IP telephony security overview

Martin Skala

Fakulta informatiky Masarykovy univerzity

19. listopadu 2009

Souhrn z technické zprávy CESNET 35/2006 (M. Vozňak, J. Růžička)

Obsah I

Obsah II

H.323

- VoIP protokol (ITU-T H.323 v roce 1996)
- ASN.1 + BER
- H.225.0 Q.931 - signalizace pro volání
- RAS (Registration, Admission, Status) - správa volání využívající GK (GateKeeper)
- H.245 - signalizace medií
- H.235 (ve H.323v2 z roku 1998) - autentizace
  - symetrická kryptogragie (heslo + symetrické šifrování)
  - hashování hesel
  - public-key
- CryptoToken - informace potřebné k autentizaci
  - RAS
  - H.225.0 Q.931
- RTP

Ukázka pole CryptoToken z RRQ (Registration Request) zprávy

```
cryptoTokens: 2 items
Item 0
Item: cryptoEPPwdHash (0)
cryptoEPPwdHash
alias: h323-ID (1)
h323-ID: 950012315
timeStamp: Feb 26, 2006 15:36:41.000000000
token
algorithmOID: 1.2.840.113549.2.5 (md5)
paramS
hash: 8BB5DFAE1F23EA0AA5C7E73C23B18639
```

- VoIP protokol (IETF SIP, RFC 2543, 3261)
- založený na HTTP (textově orientovaný)
- autentizace
  - HTTP Basic (zakázáno v RFC 3261)
  - HTTP Digest Access Authentication
- komunikace
  - User-to-User
  - Proxy-to-User
- RTP

- MitM (Man-In-The-Middle)
- DoS (Denial of Service)
  - Hůře zvladatelný než v případě čistě počítačových sití
  - K přetížení linek stačí menší počet zpráv
  - Obrana
    - v podobě limitu počtu požadavků z jednoho zdroje
    - účinnost řešení značně snížena DDoS
- DNS Spoofing a jiné útoky na DNS
  - rozšířené DNS záznamy
  - SRV záznamy
    - upřesnění serverů spravujících danou doménu
    - podvržení záznamu → nedostupnost nebo přesměrování
    - řešením použití DNSSec
- Upravení, přesměrování nebo ukončení probíhajícího hovoru

- SPIT (Spam Over IP Telephony)
  - Pro útok je charakteristické:
    - větší šířka pásma
    - větší nároky na hardware
    - menší množina potencionálních příjemců
    - pomalejší distribuce
  - Problém s detekcí SPITu (požadavek na real-time přenos)

- SRTP
- ZRTP
- S/MIME
- IPSec
- TLS

- SRTP (RFC 3711)
  - Šifrování datových proudů
  - AES (klíč 128b, sůl 112b)
  - Autentizace, integrita
  - Ochrana proti replay útoku
- ZRTP (IETF draft-zimmermann-avt-zrtp-16)
  - Postavené na SRTP
  - Definuje ustanovení klíče metodou Diffie-Hellman
  - Ochrana proti útoku Man in The Middle (MiTM)
  - Iniciálně Short Authentication String (SAS)

- SDP (Session Description Protocol)
  - RFC 2327, 3266, 3388, 4566
  - SIP, H.323, SAP, ...
  - session initiation, announcement, invitation
- V těle zprávy (SDP + podepsané hlavičky)
- PKI infrastruktura
- Perzistentní hlavičky
  - To, From
  - Cseq, Call-id
  - Contact - může být problém s NAT (lokální adresa)
- Obsah SDP v těle zprávy může být šifrován
- Zamezí „útočníkovi“ vidět a měnit IP, porty nebo kodeky
- End-to-End integrita a důvěrnost
- Může omezovat funkčnost Session Border Controllerů

- Tunelování
- Transparentní
- Skrytí identity volajících
- Může omezovat funkčnost Session Border Controllerů
- Ověření certifikátů během vyjednávání spojení
- Zajišťuje šifrování pouze k dalšímu hopu (hop-by-hop)
- Lze kombinovat s S/MIME

- AAI (Autentizační a Autorizační Infrastruktura)
- Kerberos, Radius, TACACS, ...
- Zprostředkování hovorů pomocí „home“ serverů
- Identita uživatele
- Autentizace uživatele a autorizace k hovoru
- Aplikace politik a skupin
  - Lokální vs. globální politika
  - Skupina student vs. profesor

- Uzavřené ostrovy (closed islands)
- GDS (Global Dialing Scheme) - hierarchie H.323 GKs (GateKeeper)
- GDS přímo nepodporuje SIP
- Dostupnost závisí na dostupnosti vyšší úrovně v hierarchii
- Příkladem síť Eduroam

- Síť RADIUS serverů
- Autentizaci napříč institucemi, které jsou do sítě eduroam připojené
- IPSec kanály minimálně na národně-institucionální úrovni
- Podobné řešení lze použít i v GDS (hierarchii GateKeeperů)

- Security Assertion Markup Language
- Založený na XML
- Standard pro výměnu autentizačních a autorizačních dat
- OASIS
- SIP-SAML

- E.164 NUmber Mapping
- Mapování mezi adresovými prostory
- Telefonní čísla na URI
- Číslice telefonního čísla tvoří hierarchicky strom
- Naming Authority Pointer (NAPTR)

Nějaké dotazy?

Nějaké dotazy?

Děkuji za Vaši pozornost

- http://www.cesnet.cz/doc/techzpravy/2006/voip-security/
- http://www.softarmor.com/wgdb/docs/draft-tschofenig-sip-saml-04.html
- http://tools.ietf.org/html/draft-ietf-sip-saml-06
- http://www.rfc-editor.org/rfc/rfc3711.txt - SRTP
- http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-16
- http://www.voip-info.org/wiki/view/SDP
- http://en.wikipedia.org/wiki/ENUM