

TALK for you

Nummer 7 - 2010

Din guide till IP

God Jul
och
Gott Nytt År
önskar
TALK TELECOM

Ur innehållet

RFID

Säker passage med plastbricka

Intertex

Nu ännu starkare säkerhet för SIP

Snom - marknadens säkraste IP-telefon

TALK TELECOM

Distribution, Installation, Integration och Expertis inom IP

Talk har ordet

IP telefoni växer starkt och de flesta är överens om att det är framtiden. Därför är det viktigt att lyfta fram att ljudet transporteras på nätverk och är därmed tillgängligt för hackare och attacker på samma sätt som data-nätverk varit i årtionden.

Taltrafiken över IP behöver därför skyddas för åtkomst från obehöriga.

Avlyssning är ett av de vanligaste problemen. Okrypterad VoIP-trafik över internet kan alla med nätverksåtkomst tjuvlyssna på t.ex. när du uppger ditt kreditkortsnummer när du bokar semesterresan. Det enda som behövs är ett verktyg för att fånga upp ljudströmmar som finns fritt tillgänglig på internet. Med detta verktyg kan man börja lyssna av rösttrafik på nätverket.

Kidnappning av växlar är ett annat problem. En hackare kan dränka din SIP PBX med falska förfrågningar, vilket gör det omöjligt att skicka eller ta emot samtal, eller tänk dig att din telefon ringer för evigt. Du plockar upp, inget svar, lägg på, och det ringer igen.

Utmaningen är att nätverk för IP baserad röstöverföring och alla IP protokoll som används för att skicka röst trafik över IP innehåller brister. Det blir därför viktigt att välja utrustning som redan från början kan täppa till de säkerhetshål som kan finnas.

Gör säkra val och välj Talk Telecom. ;-)



Mikael Johansson, Talk Telecom AB

Läs mer:

Några av de mekanismer som kan ge en säker miljö med VoIP är:

- Authorization
- Authentication
- Transport Layer Security (TLS)
- Media encryption (SRTP)

Läs gärna mer på:

<http://wiki.snom.com/Category:HowTo:SRTP>

Snom 3XX / 8XX

Förhindra avlyssning av dina telefonsamtal

Snom har ett mycket högt säkerhetstänkande i sina produkter. Snom använder sig av de mekanismer som finns för att man ska kunna ha möjligheten till en säker ljudöverföring. Samtliga Snom telefoner har en säker SIP signalering genom att använda TLS (Transport Layer Security) samt kryptering av ljudströmmen med SRTP (Secure Real-Time Transport Protocol).

SRTP är en säkerhetsprofil som är idealisk för att skydda röst över IP-trafik. I snom 370, snom 821 och snom 870 medföljer dessutom en VPN klient vilket ger möjlighet att sätta upp en VPN tunnel för att skapa säker taltrafik.

Vill du konfigurera dina snom telefoner säkert? Hör av dig till oss så hjälper vi dig med det.

Teknikfakta

- Secure SIP (SIPS), Krytering och integritets skydd (Hop-by-hop), liknande https
- Skydd för media (SRTP), idelaiskt för skydd av VoIP-trafik. AES 128 bitars kryptering.
- Transport Layer Security (TLS) -specifikation till stor del baserad på SSL (Secure Socket Layer). TLS kommunikationen mellan Snom telefon och SIP registrar är säkrad

Snom IP-telefoner försvårar avlyssning med avancerad krypteringsteknik

SNOM GER EN MYCKET HÖG IP SÄKERHET TACK VARE TLS, SRTP OCH MÖJLIGHET TILL VPN

Snom 870

Cryptophone Edition - Ny supersäker version

Cryptophone har alla funktioner som vanliga Snom 870 men är speciellt framtagen för krypterad kommunikation över vanliga IP nätverk. CryptoPhone Edition är utvecklad i samarbete med GSMK och snom.

