



HELSINKI UNIVERSITY OF TECHNOLOGY

# Kerberos V ja toistohyökkäykset

Yliopistojen tietoturvapäivät 2004

Antti Tikkanen  
Teknillinen korkeakoulu, Atk-keskus  
antti.tikkanen@hut.fi



HELSINKI UNIVERSITY OF TECHNOLOGY

## Kerberos V ja toistohyökkäykset

- Lyhyt johdanto Kerberos V -protokollaan
- Mitä toistohyökkäykset ovat
- Kuinka niiltä suojaudutaan
- Kokemuksia tuotteista
  - Windows Server 2003
  - Windows Server 2000
  - NetApp Data ONTAP 6.4R1
  - Samba 3.0
- Käytännön suosituksia



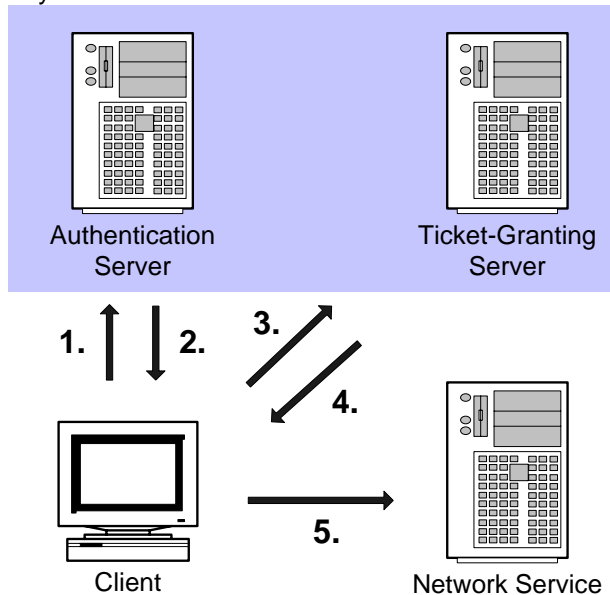
# Kerberos V

- Autentikointiprotokolla, joka perustuu
  - symmetriseen salaukseen
  - luotettuun kolmanteen osapuoleen
- Ensisijainen autentikointimekanismi Windows 2000 ja 2003 –ympäristöissä
  - SMB-yhteydet tiedosto- ja tulostuspalvelimille
  - LDAP-yhteydet Active Directoryyn
- Turvallisuutta kritisoitu aikaisemmin artikkelissa *Limitations of the Kerberos Protocol* (S. Bellare, 1991)
  - "A number of weaknesses are apparent; the most serious is its use of an authenticator to prevent replay attacks."



# Kerberos V

Key Distribution Center



1. KRB\_AS\_REQ
2. KRB\_AS\_REP
3. KRB\_TGS\_REQ
4. KRB\_TGS\_REP
5. KRB\_AP\_REQ



# Toistohyökkäykset

- Perustuvat viimeisen viestin (KRB\_AP\_REQ) hyväksikäyttämiseen
- Viesti ei esiinny yksin, vaan toisen protokollan sisällä
  - SMB: SESSION\_SETUP\_ANDX
  - LDAP: Bind Request
- KRB\_AP\_REQ:  $\{A_{c,s}, T_{c,s}\}$ 
  - **Ticket**  $T_{c,s}$ : server, {client, addr, validity,  $K_{c,s}$ , flags} $K_s$
  - **Authenticator**  $A_{c,s}$ : {client, time, checksum, seskey} $K_{c,s}$
- Hyökkääjä voi verkkoa kuuntelemalla
  - toistaa jo käytetyn viestin (passiivinen hyökkäys); tai
  - estää palvelinta saamasta viestiä ja käyttää sen itse (aktiivinen hyökkäys)



