ID vrednosti (rand() vrne naključno celo število):

- $(\text{rand}() \bmod 4095) + 1$
- $\text{rand}() \bmod 4096$
- $\text{rand}() \bmod 4094$
- $(\text{rand}() \bmod 4094) + 1$

$(\text{rand}() \bmod 4095) + 1$, ker vedno vrne števila od 1 do 4094.

Utemeljite odgovor.

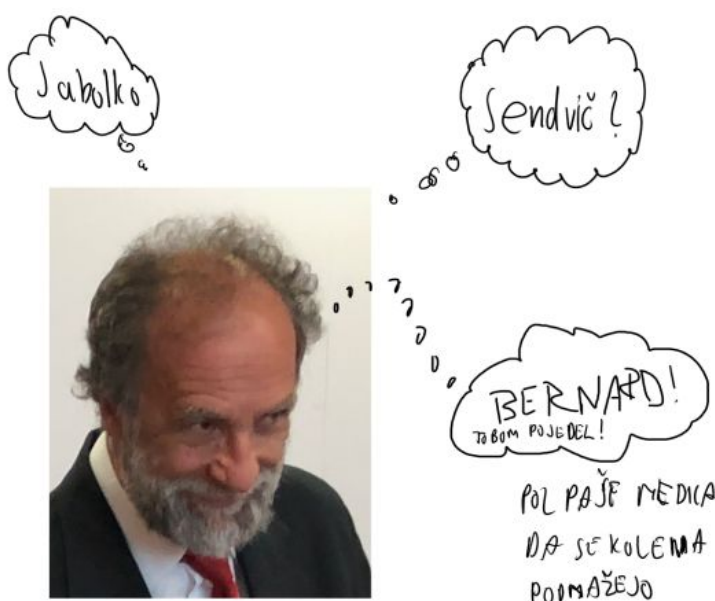
NAMIG: Upoštevajte, vendar ne uporabite, rezervirane vrednosti za VLAN ID (IEEE 802.1Q).

2014/15 Drugi kolokvij

1. naloga: AAA in RADIUS.

1. Peter se je odpravil tokrat v skladko-grenke posle. Prodajati je pričel kavo in čokoladne tablice preko avtomatov. Menite, da bi lahko pri tem uporabil RADIUS protokol? Utemeljite odgovor.

NAMIG: Slika s shemo sistema bi pomagala.



2. Peter je postavil strežnik RADIUS in ustvaril nekaj uporabnikov. Sedaj se boji, da Cefizlju ne bi uspelo prikrasti na njegov strežnik ter ukrasti (prebrati) datoteke /etc/freeradius/users z gesli vseh uporabnikov. Kako naj Peter prepreči škodo ob morebitni takšni kraji? Kako lahko poskrbi, da gesla ne bodo shranjena na strežniku RADIUS v tekstovni obliki? Opišite vsaj 2 načina.

3. Ali imamo lahko FTP strežnik *abc.primer* na IP naslovu X, medtem ko bi imeli poštni strežnik za naslove ...@*abc.primer* pa na naslovu Y? Utemeljite odgovor.

2. naloga: Imeniške strukture in LDAP.

1. Pri protokolu LDAP lahko za varnost prenesenih podatkov poskrbimo na več različnih načinov. Eden je tako, da poženemo LDAP strežnik na posebnih vratih, ki že vsebujejo SSL (ldaps).

(i) Kaj pa, če tega ne naredimo? Kako lahko zaščitimo komuniciranje?

Lahko zaščitimo z IPsec, STARTTLS, SASL

(ii) Pri protokolih imamo pogosto možnost sistematično dodati nove ukaze. Ali ta možnost obstaja tudi pri LDAP? Utemeljite odgovor.

Da, obstaja. Imamo ukaz *extended*, ki ima možnost poljubnega dodatnega ukaza

2. Peter ima obsežen telefonski imenik prijateljev, ki ga hrani v relacijski podatkovni bazi MySQL. Za vsakega prijatelja hrani ime, priimek in telefonsko številko. Peter želi prijateljem ustvariti uporabniška imena in nastaviti gesla za dostop do svoje spletne strani. Poleg tega bi ta uporabniška imena rad uporabljal še za prijavo na računalnike.

(i) Predlagajte dva protokola, ki ju lahko uporabi za prijavo?

