Security-aspecten bij Voice over IP

Will Franken

Voice over IP (VoIP) is een techniek die het mogelijk maakt om datanetwerken in te zetten voor telefonie. De populariteit van VoIP neemt toe zowel bij bedrijven als particulieren. Het geloof van de markt in VoIP is onder andere te zien aan de aspiraties die datacommunicatie leveranciers en applicatie service providers nu in een hoog tempo ontwikkelen.

W.A.J. (Will) Franken RE CISA is mede-eigenaar van Audiris, een adviesorganisatie gericht op IT-auditing en Information Risk Management. Sinds 1996 is hij als IT-auditor en consultant werkzaam op het gebied van informatiebeveiliging, risicomanagement en compliance. Hij heeft dit artikel op persoonlijke titel geschreven.

Voice over IP ontwikkelt zich stormachtig en niet in de laatste plaats door de kostenbesparingen die in het vooruitzicht worden gesteld. Organisaties hoeven minder te investeren in infrastructuur en ook op belkosten zijn aanzienlijke besparingen te realiseren. Daarnaast is het vanuit een beheerperspectief goedkoper om één netwerk te beheren in plaats van twee. VoIP-specifieke opties zoals *instant messaging* en *rich media conferencing* (gecombineerd spraak, data en video) worden minder genoemd als motivatie om over te stappen naar Voice over IP maar worden wel steeds belangrijker in de communicatie.
De voordelen zijn evident, echter, vermeld dient te worden dat het (IP) datanetwerk niet is ontworpen voor telefonie. Quality of Service en beveiliging zijn twee belangrijke issues die moeten worden opgelost. In dit artikel zal vooral worden ingegaan op de beveiliging van VoIP.

Voice over IP

Voice over IP betreft de infrastructuur en technologie die de transmissie van spraak over een pakket geschakeld IP netwerk mogelijk maakt. Vergeleken met circuit geschakelde netwerken waarbij resources niet hoeven te worden gedeeld met andere sessies, gaan pakket geschakelde netwerken weliswaar efficiënter om met de beschikbare netwerkcapaciteit maar kunnen minder garanties bieden ten aanzien van de kwaliteit van de verbinding zoals die door de gebruiker wordt ervaren.

In tegenstelling tot de transmissie van data waarbij veel toepassingen niet of nauwelijks gehinderd worden door kleine vertragingen is Voice over IP juist wel erg gevoelig voor performance degradatie. Bij de inrichting en beheer van VoIP netwerken is er dan ook veel aandacht voor *quality of service* en *traffic shaping*[1] en is er weerstand tegen beveiligingsmaatregelen omdat die mogelijk ten koste gaan van performance en/of bandbreedte.

Overzicht Voice over IP

Hardware infrastructuur

Een standaard VoIP architectuur wordt gekenmerkt door de aanwezigheid van een aantal specifieke componenten. De fysieke uitvoering van deze componenten is leveranciersafhankelijk waarbij sommige leveranciers ervoor hebben gekozen om bepaalde functionaliteiten te integreren in één appa-

raat, terwijl anderen, omwille van redundantie, juist weer opteren voor spreiding van functionaliteiten over meerdere apparaten. Daarnaast zijn er componenten die in elk netwerk wel voorkomen zoals firewalls, switches en routers. Echter, om VoIP te ondersteunen dienen deze componenten wel om te kunnen gaan met Quality of Service instellingen zoals DiffServ[2] en RSVP[3] waarmee voice verkeer kan worden geprioriteerd en waarmee pakketten die een denial of service aanval kunnen veroorzaken kunnen worden uitgesloten.
Er dient te worden opgemerkt dat de markt voor de zogenoemde 'converged networks'[4] sterk in beweging is. Zo zal OCS 2007[5] (Microsoft Office Communications Server 2007) in voorkomende gevallen een alternatief zijn voor een op IP gebaseerde telefooncentrale.
Hierna volgt een overzicht van de belangrijkste componenten in een VoIP architectuur**.**

User agents

Een user agent is een verzamelnaam voor IP phones, softphones of elk ander apparaat dat in staat is om een communicatie sessie te initiëren over een pakket geschakeld netwerk.

Een IP phone (*hard phone*) is een client apparaat dat via een ethernet aansluiting wordt aangesloten op het computernetwerk. Ieder toestel heeft een IP adres waarmee het zich identificeert bij een telefooncentrale. Het apparaat ondersteunt onder andere compressie en decompressie, netwerk management en signalering.

Een softphone is een software programma waarmee spraakverkeer wordt afgehandeld gebruikmakend van computer audioapparatuur. Maar een *softphone* kan ook zonder computer speakers en microfoon. De softphone kan via de media server aangeven welk PSTN (Public Switched Telephone Network ofwel vaste net) nummer te bellen voor het versturen en ontvangen van gesprekken. Op die manier kunnen ook gewone telefoons deel uitmaken van het netwerk.