# SMB ja KRB\_AP\_REQ

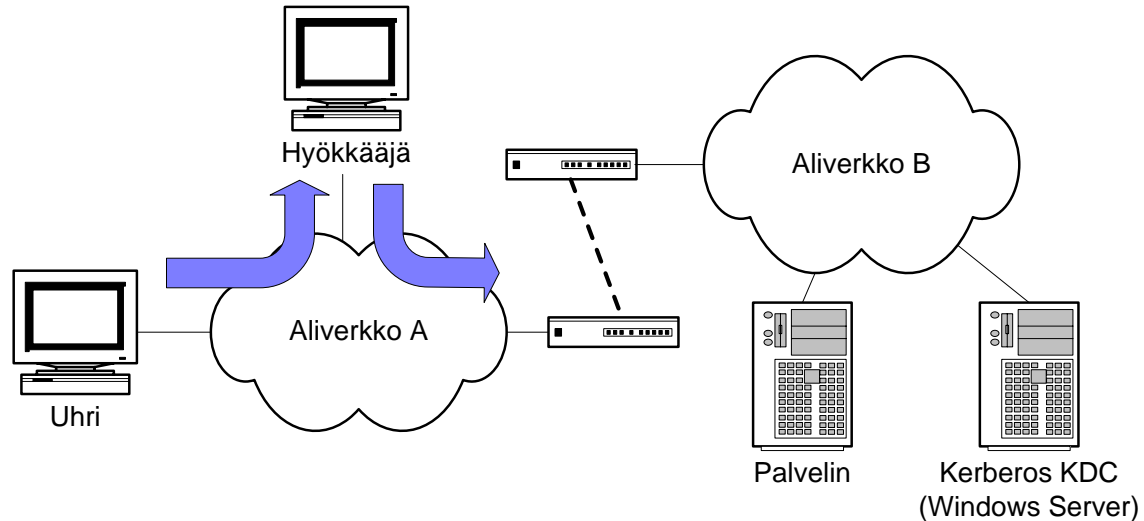
```

GSS-API
  OID: 1.3.6.1.5.5.2 (iso.3.6.1.5.5.2) (SPNEGO - simple Protected Negotiation)
  SPNEGO
    negTokenInit
      mechType
      mechToken
        krb5_blob: 6082059706092A864886F71201020201...
          OID: 1.2.840.113554.1.2.2 (iso.2.840.113554.1.2.2) (KRB5 - Kerberos 5)
          krb5_tok_id: KRB5_AP_REQ (0x0001)
            Kerberos
              Version: 5
              MSG Type: AP-REQ
              APOptions: 0020000000
              Ticket
                Version: 5
                Realm: WIN.HUT.FI
                Service Name: CCPRINT02$
                Encrypted Data: Ticket data
                  Type: rc4-hmac
                  CipherText: 658A59409E90548D7B51AC0B591765C0...
                Encrypted Data: Authenticator
                  Type: rc4-hmac
                  CipherText: 31CC7A15D437533DF3274068CD29BD85...

```



## Esimerkkiskenaario



## Esimerkkihyökkäys: SMB

- Kytke IP-forwarding päälle
  - `echo '1' > /proc/sys/net/ipv4/ip_forward`
- Ohjaa uhrilta tuleva SMB-liikenne proxyllle
  - `iptables -t nat -A PREROUTING -i eth0 -p tcp -s <victim ip> -d <server ip> --dport 445 -j REDIRECT --to-port 445`
- Käynnistä proxy
  - `smb_catchblob -s <server ip> -l <attacker's external ip> -p 445`
- Ohjaa uhrin liikenne oletuskäytävän sijasta itsellesi
  - `arp spoof -t <victim ip> <gateway ip>`
- Ota yhteys palvelimelle muunnellulla asiakasohjelmistolla
  - `smbclient //<server ip>/<share> -k`



# Hyökkäyksen seuraukset

- Yhteys palveluun käyttäjän oikeuksin
    - Kerberosin aikarajoituksilla ei enää merkitystä, yhteysaika rajoittamaton
  - Tavallista käyttäjää vastaan
    - Pääsy käyttäjän tiedostoihin (SMB)
    - Pääsy käyttäjän henkilökohtaisiin tietoihin (LDAP)
  - Ylläpitäjää (Domain Administrator) vastaan
    - Täydet oikeudet kaikkiin palvelimen tiedostojakoihin ja paikallisiin levyihin (SMB)
    - Täydet oikeudet kaikkiin objekteihin Active Directoryssa (LDAP)
    - Käytännössä täysi kontrolli kaikkeen
- 
- 