Uporabili bi lahko naslov kot geslo, če bi bili IP naslovi prijateljev statični

Ali pa posrednike za razpečevanje gesel (key distribution center)

Ldap - Njihova gesla bi zgeneriral iz njihovih podatkov, ki bi služili kot del celotnega gesla razločevalno ime, Distinguished Name

(ii) Kaj bi moral nastaviti, da bi se uporabniki na računalnikih avtenticirali neposredno z uporabo MySQL?

3. Naštejte vsaj dve pomembni razliki med LDAP v2 in LDAP v3?

LDAPv2 ne zagotavlja ustreznih varnostnih funkcij za uporabo na internetu.

LDAPv2 ne zagotavlja nobenega mehanizma za podatke, celovitost ali zaupnost.

LDAPv3 uporablja Certificate authentication in storitve za varstvo podatkov.

3. naloga: Varnostni elementi.

1. Peter Zmeda je med svojo pisarno v Zgornjih Butalah in županovo pisarno v Spodnjih Butalah vzpostavil VPN. Pri tem je uporabil sistem OpenVPN. Za konec tedna je deževalo in je bil večino časa doma ter je prebral prosojnice predmeta KPOV ter spoznal, da obstaja tudi IPsec.

(i) Ali lahko vzpostavi OpenVPN preko IPsec ali obratno? Utemeljite odgovor.

OpenVPN ni kompatibilen s protokolom IPsec.

(ii) Ali je katerakoli od dveh možnosti smiselna? Utemeljite odgovor.

A ne da IPsec omogoča VPN? Ker VPN omrežje je **navidezno** in **zasebno**. Kar prav tako omogoča IPsec (zakrivanje, celovitost, zaščito pred ponovitvijo komunikacije, zagotavljanje avtentikacije izvora).

2. Peter in Konrad sta z uporabo OpenVPN vzpostavila navidezno lokalno omrežje. Uporabila sta spodnji konfiguraciji: Peter:

```
proto tcp
remote vpn.pavel.net
dev tap
secret skrivnost.key
```

in Konrad:

```
proto tcp
dev tap
secret skrivnost.key
```

Sedaj bi na svojo mrežo rada priklopila še Polono.

(i) Kako bi to lahko storila in ali lahko za priklop Polone uporabijo isto skrivnost?

Storila bi enako kot Peter. Vendar s svojo skrivnostjo.

(ii) Narišite skico omrežja, če Peter in Konrad obdržita trenutne nastavitve in priklopita še Polono.

(iii) Potem narišite še skico omrežja, če se bo poleg Polone na omrežje priklopilo še njenih 7 prijateljic.

(iv) Kaj vse bodo Polona in prijateljice potrebovale na svojih računalnikih, da se bodo lahko prijavile na omrežje?

3. Koliko mora biti najkrajša dolžina gesel, če jih sestavljamo zgolj iz malih črk angleške abecede (26 črk) in števk 0-5, če želimo, da je varnost enakovredna (ali večja) kot pri ključih dolžine 192 bitov?

4. naloga: Razno.

1. Pri standardu IEEE 802.1x nastopajo tri naprave.

(i) Narišite shemo, vpišite vanjo naprave, opišite kakšne so lahko povezave med njimi in opišite vlogo posamezne naprave. Peter Zmeda je dobil čudnega odjemalca, ki zna govoriti pri avtentikaciji za potrebe dostopa do omrežja samo PAP.

(ii) Kje in kaj lahko Cefizelj napade? Razmislite, kakšno škodo lahko povzroči?

(iii) Imate kakšen predlog za zaščito?

2. Peter je v prostem času ovčjerejec in rad gleda filme ovac, 1 ki se pasejo na travnikih. Zaenkrat jih predvaja s strežnika, na katerem ima VLC predvajalnik. VLC v neskončnost predvaja zaporedje videov o ovčkah. Petra malce moti dejstvo, da, če se prijavi na strežnik, skoraj nikdar ne ujame začetka videa. Poleg tega bi rad postavil storitev Video-na-zahtevo.

(i) Kateri kos programske opreme lahko v ta namen uporabi?

(ii) Ali lahko na istem strežniku nudi obe storitvi (video v živo in na zahtevo)?

(iii) Kaj pa na istem naslovu? Utemeljite odgovore!

3. Kako protokol CHAP preprečuje napade s ponavljanjem? Opišite korake, ki jih izvede in kako z njimi preprečuje napade.

Strežnik pošlje izziv

Odjemalec izziv združi z geslom in ga vrne nazaj širifranega z enosmerno razpršilno funkcijo (žeton)

Strežnik preveri pravilnost odgovora

Ker je izziv vedno drugačen, se tako preprečuje napade s ponavljanjem.