Authentication, Authorization, Accounting and Auditing

Markus Peuhkuri

2002-03-XXX

Luennon aiheet

- Yleistä turvallisuudesta
  - helppo tehdä väärin (enemmän seuraavalla luennolla)
- Käyttäjien kirjautuminen verkkoon
- Laskutus
- Auditointi

Kirjasta kappaleet

-

Turvallisuus: tunnistaminen

- THK 47/1999 M

  > Teleyrityksen televerkoissa ja telepalveluissa on oltava tilaajan tai käyttäjän ja teleyrityksen väliseen sopimussuhteeseen liittyvät todentamis-, pääsynvalvonta- ja kiistämättömyysmenettelyt.

- Laskutus
- Pääsynvalvonta
- Väärinkäytökset
- Molemminpuolinen autentikointi

Miten tunnistetaan

1. Tietää jotain
   - salasana, PIN-koodi
2. On jotain hallussa
   - fyysinen avain
   - älykortti
3. On jotain
   - sormenjälki
   - käsiala

Tietämyksen osoittaminen

- Jotain, minkä vain yksi (harva) henkilö tietää
  - salasana
  - henkilötunnuksen loppuosa
  - äidin tyttönimi
- Edut
  - toteutettavissa ohjelmallisesti
  - aina mukana
- Haitat
  - salakuunneltavissa verkossa ja/tai päätelaitteessa
    $\Rightarrow$ toistohyökkäys
  - arvattavissa / selvitettävissä
  - jaettavissa
  - unohtuneiden selvittäminen 20–40 euroa / tapaus

Salasanan käyttötavat

- Unix-salasana
  - palvelimessa salattuna
  - annettu salasana salataan ja verrataan tallennettuun arvoon

  $\Rightarrow$salasana selvitettävissä vain kokeilemalla tai salakuuntelemalla
- CHAP, HMAC [3]
  - jaettu salaisuus
  - haasteeseen tai aikaan perustuva tulos välitetään
    $\Rightarrow$ ei paljastu salakuuntelulla
  - HMAC: $H(K \oplus opad, H(K \oplus ipad, text))$

H	tiivistealgoritmi (MD5, SHA)
K	jaettu avain
$text$	haaste tai ajasta riippuva teksti
$opad$	tavujono merkkiä 0x5C
$ipad$	tavujono merkkiä 0x36
- Julkiseen avaimeen perustuvat algoritmit
  - avain suojattu esim. salalausesta muodostetulla avaimella

Jotain hallussa

- Magneettikorti
- Älykortti (-avain)
  - avain kortilla, vain operaatioiden tulos ulos
    $\Rightarrow$ periaattessa turvassa. Avain voidaan selvittää mahdollisesti analysoimalla virrankulutusta tai selvittämällä piirin sisäiset kytkennät. Voidaan pilata myös huonolla algoritmillä, GSM SIM kopioitavissa fyysisesti alle 8 tunnin, ehkä alle viikossa radiorajapinnan yli. `http://www.isaac.cs.berke`
- Tilaajajohto
- Edut
  - helposti käsitettävissä

  - allekirjoitusmahdollisuus (eräissä)
- Haitat
  - mahdollisuus hukata, lainata
  - hallintakustannukset
  - mahdollisesti useita yhdellä henkilöllä

On jotain

- Biometria
  - sormenjälki
  - käden suhteet
  - silmänpohja (retina)
  - iris
  - kasvontunnistus
  - äänentunnistus
  - allekirjoitus
  - näppäilyrytmi
- Edut
  - “helppo”
  - vaikeahko väärentää, tosin monet markkinoilla olevista laitteista kotikonstein huijattavissa: `http://www.heise.de/ct/english/02/11/114/`, `http://www.theregister.co.uk/content/`
- Haitat
  - voi hukata, esim. sairaus tai loukkaantuminen
  - ei vaihdettavissa, jos varastetaan
  - väärät positiiviset vs. väärät negatiiviset

Autentikointi verkon yli

- Onko päätelaite luotettava?
  - esim. sormenjälkiskanneri tallentaa kuvan, toistaa myöhemmin
  - takaportit `http://www.acm.org/classics/sep95/`
  - PIN-koodi
- Onko asiakas luotettava
  - voiko asiakas saada etua tekeytymällä toiseksi
  - ilkivalta
- Onko verkko luotettava?
  - salakuuntelu, tekeytyminen
  - molemminpuolinen autentikointi
  - oltava off-line tietoa
- Onko autentikointpalvelin luotettava