# Protokollan omat suojamekanismit

- Ticketin tulisi sisältää asiakkaan verkko-osoite
    - Palvelin vertaa käyttöjärjestelmän ilmoittamaan lähdeosoitteeseen
  - Palvelin ei saa hyväksyä liian vanhoja autentikaattoreita
  - Palvelimen tulisi muistaa jo käytetyt autentikaattorit
  - Kuitenkin:
    - Toteutusten yksityiskohdat vaihtelevat
    - Vaikka kaikki olisi toteutettu oikein, nämä mekanismit eivät ole riittäviä
- 
-



## Muut suojautumiskeinot

- Suojautuminen verkkoliikenteen kaappauksilta lähiverkossa (ARP spoofing)
  - Staattiset ARP-taulut
  - IDS-järjestelmät
- IPSec
  - Konfigurointi siten, ettei mahdollisuutta pudota selväkieliseen liikennöintiin
- SMB- ja LDAP-liikenteen eheyden varmistaminen
  - Konfigurointi siten, että tarkistussummat vaaditaan aina
  - Hyökkääjä ei tiedä sessioavainta  $K_{c,s}$  eikä voi generoida tarkistussummia
  - Yleensä tehokkain ja helpoin suojautumiskeino



## Kokemuksia tuotteista: Windows Server 2000 ja 2003

- KDC ei sisällytä ticketteihin verkko-osoitteita
  - Hyökkääjän ei tarvitse väärentää lähdeosoitetta
- LDAP- ja SMB-palvelimet muistavat käytetyt autentikaattorit
  - Aktiivinen hyökkäys edelleen mahdollinen
- Liikenteen eheyden varmistus mahdollista
  - SMB-protokolla suojaton Windows 2000 Serverin oletusarvoilla
- Erityinen huomio: palvelunimien käsittely puutteellista
  - Palvelut käyttävät samaa konetunnusta



## Kokemuksia tuotteista: NetApp Data ONTAP 6.4R1

- Oma käyttöjärjestelmä levypalvelimia varten
    - Paino suorituskyvyssä ja saatavuudessa
  - Ei muista käytettyjä autentikaattoreita
    - Passiivinen kuuntelu riittää hyökkäjälle
  - Ei tukea asiakkaiden SMB-liikenteen eheyden varmistamiselle
  - Suojautuminen hyvin vaikeaa
    - Versiossa 6.5 mukana parannuksia?
- 
- 
- 



## Kokemuksia tuotteista: Samba 3.0 beta

- Tutkimukset kesällä 2003 versiolla 3.0 beta1
  - Ei muista käytettyjä autentikaattoreita
  - Ei palvelinpuolen tukea SMB-liikenteen eheyden varmistamiselle
  - Puutteet korjattiin lopulliseen versioon
    - Oletuskonfiguraatiossa palvelin ei käytä eheyden varmistamista (SMB Signing)
- 
- 
-



# Käytännön suosituksia

- Oman verkon fyysisen turvallisuuden varmistaminen
    - Esimerkiksi kampusympäristössä lähes mahdotonta
  - Linkkikerroksen turvallisuus
    - Kytetty verkko ei riitä
    - Staattiset ARP-taulut työasemissa
  - Verkkokerroksen turvallisuus
    - IPSec
    - Konfigurointi siten, että putoaminen selväkieliseen liikenteeseen ei mahdollista
  - Sovelluskerroksen eheyden varmistaminen (LDAP, SMB)
    - Konfigurointi siten, että tarkistussummat vaaditaan aina
- 
- 



# Työkalut ja linkit

- Alkuperäinen paperi "Kerberos V Security: Replay Attacks"
    - <http://www.hut.fi/u/autikkan/kerberos/>
  - Valmiit työkalut
    - arspoof: <http://naughty.monkey.org/~dugsong/dsniff/>
  - Omat työkalut
    - smb\_catchblob
    - ldap\_catchblob
    - Modifioitu smbclient
    - Saatavilla pyynnöstä: antti.tikkanen@hut.fi
- 
-