



HoGent

Faculteit Bedrijf en Organisatie

Wat is VOIP, hoe beveilig ik mijn netwerk hiervoor en hoe werkt het met IPV6

Ritchie Van Mele

Scriptie voorgedragen tot het bekomen van de graad van
Bachelor in de toegepaste informatica

Promotor:
Johan Decorte
Co-promotor:
Krist Vanneste

Instelling: Hogeschool Gent

Academiejaar: 2014-2015

Tweede examenperiode

Faculteit Bedrijf en Organisatie

Wat is VOIP, hoe beveilig ik mijn netwerk hiervoor en hoe werkt het met IPV6

Ritchie Van Mele

Scriptie voorgedragen tot het bekomen van de graad van
Bachelor in de toegepaste informatica

Promotor:
Johan Decorte
Co-promotor:
Krist Vanneste

Instelling: Hogeschool Gent

Academiejaar: 2014-2015

Tweede examenperiode

Samenvatting

Deze bachelorproef draait rond voice over IP (VOIP). In deze proef stel ik mezelf vragen en tracht daarop antwoorden te vinden. Ik ga trachten duidelijk te maken wat VOIP is en hoe ze verschilt van traditionele telefonie. Bij VOIP wordt de telefonie over een netwerk gestuurd. Ik ga dan ook onderzoeken welke invloed VOIP heeft op dit netwerk en of dit een probleem geeft voor je beveiliging. Beveiliging zowel t.o.v. het bestaande netwerk maar ook ten opzichte van je telefonie. Dan ga ik ook kijken naar op welke manieren je een onbeveiligd VOIP netwerk kan misbruiken en hoe je te beschermen tegen deze praktijken. De bedoeling is dat je na het lezen van deze proef weet wat VOIP is met alle voor en nadelen. Hoe het veilig en onveilig is en hoe je te beschermen tegen inbreuken. Deze proef sluit aan bij mijn stage bij SmartTelecom NV. Hier implementeer en beheer VOIP in nieuwe en bestaande netwerken bij klanten. Op deze manier kom ik dagelijks in contact met de voor en nadelen van VOIP. Alsook met de gevaren ervan en hoe te beveiligen tegen deze gevaren. Research via deze stage is dan ook mijn voornaamste aanpak van de probleemstelling.

Voorwoord

Deze thesis is in het kader van mijn bachelorproef voor toegepaste informatica aan de hogeschool Gent.

Ik wil mijn stagementor en copromotor Krist Vanneste van SmartTelecom NV bedanken voor de hulp en research mogelijk door hem.

Ook bedank ik mijn stage partner Dries Vandooren voor de nuttige invloed tijdens de stage en in het onderwerp VOIP.]

Inhoudsopgave

1	Inleiding	4
1.1	Probleemstelling en Onderzoeksvragen	7
1.1.1	Samenwerking met andere Technologieën	7
1.1.2	Beveiligingsdreigingen	7
1.1.3	VOIP met IPV6	8
2	Methodologie	9
3	Corpus	10
4	Conclusie	11

Hoofdstuk 1

Inleiding

Wat is VOIP? VOIP of Voice Over IP(Internet Protocol) is de technologie waar je telefonie en multimedia sessies(conference call met beeld) gaat sturen over een IP netwerk. Men verwijst vaak naar VOIP als internet telefonie. Hierbij ga je je communicatie(stem, sms, fax, ...) sturen over het internet in tegenstelling tot bij traditionele telefonie waarbij dit via een public telefonie netwerk gebeurde. In tegenstelling tot wat de naam zegt is internet verbinding niet altijd nodig bij VOIP. VOIP betekend eenvoudig dat je je communicatie gaat versturen via dezelfde protocollen als degene het internet gebruikt. Zo kan je binnen een groot bedrijf elke werknemer voorzien van VOIP telefoons en deze kunnen elkaar bellen via VOIP zonder dat ze verbinding maken met het internet. Eens ze willen bellen naar locaties buiten hun netwerk dan komt er uiteraard internet aan te pas.

Maar we lopen vooruit op de feiten. We starten met telefonie waar het allemaal bij startte. De eerste telefoons. De eerste telefoonlijn was een directe lijn tussen 2 toestellen. Eens er meer en meer toestellen kwamen maakte men gebruik van POTS wat staat voor "Plain Old Telephone Service". Vertaalt is dit "de eenvoudig oude telefoon service". POTS ging over een netwerk genaamd PSTN("public switched telephone network" of " publiek verdeeld telefoon netwerk"). Bij directe verbindingen tussen toestellen was er sprake van een analoog signaal tussen de 2. De stem werd op deze manier overgebracht. POTS en PSTN werden mogelijk toen de ontdekking werd gemaakt dat men dit analoog signaal kon omvormen naar een digitaal signaal. Een stem die in origine analoog was kon worden omgevormd naar een digitaal signaal en kon worden verstuurd als nullen en eentjes. Een betere technologie was ontwikkeld en de basis voor wat later zou uitgroeien tot VOIP was gelegd.

