**AAA in RADIUS**

1. **RADIUS protokol omogoča tudi beleženje dogodkov.**

**a) Katere vrste dogodkov, ki jih lahko beležimo, pozna protokol?**

* Začetek rabe storitve
* Nadaljnjo rabo ali popravljene podatke
* Zaključek rabe

**b) RADIUS pozna nekaj varnostnih elementov in glavni med njimi uporablja v RADIUS paketu polje Authenticator. Kako točno se ga uporablja pri beleženju?**

Je podpis in je edini vir zagotavljanja verodostojnosti poslanega paketa  
**UPORABA**

* **Odjemalec:** Pošlje strežniku 128 bitno število izračunano iz skrivnosti, vsebine paketa
* **Strežnik (preveri): A se število ujema z skrivnostjo in vsebino paketa**
* **Strežnik (odgovor):** 128 bitno število izračunano iz **skrivnosti**, **podpisa odjemalčevega paketa** in **vsebine paketa**
* **Odjemalec (preveri): A se število ujema z skrivnostjo, podpisom odjemalčevega paketa in vsebine paketa**
* **Če je vse vredu naj bi bil paket verodostojen**

**c) Ta mehanizem žal ne ščiti pred napadamo s ponavljanjem – zakaj? Kako RADIUS ali njegovi uporabniki rešujejo potem problem napada s ponavljanjem?**

* Zato ker **računanje števila ne upošteva ničesar kar bi povedalo kaj o tem kdaj je bil paket poslan**, tako, da če nekdo postreže paket in ga pošlje še enkrat strežnik nebo vedel, da paket ne prihaja od legitimnega odjemalca
* **Problem napada s ponavljanjem lahko uporabniki rešujejo s pomočjo IPsec, ESP**. Saj v ESP glavi se hrani #Seq, ki bo imel ob ponovitvi staro vrednosti, ki se nebo ujemala s pričakovano!
* **Druga opcija je uporaba DIAMETRA**

1. **RADIUS IN CHAP**
2. **Peter se je zapletel v prepir s prijateljem Simonom in trdil da je protokol RADIUS varen protokol, saj si je zapomnil, da je del paketa tudi avtentifikator. Pojasnite vlogo avtentifikatorja v protokolu RADIUS.**

* Avtentifikator v protokolu RADIUS je zgolj podpis, da paket res prihaja od tam kjer naj bi prihajal.
  + **Pri AA. Paketih** ščiti le odgovor **(lahko nekdo spreminja zahtevo in uporabnik nebo avtoriziran)**
  + **Pri podpisovanju ..A paketov** pa ščiti zgolj odjemalčevo zahtevo za beleženja ne pa tudi odgovora **(nekdo se lahko postavi vmes, zavrže pravi paket in pošlje drugačen odgovor)**

1. **Napišite tri scenarije napada na RADIUS protokol in kakšno škodo lahko napad povzroči.**

* **Replay attack:** Radius ne ščiti proti napadu z ponovitvijo, nekdo lahko odgovor avtentikatorja prestreže in po tem, **ko uporabnik ni več avtoriziran pošlje takratni odgovor in uporabniku bo še vedno dovoljen dostop**
* **DoS attack**: ker ne ščiti zahteve odjemalca lahko iz katerega koli serverja pošiljamo številne zahteve avtentikatorju in s tem **zabijemo avtentikator**
* **Man in The Middle:** ker ne ščiti odgovor ..A paketov lahko zamenjamo paket z kakšnim spremenimo paket in **odjemalec nebo vedel, da je dobil napačen odgovor**

1. **Kako protokol CHAP preprečuje napade s ponavljanjem?**

**Z menjavanjem izzivov**. Saj je CHAP tri koračni protokol. Najprej se pošlje izziv potem se ta izziv z enosmerno razpršilno funkcijo združi z geslom in se vrne zakriptiran. Nato pa se preveri pravilnost odgovora. **Če se odgovor kadar koli ponovi izziv več nebo enak!**

1. **CHAP PROTOKOL**

**Peter Zmeda se je tokrat lotil implementacije CHAP protokola, vendar je malce površno prebral RFC, ki opisuje CHAP. Njegova implementacija avtentikacije**

Boruta pri Ani je bila naslednja:

1. Borut pošlje Ani sporočilo, **da se želi avtenticirati**2. Ana Borutu pošlje kot **izziv naključno 192-bitno sporočilo X**3. Borut vzame **skupno skrivnost S, ki je prav tako 192-bitna in izračuna bitni XOR med S in X** ter dobi odgovor **Y : Y = X XOR S**, ki ga vrne Ani  
4. Ana sedaj **pozna tako izziv X, skupno skrivnost S in Borutov odgovor Y** ter lahko preveri, ali je res na drugi strani Borut.

1. **Kako Ana preveri, če je na drugi strani res Borut? Utemeljite odgovor.**

Ana preveri to s pomočjo skupne skrivnosti (kateri zaupa), Boruta avtenticira tako, da mu pošlje neko število in Borut ga mora zakriptirati z dogovorjenim algoritmom in skupno skrivnostjo ter ga poslati nazaj Ani. Če ga Ana z funkcijo in skupno skrivnostjo odkriptera sporočilo in dobi enako število kot ga je poslala.. Potem je Borut res Borut.

1. **Petrova shema ima veliko napako. Katero? Utemeljite odgovor in predlagajte rešitev.**

Problem je, da uporablja za enkripcijo X-a **XOR,** ki nikakor ni primeren zato, ker lahko napadalec z brute forcom zelo zelo hitro ugotovi skupno skrivnost in avtentikacija je kompromizirana!

**Rešitev:** lahko dobro zavarujemo povezavo npr. IPsec ali pa uporabimo močnejšo funkcijo za izračun, ki je Peter nebo strl kot keks

1. **Kaj je to napad z mavričnimi tabelami in kako deluje?**

Mavrična tabela je (večja ko je boljše) zbirka gesel (plain text) in njihovih **hash** vrednostmi. Če napadalcu potem uspe ukrasti **hash** vrednost gesla, in ima ta **hash** shranjen v zbirki potem ugotovi kakšna je plaintext verzija tega gesla in lahko nam vdre v račun

1. **Kako se branimo pred takšnim napadom?**

Pred takšnim napadom se branimo z **soljo** sol je naključno generiran niz, ki se doda geslu. Posledično imamo daljše geslo ter pomembneje **enaki gesli se ne preslikata v isti hash!**