Telefonen är helt kompatibel med GSMK CryptoPhone IP mobil och satellittelefoner, och bygger på den senaste tekniken för säker end-to-end krypterad röstkommunikation. Den har 256-bit AES och Twofish sessionskryptering samt 4096-bit Diffie-Hellman key exchange, readout-hash based key authentication, och sessionsnycklar som genereras för varje samtal och därefter förstörs efter samtalet avslutas. Lanseras Q1 2011



Säkra telefonen från obehörig användning med knapplås och PIN-kod

Vill du förhindra obehörig användning kan du låsa telefonen med en kod, precis som på en mobiltelefon. En bra funktion att använda i kontorsmiljö med t.ex. free seating.

Knapplåset aktiverar man via telefonens webbgränssnitt och för att sedan kunna använda telefonen behöver PIN-koden anges på skärmen först. Det går även att få ytterligare nivå av säkerhet genom att ange administratörsrättigheter med användarnamn och lösenord.

Läs mer på:

http://wiki.snom.com/wiki/index.php/Settings/keyboard_lock_pw

Fler tips för säkrare telefoni med Snom:

- Säkra webbgränssnittet med användarnamn och lösenord
- Stäng av http-åtkomst och tillåt endast https
- Aktivera gömda tecken för lösenord (hidden tags)
- Sätt separat användarnamn och lösen för adminläget



Baudisch

Öppna porten med en bricka

Baudisch kompletta lösningar för dörröppning med Bild och Tal över standard SIP. Ansluts direkt mot LAN och med standard SIP kommunikation. Tack vare matning över Lan (PoE) behöver inte ens ström dras fram.

Nu är det enkelt att integrera RFID kontroll i Baudisch dörrpassagesystem. Med en ”plastbricka” (transponder chip) öppnas dörren för passage. Transponderläsaren passar modulärt i Baudisch dörrsystem, läser av chip och med ett relä öppnas dörren. Går att bygga ut med en centralenhet som kan administrera och godkänna, och hålla reda på, passage-rättigheter på olika tider.



SIP Brandvägg IX78 - Nu med ännu starkare säkerhet

Ett antal nya och bekväma säkerhetsfunktioner har introducerats i samband med att mjukvarureleasen 5.30 blivit tillgänglig för IX78. Vi rekommenderar alla att uppdatera sina brandväggar. Detta kan enkelt göras via brandväggens webbgränssnitt.

De nya och viktiga säkerhetsfunktionerna är de följande;

Signaturigenkänning

De vanligaste attackerna från programmet SipVicious stoppas automatisk med senaste mjukvara 5.30F2. Om den interna SIP-proxyn detekterar kända signaturer i SIP-headrar från någon som attackerar så blockeras IP-adressen i 60 sekunder. Du kan dessutom lägga till nya signaturer manuellt.

SIP flood detektering

Ett generellt SIP DoS-attack skydd som används mot attacker utan känd signatur. Om den interna SIP-proxyn detekterar mer än 40 paket/sekund från samma IP-adress säger den till den interna brandväggen att blockera IP-adressen i 300 sekunder och svarar inte förrän SIP pakethastigheten är lägre än 5 paket/sekund. Du måste själv konfigurera detta skydd.

Skydd mot brute force attack

Skydd mot SIP "brute force dictionary"-attacker, dvs man kan inte gissa lösenord hur många gånger som helst från samma IP-adress. Endast 3 registreringsförsök från en viss IP-adress inom 30 sekunder är tillåtna. Du måste själv konfigurera detta skydd.

Lösenord

Använd aldrig svaga lösenord som lätt kan gissas av en robot. Det kan bli väldigt dyrt om någon lyckas gissa sig till dina kontouppgifter och dessutom lyckas ringa på din bekostnad. Lösenordet bör vara minst 10 tecken långt bestående av blandade gemener och versaler, siffror samt tecken.

Exempel på ett starkt lösenord: Zi!VpX#r7L. Ett konto som endast har 4 siffror (1952) som lösenord knäcks normalt mycket snabbt. Lösenordet är din säkerhet - ingen kedja är starkare än den svagaste länken. Tänk även på att lösenordet till din Intertext router bör vara starkt om du öppnar upp den för fjärrkonfigurering utifrån. Det finns även möjlighet att begränsa så att fjärrkonfigurering av din router endast tillåts från en IP eller subnät, samt kan välja HTTPS om du har en IX78.

BRANDVÄGGAR FRÅN INTERTEX GÖR DIN IP-TELEFONI SÄKER OCH BEKYMMERSFRÄ