IP-PBX

Een PBX (Private Branch eXchange) is een telefooncentrale die is belast met het opzetten en onderhouden van verbindingen tussen aansluitingen (*call management*) en additionele communicatie opties zoals *call forwarding* en *voicemail*. Een IP-PBX en ook een hybride PBX hebben in essentie dezelfde functionaliteiten maar bieden tevens ondersteuning voor Voice over IP, naast tal van andere opties. Een voorbeeld van een optie die kan worden aangezet in sommige IP-PBX'en is: 'Disaster Routing' waarmee meerdere paden voor voice verkeer kunnen worden ingesteld. Mocht één van de verbindingen naar een Internet Service Provider (ISP) niet beschikbaar zijn dan is er een automatische routering mogelijk naar een andere ISP of kan ervoor worden gekozen om het voice-verkeer te routeren naar de Telecom operator voor een routering over het vaste netwerk [PORT06].

IP Centrex en hosted IP telefonie diensten bieden de mogelijkheden van een on-site PBX systeem. Bij IP Centrex staat de telefooncentrale echter niet bij de organisatie zelf maar wordt deze extern gehost bij de Telecom operator en gedeeld met andere bedrijven.

Media servers

Bij een gebrek aan naamconventies in de VoIP wereld, wordt de term 'media server' gebruikt als een verzamelnaam voor alle servers die zich bezighouden met het opslaan en delen van diverse soorten digitale media zoals spraak, data en video [PORT06]. Media servers zijn grofweg te verdelen in twee groepen:

1. Servers voor het interactief verwerken van media zoals Interactieve Voice Response (IVR) servers.
2. Call control servers voor het afhandelen van communicatie resources in een VoIP netwerk. Gatekeepers, Registration servers en Redirect servers zijn voorbeelden van call control servers en worden verderop behandeld bij de H.323 / SIP architectuur.

Media gateway

Een media gateway is een netwerkcomponent voor het vertalen van protocollen tussen anders onverenigbare netwerken. Een voice gateway kan een rol vervullen in het verkeer van analoge - naar digitale (VoIP) netwerken en andersom. Een simpele uitvoering van een VoIP gateway is een Analog Telephone Adaptor (ATA). Dit is een apparaat om een analoge telefoon aan te sluiten op een VoIP netwerk en heeft doorgaans zowel een netwerk- als een telefoonaansluiting.

VoIP protocollen

VoIP protocollen kunnen worden ingedeeld naar hun rol in de transmissie van VoIP verkeer. H.323 en SIP zijn de belangrijkste protocollen voor **signalering** en zorgen voor het opzetten en verbreken van gesprekken. H.323 en SIP ondersteunen elk vergelijkbare opties maar zijn niet direct uitwisselbaar.

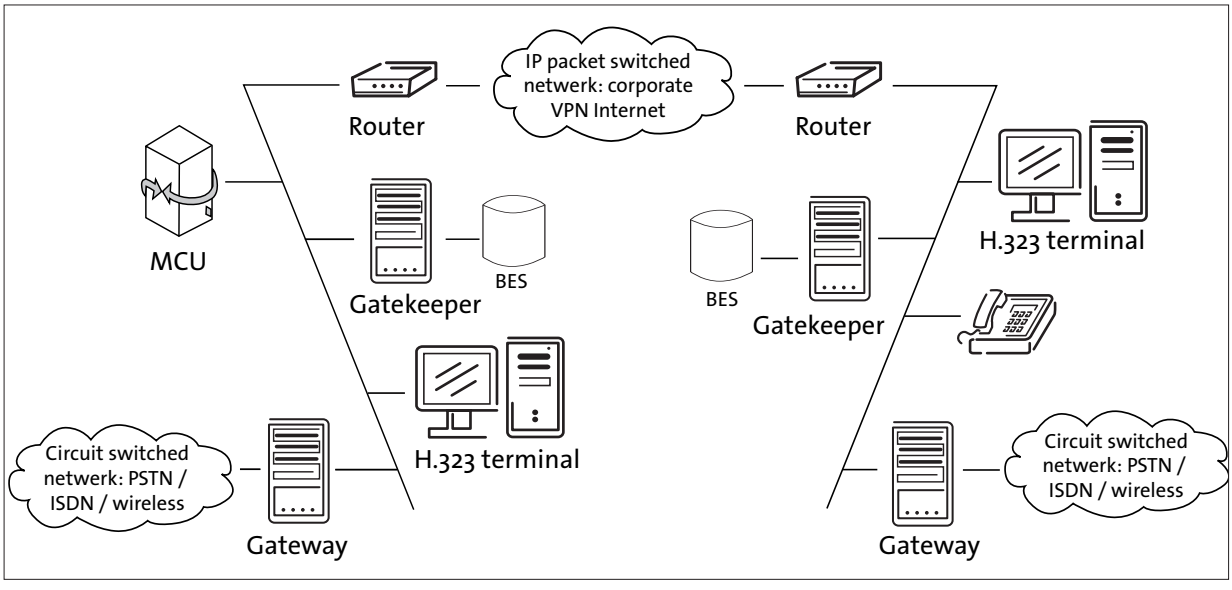
Voor het **transport** van spraak en multimediadata wordt hoofdzakelijk RTP (Real-Time Protocol) gebruikt. RTCP (Real-Time Control Protocol) en RTSP (Real-Time Streaming Protocol) worden gebruikt voor het **monitoren** van het transport van data en streaming media tussen deelnemers.
SDP (Session Description Protocol) wordt gebruikt om informatie over multimedia te versturen over het netwerk.