Asiakkaan tulo verkkoon

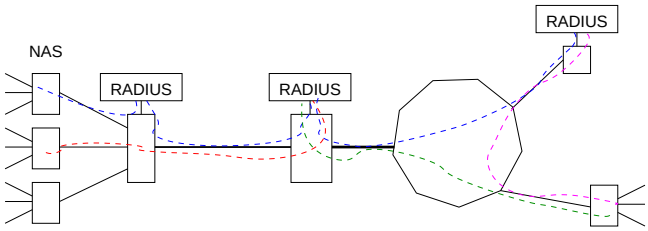
- Ottaa yhteyden pääsypalvelimeen (NAS: Network Access Server)
  - sisäänsoittopalvelin
  - tunnelointipalvelin (IPSEC, L2TP, PPPo{A,E})
  - reunareititin
  - langaton verkko (WLAN,...)
- Esittää valtuudet
  - PAP, CHAP, PKC, biometria...
  - puhelinnumero, tilaajajohto...
- NAS tarkistaa *identiteetin* autentikointipalvelimelta
  - mahdollisesti lisäkysymyksiä
- Pääsyn salliminen ja asetukset valtuutuspalvelimelta
  - IP-osoite, tunnelointi, palomuuriasetukset, kaistanleveys
- Laskenta
  - yhteyden käyttämät resussit laskutusta varten
- Seuranta
  - onko käyttö "oikeanlaista"
  - tarpeita kehittää verkkoa (SLA/QoS-monitorointi)

RADIUS: Remote Authentication Dial-In User Service [5]

- Komponentit
  - käyttäjä
  - asiakas (yleensä NAS)
  - palvelin
- *NAS* lähettää autentikointipyynnön
  - käyttäjän salasana (tai haaste/vaste) salataan salasanasta ja NAS:n ja autentikointipalvelimen jaetusta avaimesta muodostetulla avaimella
    $\Rightarrow$ salii yhteydenotot ainoastaan "oikeilta" NAS:lta
- Tarvittaessa välitetään eteenpäin
  $\Rightarrow$ autentikointipalvelin asiakas toiselle
- Useita autentikointipalvelimia
  - vikasietoisuus
  - erilliset käyttäjähallinnoinnit
- Tukee eri autentikointityyppejä
  - salasana
  - haaste-vaste
  - EAP (PPP Extensible Authentication) [2] tarvittaessa läpinäkyvästi [4]
  - myös esim. porttityyppiä[1] tai puhelinnumeroa voidaan käyttää apuna

[1] Esim. modeemi, ISDN, virtuaalinen (eri tunneleita), xDSL,...

RADIUS



RADIUS - valtuutus

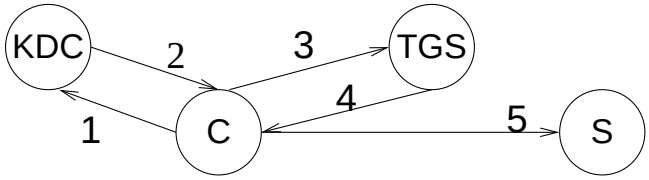
- Käyttäjäparametrien asettaminen
  ⇒ sopeutus tilaajakohtaiseen käyttöön
- Suodatukset
  - suodatintunniste
- Aikavalvonnat
- Takaisinsoitto
- Porttien määrä esim. monikavava-PPP:n kanssa [6]

RADIUS - laskenta

- Resussien käytön seuranta
  - aika
  - paketti- ja tavumäärät
  - yhteyden purkusyy
- Aloitus- ja lopetussanomat
- Käyttäjäluokka läpinäkyvästi valtuutussanomasta
- Moniyhteys: useita yhteyksiä
  - esim. monikanava-PPP: uusi yhteys kanavamäärän muuttuessa, sama moniyhteys

Kerberos

- Osittain luotetut päätelaitteet
- Oikeus kommunikoida kolmannelta osapuolelta
  1. käyttäjä autentikoituu salasanalla salatulla viestillä avainpalvelimeen
  2. saa lipun lipunmyöntöpalvelimelle (rajallinen elinikä)
  3. hakee lipun tiettyyn palveluun lipunmyöntölipun avulla
  4. saa lipun tiettyyn palveluun
  5. yhteys muodostetaa, esittää lipun
- Eri KDC:n autentikoiduttava ristiin
  ⇒ helposti turvaongelma