Tot op dat moment werd er gekozen om de telefonie gescheiden te houden van het opkomende computernetwerk. In computernetwerken werd er gewerkt met pakketten. Om VOIP gebruik te laten maken van deze netwerken zou het ook zo gaan werken.

VOIP gaat de geluidssignalen opsplitsen in pakketten en deze versturen over het netwerk. Deze pakketten bevatten behalve het geluid signaal ook het netwerk adres van de beller en ontvanger. En door het gebruik van pakketten werd het mogelijk om meer informatie mee te sturen om de communicatie te ondersteunen en verbeteren.

Waar POTS specifieke benodigdheden had is VOIP enorm veelzijdig. Het werkt op verscheidene soorten netwerken. En het werkt niet alleen met VOIP telefoons maar ook met computers, Pda's en zelf smartphones. Deze toestellen bevatten allemaal een NIC(Network Interface Card) net zoals een computer. Via deze NIC's krijgen de toestellen dan een netwerk adres(IP-adres). Op deze manier zijn VOIP toestellen deel van je computer netwerk.

Wat zijn nu de voor en nadelen van POTS en VOIP.

POTS:

- voordelen
 - Het is in vele gevallen al aanwezig.
- nadelen
 - Het aantal main telefoonlijnen is het aantal oproepen je bedrijf tegelijk aankan.
 - Het aantal extenties je kan hebben is bepaald door je PBX(private branch exchange)
 - Het werkt enkel met analoge telefoons. Geen pc's, smartphones, ...

VOIP:

- voordelen
 - Ongelimiteerd aantal oproepen dat je tegelijk kan afhandelen(als je internet snel genoeg is)
 - Ongelimiteerd aantal extenties.
 - Bied meer aan dan enkel telefonie zoals Video calls,bellen vanop PC's, ...
 - Geen gescheiden netwerk voor telefonie(geen dubbele bekabeling)
- nadelen
 - Er is een investeringskost bij aankoop van toestellen en PBX

Het is dus zeer duidelijk dat de overstap maken naar VOIP een zeer goede stap is voor bedrijven. Het geeft hen meer opties en de voordelen wegen meer door dan de nadelen.

Eens een bedrijf de stap maakt naar een Voice over Internet Protocol systeem is er nog een beslissing die te nemen is. Kies je voor een hosted Voip of voor een niet hosted voip. In de voorgaande analyse ging ik er van uit dat alle apparatuur zich on site bevond. Dit wil zeggen dat alle apparatuur zoals telefoons en PBX zich op de locatie van het bedrijf bevinden. Dit is niet de eenige mogelijkheid. Je kan er ook voor kiezen om je PBX te laten hosten door een hosting bedrijf. Hierbij zullen je VOIP telefoons geen verbinding maken met een PBX binnen je netwerk. Maar met een PBX centrale die zich op het internet bij een bedrijf die de diensten van hun PBX aanbied. Op deze manier kan je als bedrijf kosten sparen door de aankoop van een eigen PBX systeem te vervangen door een maandelijkse hosting kost. De voordelen van een hosted VOIP zijn dat je geen grote aankoopkost hebt, alsook dat je geen onderhoudskosten hebt. Ook kan je hierbij je VOIP telefoon toestellen plaatsen waar je wil. Je kan je toestel na het werk meenemen naar huis en daar bereikbaar zijn op het nummer van op werk. Bij een beheren van je eigen PBX is er een investering in materiaal, maar dit geeft je de mogelijkheid je VOIP netwerk te beheren zoals jij dat wil. In theorie zou je verbindingen kunnen open stellen waarbij je je toestel ook zou kunnen thuis zetten. Dit wordt wel afgeraden omdat dit je netwerk minder veilig maakt. Meer informatie later in deze thesis.

1.1 Probleemstelling en Onderzoeksvragen

VOIP is een nieuwe technologie, en een nieuwe technologie toevoegen aan je netwerk levert mogelijk problemen op. Je kan problemen hebben in samenwerking met andere gebruikte technologieën of je kan beveiligingsproblemen hebben. De probleemstelling is dan ook duidelijk. Wat is de impact van de implementatie van VOIP op een netwerk? Ook is er de opkomende IPV6 technologie. Hoe gaat VOIP samenwerken hiermee.