Daarnaast vereist het transport van VoIP een groot aantal **ondersteunende** protocollen onder andere ten behoeve van Quality of Service (RSVP), naamresolutie (DNS), firmware - en software upgrades (TFTP), tijd synchronisatie (NTP), routeren van gesprekken (TCP/IP) en het monitoren van performance (SNMP).

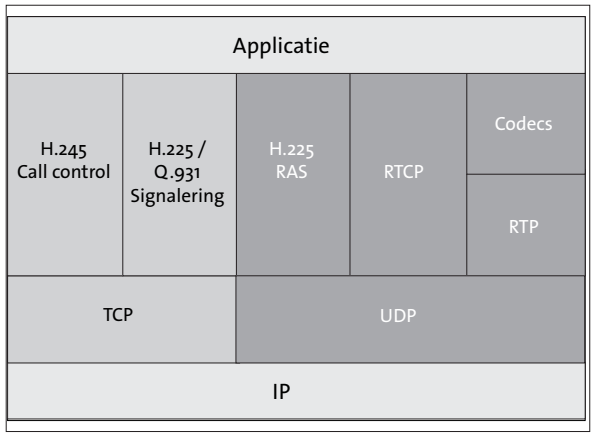
H.323 architectuur

H.323 is een door de ITU (International Telecommunication Union) gepubliceerde standaard voor multimediacommunicatie over IP datanetwerken.

Figuur 1: H.323 architectuur



Figuur 2: H.323 protocol stack



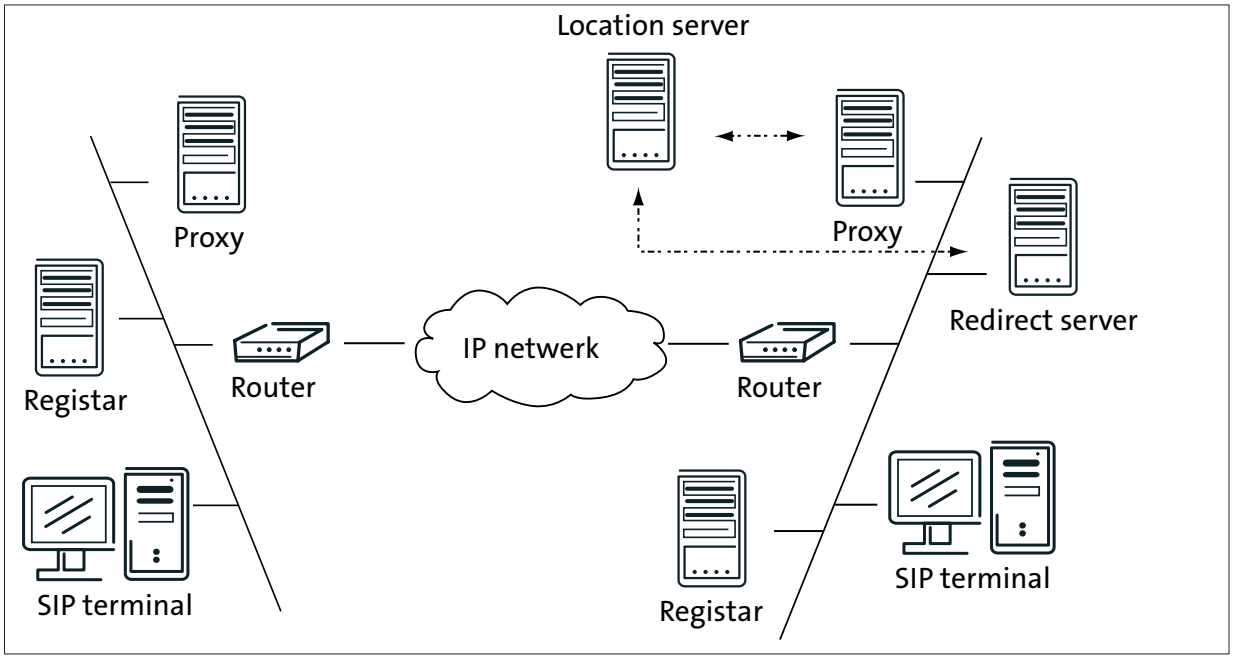
Figuur 1:
Gateways en Gatekeepers zijn optioneel in een H.323 architectuur. Gateways zorgen voor het transport van signalering - en media verkeer en verzorgen een brugfunctie naar andere netwerken zoals ISDN, PSTN of andere H.323 netwerken. Indien aanwezig, registreren Gateways zich bij een Gatekeeper. Gatekeepers zorgen voor registratie, adresvertaling en toegang tot VoIP terminals en gateways. Daarnaast kunnen Gatekeepers optreden als 'authoritive source' waardoor snel wijzigingen kunnen worden uitgerold over een netwerk. Verder worden Gatekeepers gebruikt voor het monitoren van performance en het beheren van bandbreedte in het netwerk. Een MCU (Multipoint Control Unit) ondersteunt allerlei vormen van communicatie tussen twee of meer eindstations. De BES (Back End Service) zorgt onder andere voor authenticatie, service autorisatie, accounting en billing. In een eenvoudig netwerk voorziet een Gateway of Gatekeeper in dergelijke services.