Tulevaisuus

- Käyttö lisääntyy
  - mitä tahansa käyttäjiä
  - mihin tahansa
  - millä tavoin tahansa
  - millaista käyttöä tahansa
- Suuri määrä osapuolia
  - GSM-operaattoreita joitakin satoja
  - internet-operaattoreita kymmeniä tuhansia: aktiivisia autonomisia alueita yli 120,000
- Eri A-komponenttien eriyttäinen
  - DIAMETER: valmis 2003 lopussa?
- Verkkoriippumaton autentikointimenetelmä
  - PANA: Protocol for carrying Authentication for Network Access

Vaatimuksia AAA-protokollille [1]

- Skaalautuvuus
- Vikasietoisuus
- Keskinäinen autentikointi
- Kuljetuskerroksen turvallisuus
- Tietojen luottamuksellisuus
- Tiedon eheys myös palvelimien läpi
- Sertifikaattien kuljetus
- Luotettava AAA-kuljetusmekanismi
- IPv4, IPv6-yhteensopivuus
- Välityspalvelimien ja reititysvälittäjien tuki
- Auditoitavuus
- Ei kaksinkertaista turvallisuutta
- Palvelukohtaiset määritteet läpinäkyvästi

Autentikointivaatimukset

- Osoitepohjainen tunnistus
- CHAP-tuki
- EAP-tuki
- PAP/selvätekstituki
- Uudelleenautentikointi pyydettäessä
- Valtuutus ilman autentikointia

Valtuutusvaatimukset

- Staattinen ja dynaaminen osoitejako
- Radius-yhdyskäytävätuki
- Hylkäysmahdollisuus
- Ei edellytä linkkikerroksen (2) tunnelointia
- Uudelleenvaltuutus pyydettäessä
- Tuki pääsysäännöille, rajoituksille ja suodatuksille
  - yhteyden kestoaika ja käyttämättömyyskatkaisu
  - pakettisuodatus
  - staattiset reitit
  - QoS-vaatimukset
- Tilan neuvottelu
- Sopimaton purku verkon puolelta

Laskennan vaatimukset

- Reaaliaikainen laskenta (sekuntteja)
- Tiiviit tietueet
- Tietueiden laajennettavuus
- Erälaskenta
- Taattu välitys
- Aikaleimat
- Dynaaminen laskenta

Yhteenveto

- RADIUS nykyisin käytetyin AAA-järjestelmä
- DIAMETER laajentaa, monipuolistaa: 3G
- AAA edellytys
  - käyttöpohjaiselle laskutukselle
  - käyttäjäprofiileille
- Yhteensopivuus ja päästä-päähän resussointi kysymyksiä
- Turvallisuus vaikea tehdä oikein

Viitteet

[1] B. Aboba, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, G. Zorn, G. Dommety, C. Perkins, B. Patil, D. Mitton, S. Manning, M. Beadles, P. Walsh, X. Chen, S. Sivalingham, A. Hameed, M. Munson, S. Jacobs, B. Lim, B. Hirschman, R. Hsu, Y. Xu, E. Campbell, S. Baba, and E. Jaques. Criteria for Evaluating AAA Protocols for Network Access. Request for Comments RFC 2989, Internet Engineering Task Force, November 2000. (Informational). URL:`http://www.ietf.org/rfc/rfc2989.txt`.

[2] L. Blunk and J. Vollbrecht. PPP Extensible Authentication Protocol (EAP). Request for Comments RFC 2284, Internet Engineering Task Force, March 1998. (Internet Proposed Standard) (Updated by RFC2484). URL:http://www.ietf.org/rfc/rfc2284.txt.

[3] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments RFC 2104, Internet Engineering Task Force, February 1997. (Informational). URL:http://www.ietf.org/rfc/rfc2104.txt.

[4] C. Rigney, W. Willats, and P. Calhoun. RADIUS Extensions. Request for Comments RFC 2869, Internet Engineering Task Force, June 2000. (Informational). URL:http://www.ietf.org/rfc/rfc2869.txt.

[5] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). Request for Comments RFC 2865, Internet Engineering Task Force, June 2000. (Internet Draft Standard) (Updated by RFC2868) (Obsoletes RFC2138). URL:http://www.ietf.org/rfc/rfc2865.txt.

[6] K. Sklower, B. Lloyd, G. McGregor, D. Carr, and T. Coradetti. The PPP Multilink Protocol (MP). Request for Comments RFC 1990, Internet Engineering Task Force, August 1996. (Internet Draft Standard) (Obsoletes RFC1717). URL:http://www.ietf.org/rfc/rfc1990.txt.