- Zijn er problemen in samenwerking met andere technologieën?
- Wat zijn de beveiligingsdreigingen van VOIP?
- Hoe werkt VOIP met IPV6?

1.1.1 Samenwerking met andere Technologieën

Kan VOIP ervoor zorgen dat de werking van je netwerk in het gedrang komt? Dan denk ik niet aan inbreuken via de VOIP maar eerder of de benodigdheden voor VOIP en de netwerklast die dit veroorzaakt problemen geeft voor de andere zaken die gebruik maken van het netwerk.

1.1.2 Beveiligingsdreigingen

Hier ga ik opsommen wat de voornaamste dreigingen zijn op het gebied van beveiliging van VOIP systemen.

Met behulp van packet sniffing software kan je de packetten van VOIP bekijken. Dit geeft je informatie over welk nummer op welk IP-adress belt naar welk nummer. Deze informatie kan misbruikt worden. Door middel van bijvoorbeeld VOMIT, voice over misconfigured internet telephones, kan je de datastream van VOIP gesprekken omzetten naar een beluisterbaar formaat. Op deze manier kan je gesprek letterlijk worden afgeluisterd. Alle gevoelige informatie is dan dus niet meer veilig.

Zoals vroeger met traditionele telefonie is er bij VOIP ook altijd belang naar het verkrijgen van gratis telefonie. Men noemt dit phreaking. Hierbij gaat een fout individu trachten toegang te krijgen tot je VOIP netwerk. Op deze manier gaat deze persoon dan kunnen bellen op kosten van de eigenaar. Hij gaat dit trachten te doen door de authenticatiegegevens van een VOIP gebruiker te verkrijgen.

Indien je je netwerk veiliger maakte met de implementatie van een aparte vlan voor je VOIP telefonie is er de kans dat een individu gaat trachten toegang te krijgen tot je telefonie vlan door middel van VLAN hopping.

Er zou iemand kunnen proberen om de gesprekken te verstoren. Dit is mogelijk door geluid pakketten te injecteren in de communicatie stream. Op deze manier kan de kwaliteit van een gesprek enorm verminderen, de twee sprekers kunnen zelf voor langere periodes stilte horen.

VOIP telefoons zijn zoals computers ook toestellen op je netwerk. Dit laat hen kwetsbaar voor een DOS aanval. Op deze manier kan iemand de telefoon spammen met onnodig veel SIP calls. Hierdoor wordt het toestel overbelast en kan het niet meer bellen of gebelt worden.

Waar traditionele telefoons een nummer hebben hebben VOIP telefoons een IP address. Traditionele telefoons krijgen soms reclame oproepen. Bij VOIP oproepen is het mogelijk om via scripts naar enorme hoeveelheden IP adressen reclame boodschappen te sturen. Degene toe terecht komen bij toestellen zouden voor de zender voordelig zijn maar niet voor de eigenaar van dat toestel. Deze manier van reclame spamming noemt SPIT(Spamming over Internet Telephony).

1.1.3 VOIP met IPV6

Nu het duidelijk is dat we op het internet met een enorm tekort zitten aan publieke IP adressen is het dan ook geen verrassing dat er een nieuw internet protocol aankomt. Dit nieuwe protocol komt in de vorm van IPv6(Internet Protocol Versie 6). Elke overstap naar een nieuw protocol, van welke aard dan ook, brengt veranderingen met zich mee. Het zorgt voor vernieuwing maar het zorgt er ook voor dat je als gebruiker je netwerkinfrastructuur moet aanpassen zodat het met dit nieuwe protocol kan werken. Het is dan ook logisch dat we ons moeten afvragen wat de impact zal zijn van IPv6 op ons netwerk. En in het bijzonder de invloed op VOIP binnen ons netwerk? In dit deel zal ik onderzoeken wat de voordelen zijn voor VOIP en hoe we ons zullen moeten aanpassen om VOIP te laten werken met IPv6.

Hoofdstuk 2

Methodologie

Hoofdstuk 3

Corpus

Hoofdstuk 4

Conclusie

Bibliografie

Creeger, M. (2009). CTO Roundtable: Cloud Computing. *Communications of the ACM*, 52(8):50–56.

Knuth, D. E. (1998). *The art of computer programming, volume 3: (2nd ed.) sorting and searching*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA.

Pollefliet, L. (2011). *Schrijven van verslag tot eindwerk: do's en don'ts*. Academia Press, Gent.

Lijst van figuren

Lijst van tabellen