De H.323 standaard definieert een algemene set van protocollen ten behoeve van het opzetten van gesprekken en procedures voor onderhandeling.

Figuur 2 [PORT06]:
H.225.0 / Q.931: dit protocol beschrijft de standaarden ten behoeve van signalering voor het opbouwen, beheren en afbreken van gesprekken.
H.225.0 / RAS: dit gedeelte van het H.225 protocol specificeert RAS (Registration, Admission, Status) waarmee registratie, toegang en status met betrekking tot bandbreedte wordt geregeld tussen eindstations en Gatekeepers.
H.245: specificeert berichten ten behoeve van call control onder andere voor het onderhandelen van de terminal mogelijkheden en het communiceren van informatie over het te gebruiken kanaal.
Real Time Protocol (RTP): beschrijft het end-to-end transport van real-time data.
Real Time Control Protocol (RTCP): beschrijft de end-to-end monitoring van het data transport. De primaire functie van RTCP is het geven van feed-back op de kwaliteit van het data verkeer.
Codecs: G.700 series voor VoIP codecs waarmee analoge spraak wordt geconverteerd naar digitale data en vice versa, inclusief het (de)comprimeren van data voor een efficiënte transmissie.

De H.323 call flow is afhankelijk van de aanwezigheid van bepaalde entiteiten zoals Gateways en Gatekeepers. In geval van een directe communicatie tussen twee eindstations, worden er twee TCP kanalen opgezet, één voor call setup (H.225.0 / Q.931) en één voor onderhandeling en call control (H.245). H.225.0 / Q.931 call signalering berichten worden gebruikt voor het initiëren van verbindingen tussen H.323 eindstations. Deze berichten zorgen ervoor dat het gebelde eindstation gaat rinkelen. Vervolgens wordt een

Figuur 1: 3 SIP architectuur



tweede end-to-end kanaal opgezet waarover H.245 berichten worden uitgewisseld. Aan het eind van deze uitwisseling wordt het gesprek beantwoord door de ontvanger.

Met H.235 wordt een reeks van security profielen gedefinieerd waarmee verschillende beveiligingsniveaus kunnen worden gerealiseerd. Een H.235 security profiel bestaat uit definities, requirements en procedures en kan als module worden geïmplementeerd in elke gewenste combinatie. Het H.235 basis security profiel voorziet met behulp van passwordbeveiliging en hashing in authenticatie en bescherming van de integriteit van het H.225.0 / RAS en H.225.0 / Q.931 verkeer terwijl de H.245 berichten worden beschermd met password beveiliging. Dit basis security profiel beschermt onder andere tegen man-in-the-middle attacks, replay attacks, spoofing en connection hijacking maar weer niet tegen sniffing. Hiervoor heeft H.235 weer andere security profielen waarmee inbreuken op de vertrouwelijkheid kunnen worden voorkomen.
Kenmerkend voor H.235 is de focus op authenticatie, vertrouwelijkheid en integriteit van het VoIP verkeer. Denial of service wordt niet geadresseerd [PORT06].

SIP architectuur

SIP (Session Initiation Protocol) is een IETF (Internet Engineering Task Force) standaard die is beschreven in RFC 3261. Toepassingen zoals VoIP, Video Conferencing en Instant Messaging die gebruik maken van real-time communicatie tussen gebruikers kunnen SIP gebruiken voor het opzetten van een verbinding tussen twee of meer eindstations. De gebruikers van deze toepassingen zijn niet gebonden aan één locatie en kunnen verschillende computers, gebruikersnamen en accounts gebruiken. Daarom werkt SIP samen met netwerk componenten die zorgen voor registratie en routering zodat gebruikers kunnen worden geïdentificeerd en gelokaliseerd.

SIP is een signaleringsprotocol voor het opzetten en termineren van VoIP sessies. Zodra er een sessie tot stand gekomen is, nemen andere protocollen bepaalde taken over zoals het transport tussen eindstations en het onderhandelen over de uitwisseling van media [IETF02].

Een SIP-netwerk bestaat uit user agents en SIP servers. Hieronder worden enkele rollen beschreven die SIP servers kunnen aannemen in een VoIP netwerk.

User Agents

Elke deelnemer in een SIP sessie is een user agent. De user agent die het verzoek doet is de User Agent Client (UAC), de user agent die de service verleent is de User Agent Server (UAS). De user agent kan allerlei vormen aannemen, variërend van een IP phone, een applicatie, een PDA, tot een gateway naar het PSTN netwerk. In elk van deze hoedanigheden kan de user agent de rol vervullen van UAC en UAS.

SIP server: registratie service

Een user agent meldt zich aan bij een Registrar server met zijn gebruikersnaam en IP adres. Tevens wordt de huidige online status van de user agent doorgegeven. De Registrar server ontvangt de registratie verzoeken en koppelt het SIP adres aan de huidige gebruikerslocatie van de user agent. SIP adressering wordt verderop uitgelegd.

SIP server: proxy service

Een proxy server onderschept berichten van user agents,

inspecteert het 'To:' veld, maakt contact met de location server, vertaalt de username naar een IP-adres en stuurt het bericht naar de eindbestemming of naar een andere server. In deze rol kunnen ook additionele functies worden vervuld zoals network access control, authenticatie en autorisatie.

SIP server: redirect service
Een redirect server ontvangt het actuele adres van een bestemming van een location server en stuurt deze informatie naar de user agent waar het verzoek vandaan komt.

SIP server: location service
Een location server heeft een directory van alle user agents die op dat moment zijn ingelogd met hun gebruikersnaam, IP adres, SIP adres en huidige status. Location servers verstrekken informatie over de mogelijke locaties van een beller aan redirect en proxy servers.

Voordat twee user agents met elkaar kunnen communiceren, moet elke user agent zich registreren bij een Registrar server. Nadat het verzoek is gehonoreerd worden het SIP adres en het IP adres verstrekt aan de location server. Vervolgens kan het proces voor het opzetten van een VoIP sessie verlopen volgens een aantal stappen:

1. User agent A stuurt een SIP INVITE naar de proxy server met het verzoek om een sessie op te zetten met user agent B.
2. De proxy server doet een beroep op de location server voor het verstrekken van het IP adres van user agent B.
3. De SIP INVITE wordt doorgestuurd naar user agent B.
4. User agent B accepteert de SIP INVITE en koppelt dit terug naar de proxy server.
5. De proxy server geeft het antwoord van B door aan user agent A.

Nadat er een sessie tot stand is gekomen, verloopt de communicatie via het RTP protocol en kunnen A en B rechtstreeks met elkaar communiceren.

Bij Voice over IP is een beller niet gebonden aan een vaste plaats. Gebruikers met een onbekend IP adres kunnen inloggen op een Registrar server die dan vervolgens zorgt voor routering van het gesprek via de juiste gateways. Op deze manier kan een gebruiker één telefoonnummer gebruiken ongeacht zijn fysieke locatie.

Adressering
SIP maakt gebruik van Uniform Resource Identifiers (URI's) voor het identificeren van gebruikers. De syntax is vergelijkbaar met die van email adressen. De URI bestaat uit een domein gedeelte waar de gebruiker is gelokaliseerd en een deel dat het account weergeeft. Dit kan een gebruikersnaam of telefoonnummer zijn. Een voorbeeld van een SIP URI:
sip: will.franken@audiris.nl.
Een URI kan ook additionele informatie bevatten zoals poortnummers, passwords of andere parameters. Dit maakt bijvoorbeeld het verzenden van data over een veilige verbinding mogelijk. Een voorbeeld van een met TLS (Transport Layer Security)[6] beveiligde VoIP sessie:
Sips: 0611510863@216.24.1.106.

Kwetsbaarheden VoIP
Voice over IP is een relatief nieuwe technologie. Er is nog niet zo heel veel bekend over beveiligingsincidenten in VoIP netwerken maar dát we ermee zullen worden geconfronteerd is slechts een kwestie van tijd. De redenen hiervoor liggen voor de hand. Allereerst zijn alle beveiligingsproblemen met het IP protocol onverkort van kracht op VoIP toepassingen inclusief spoofing, sniffing, replay attacks en message integrity attacks. Daarnaast wordt er bij Voice over IP gebruik gemaakt van ondersteunende internet applicaties zoals DNS, SNMP en TFTP die elk hun inherente zwakheden bevatten. Verder kan worden gesteld dat VoIP netwerken, vanuit hun aard, zeer vatbaar zijn voor denial of service (DOS) aanvallen [NIST05]. Virussen en wormen zijn een belangrijke bedreiging voor de beschikbaarheid van de gehele VoIP infrastructuur. Daarbij kan worden aangetekend dat veel VoIP componenten zoals IP-PBXen en gateways zijn uitgevoerd op veelvuldig beproefde besturingselementen als Windows en Linux. Deze systemen worden vaak uitgeleverd met veel onnodige services geactiveerd. Deze extra services kunnen potentiële security risico's opleveren.

VoIP bedreigingen kunnen grofweg worden ingedeeld in 2 categorieën:

1. VoIP dienst verstoringen en
2. Call interceptie en - manipulatie.

VoIP systemen moeten voldoen aan hoge eisen ten aanzien van beschikbaarheid. (D)DOS aanvallen kunnen in potentie de gehele telecommunicatie van een organisatie platleggen. De gevolgen van call interceptie en - manipulatie zijn minder voorspelbaar maar kunnen eveneens veel schade toebrengen. Een voorbeeld met betrekking tot pharming laat zien waar een en ander toe kan leiden. Pharming maakt gebruik van zwakheden in het DNS systeem. Met behulp van DNS poisoning[7] kunnen VoIP gebruikers naar onbedoelde adressen worden geleid. Het is dan niet ondenkbaar dat een rekeninghouder die zijn bank belt (maar ergens anders uitkomt), wordt verleid tot het noemen van vertrouwelijke gegevens.

Ook SPIT (Spam over Internet Telephony) wordt algemeen gezien als een reëel gevaar. Een server is in staat om enkele honderden gesprekken gelijktijdig te voeren over een enkele internet verbinding. Het wordt dan mogelijk om volautomatisch een ingesproken boodschap naar honderden telefoonnummers te verzenden, tegen zeer beperkte kosten.

Hierna volgt een niet uitputtende opsomming van enkele specifieke bedreigingen ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van Voice over IP.

User agents
IP phones waaronder PDA's / handheld phones en eerste

generatie VoIP IP phones met bijvoorbeeld WinCE - of PalmOS besturingssystemen zijn kwetsbaar omdat ze geen antivirus bescherming bieden en een minder robuust besturingssysteem hebben. Daarnaast worden veel VoIP apparaten afgeleverd met een overdaad aan services en zijn via de open poorten vatbaar voor denial of service aanvallen, buffer overflows of authenticatie bypasses.
Voor het ophalen van configuratie gegevens wordt door VoIP apparaten nog al eens het onveilige TFTP protocol gebruikt. TFTP biedt geen mogelijkheden voor authenticatie en encryptie en is dus niet geschikt voor het ophalen van vertrouwelijke gegevens. Iedereen die zich toegang verschaft tot TFTP sessies is in staat om credentials te achterhalen.

Een generiek probleem met softphones is dat deze programma's worden geïnstalleerd op computers waarop ook andere applicaties actief zijn. Kwetsbaarheden in deze applicaties vormen dan een beveiligingsrisico voor VoIP toepassingen (overigens is het omgekeerde ook waar). Indien PC's zijn beveiligd met een firewall, moet voor de softphones een aantal hoge UDP poorten worden opengezet. Deze ruimte in de firewall ruleset is dan automatisch van negatieve invloed op alle overige applicaties die op de desktop zijn geïnstalleerd.
Andere problemen met softphones zijn vaak product specifiek. Zo worden in sommige softphones de credentials van de gebruiker onversleuteld opgeslagen in de Windows registry.

Netwerk

Voice verkeer op een pakket geschakeld datanetwerk is kwetsbaar voor afluisteren op basis van dezelfde technieken die worden gebruikt om ander verkeer te sniffen op een LAN of WAN. Eén van die technieken is ARP spoofing. ARP, het Address Resolution Protocol zorgt ervoor dat op basis van IP-adressen, de bijbehorende fysieke Ethernet-adressen gevonden kunnen worden. Manipulatie van ARP pakketten is een beproefde aanvalsmethode die zeker ook werkt op VoIP netwerken. ARP heeft enkele inherente zwakheden. Om te beginnen is het protocol niet in staat om ARP verzoeken en antwoorden te authenticeren. Verder, omdat ARP een stateless protocol is, zal een besturingsysteem zijn cache bijwerken bij ontvangst van een ARP reply ongeacht of er een verzoek is uitgestuurd. Dit laatste kan worden gebruikt voor ARP spoofing.

Een andere techniek is ARP redirecting waarbij een Man in the Middle aanval wordt opgezet. Hierbij wordt alle IP verkeer inclusief spraak, email, passwords en PIN codes langs de aanvaller geleid die zonder moeite met behulp van vrij verkrijgbare tools dit verkeer kan afluisteren.

Een SIP specifieke bedreiging is Registration Hijacking. Bij Registration Hijacking doet een aanvaller zich voor als een geldige user agent, meldt zich bij een Registrar en vervangt de registratie met zijn eigen adres. Vervolgens komen alle inkomende gesprekken uit bij de aanvaller.

Denial of service aanvallen in een VoIP netwerk hebben mogelijk uitval of degradatie van de service tot gevolg. Enkele voorbeelden zijn:
- Quality of Service Modification;
- VoIP Protocol Implementation.

Bij Quality of Service Modification worden QoS gerelateerde velden in VoIP pakketten aangepast. Door bijvoorbeeld het aanpassen van de Type of Service bits in het IP pakket kan de prioriteit voor voice verkeer worden verlaagd naar die voor data verkeer waarmee de Quality of Service van een VoIP netwerk sterk negatief wordt beïnvloed. VoIP Protocol Implementation is een denial of service aanval waarbij grote aantallen QoS gerelateerde pakketten worden verstuurd naar VoIP servers of eindstations.

Beveiliging van Voice over IP

Belangrijke preventieve maatregelen voor het beveiligen van VoIP netwerken zijn:
- het 'hardenen' van alle componenten in de VoIP infrastructuur;
- toepassen van encryptie;
- maatregelen voor het identificeren en authenticeren van gebruikers en apparaten;
- toepassen van perimeter security;
- het waarborgen van de Quality of Service en
- het logisch scheiden van spraak en data verkeer.

Hieronder wordt kort stil gestaan bij elk van deze maatregelen. Het actief monitoren van VoIP netwerken is een voorbeeld van een detectieve maatregel. Daarnaast kan met behulp van penetratietesten en vulnerability scans de sterkte van de bestaande security controls worden beoordeeld. Naast de bovengenoemde generieke maatregelen zijn er natuurlijk ook tal van specifieke oplossingen die in dit artikel verder buiten beschouwing zullen blijven, vanwege de grote diversiteit daarvan.

Hardening

VoIP apparaten worden vaak uitgeleverd met een overdaad aan opties. Het toepassen van hardening en andere door leveranciers meegeleverde security instructies zijn belangrijke stappen voor de beveiliging van het VoIP netwerk.

Encryptie

Risico's met betrekking tot het onderscheppen van VoIP verkeer en inbreuken op de integriteit van dit verkeer kunnen worden voorkomen door het toepassen van encryptie. Interceptie is dan nog wel mogelijk maar is van geen waarde voor de aanvaller. Vertrouwelijkheid en integriteit kunnen op verschillende manieren worden geregeld. VoIP verkeer kan versleuteld worden verzonden tussen eindstations of worden getunneld over een Virtual Private Network (VPN) en met behulp van hashing kan de integriteit worden gewaarborgd. Meer concreet gelden TLS en S/MIME[8] als standaard oplossingen voor de beveiliging van het signaleringsverkeer.

Identificatie en authenticatie

Voor het beveiligen van VoIP netwerken dienen de identiteiten te worden geverifieerd van zowel gebruikers als de apparaten die deel uitmaken van het netwerk. Dit kan op een aantal manieren worden gerealiseerd, op laag 2 van het OSI model onder andere met 802.1x/EAP of een PKI infrastructuur. Het 802.1x protocol dwingt af dat clients zich eerst authenticeren, meestal bij een RADIUS server, alvorens zij toegang krijgen tot een LAN. EAP (Extensible Authentication Protocol) is een algemeen protocol dat voorziet in meerdere authenticatie methodes, inclusief traditionele passwords, token cards, Kerberos, digitale certificaten, en public-key authentication. Op laag 2 kan ook worden gedacht aan port security waarmee het gebruik van een switch port kan worden gekoppeld aan een specifiek MAC adres of aan een bepaalde range van MAC adressen.
In een SIP architectuur kan op de hogere lagen van het OSI model gebruik worden gemaakt van HTTP Digest Authentication om eindstations te authenticeren.

Perimeter beveiliging

Firewalls kunnen moeilijk omgaan met VoIP onder andere omdat voice conversaties kunnen worden geïnitieerd van buiten de firewall waarbij er ook nog eens sprake is van een dynamische poorttoewijzing vanuit het signaleringsproces. Dit geeft problemen bij firewalls met stateful inspection en Application Layer Gateways omdat zij sessies die worden geïnitieerd van buiten uit, niet toestaan. 'VoIP-aware' firewalls met opties voor een real-time monitoring van gesprekken, kunnen hier mogelijk een oplossing bieden.

Naast firewall beveiliging speelt ook Network Address Translation (NAT) een belangrijke rol bij perimeter beveiliging. Echter, bij toepassing van encryptie, heeft NAT problemen met het herberekenen van checksums omdat de signaleringsinformatie die wordt opgenomen in de payload van het IP datagram dan niet meer beschikbaar is.

Quality of Service

Zonder extra maatregelen werken data netwerken op een best-effort basis voor het prompt afleveren van verkeer. Echter, als alle verkeersoorten gelijke prioriteiten hebben, zijn in geval van netwerk congestie ook de kansen op vertragingen gelijk. Voor Voice over IP is dit niet acceptabel en daarom wordt voor het garanderen van de kwaliteit een aantal technieken ingezet. Met behulp van Quality of Service (QoS) en traffic shaping wordt getracht kwaliteitsverlies als gevolg van latency[9], jitter[10] en pakket verlies zoveel mogelijk op te vangen. QoS kan bescherming bieden bij een denial of service aanval door voice verkeer een veel hogere prioriteit te geven ten opzichte van het overige verkeer. Traffic shaping kan dit doen door middel van het optimaliseren van performance en bandbreedte. Daar staat tegenover dat bepaalde beveiligingsmaatregelen zoals firewalls, NAT, Access Control Lists (ACL) en encryptie/decryptie juist weer latency in de hand werken.

Logische scheiding in netwerken

De beschikbaarheid van VoIP kan worden verhoogd door een logische compartimentering van het netwerk en het logisch scheiden van VoIP - en data verkeer. Het logisch scheiden van spraak en data verkeer via VLANs is gewenst ter bescherming van VoIP verkeer tegen broadcast collisions en tegen problemen die zijn oorsprong vinden in het data netwerk. Softphones kunnen het principe van het logisch scheiden van spraak en data netwerken doorbreken omdat een op een PC geïnstalleerde softphone meestal in beide domeinen voorkomt.

Tot slot

Organisaties verschuiven in toenemende mate hun applicaties (en daarmee de beveiliging) naar de rand van hun netwerk waar zij kunnen communiceren met klanten en business partners in een dynamische internet omgeving (overigens zorgen intranets, extranets, VPN's en andere Remote Access Services ervoor dat de rand van het netwerk steeds moeilijker te definiëren is). Voice over IP versterkt deze ontwikkelingen alleen maar en omdat met de diversiteit van VoIP toepassingen er ook steeds meer network access points bij komen waardoor de netwerkcomplexiteit toeneemt, kan met recht worden gezegd dat Voice over IP een extra dimensie toevoegt aan het beveiligen van netwerken. ■

Literatuur

[NIST05] Special Publication 800-58 Security Considerations for Voice Over IP Systems

[PORT06] Practical VoIP Security

[IETF02] RFC 3261 – SIP: Session Initiation Protocol

www.voipsa.com

www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy (actueel overzicht van bedreigingen)

www.cve.mitre.org (Common Vulnerabilities and Exposures overzicht)

Noten

1 Traffic shaping is een mechanisme voor het beheren van netwerkverkeer met als doel performance optimalisatie en garanderen van bandbreedte.
2 DiffServ gebruikt het IP Type Of Service veld voor Quality of Service requirements.
3 RSVP is het Resource Reservation Protocol waarmee clients op een netwerk kunnen onderhandelen over bandbreedte.
4 Converged network: netwerk technologiën die in toenemende mate naar elkaar toegroeien.
5 OCS 2007 verbindt telefonie, email, video-conferencing en instant messaging met elkaar. De gebruiker krijgt toegang tot deze functionaliteit met communicator software die ook op mobile devices kan worden gebruikt.
6 TLS (Transport Layer Security) is een op SSL (Secure Socket Layer) gebaseerd encryptieprotocol dat zorgt voor een veilige verbinding tussen 2 computers.
7 DNS poisoning is een techniek waarbij een DNS server wordt voorzien van foutieve informatie voor de vertaling van domeinnamen naar IP adressen. Het effect is dat gebruikers naar een onbedoeld IP adres wordt geleid.
8 S/MIME (Secure/Multipurpose Internet Mail Extensions) is een protocol dat een aantal cryptografische security functies biedt ten behoeve van het electronisch berichtenverkeer zoals authenticatie, integriteit, non-repudiation en vertrouwelijkheid.
9 Latency is de hoeveel tijd die nodig is om pakketten van bron naar bestemming te brengen.
10 Jitter is een ongewenste variatie van één of meer telecommunicatie karakteristieken zoals amplitude of frequentie.