NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET
FAKULTET FOR INFORMASJONSTEKNOLOGI, MATEMATIKK OG ELEKTROTEKNIKK

PROSJEKTOPPGAVE

Kandidatens navn:	David Kristensveen
Emne:	TTM4705 - Informasjonssikkerhet, fordypningsemne.
Oppgavens tittel:	**Sikkerhetsutfordringer ved IP-telefoni**

Oppgavens tekst:

Oppgaven skal gi en oversikt over hvilke angrep og trusler som rettes mot et IP-telefonisystem og dets tilhørende komponenter. Det skal også gjøres rede for ulike tiltak og virkemidler som benyttes for å møte disse sikkerhetsutfordringene.

I tillegg skal oppgaven belyse hva slags problemstillinger tilbydere og myndigheter står overfor før IP-telefoni kan regnes som en fullverdig arvtager etter «vanlig» fasttelefoni.

Det vil i hovedsak settes fokus på IP-telefoni som er tilrettelagt for samtrafikk med de tradisjonelle telefonitjenestene.

Besvarelsen leveres innen:	2. desember 2005
Besvarelsen levert:	
Utført ved:	Institutt for telematikk
Veileder:	Martin Gilje Jaatun, SINTEF IKT

Trondheim, 30.september 2005

Svein Johan Knapskog
Professor

Forord

Dette prosjektet har vært utført høsten 2005 ved Norges teknisk-naturvitenskaplige universitet (NTNU), Institutt for telematikk.

Jeg vil først og fremst takke Martin Gilje Jaatun ved SINTEF for mange nyttige innspill og tilbakemeldinger. Videre vil jeg også takke faglærer Svein Johan Knapskog for hjelp til oppgaveformulering og igangsettelse av oppgaven.

Trondheim, desember 2005

David Kristensveen

Innholdsfortegnelse

FORORD ..... **III**

INNHOLDSFORTEGNELSE ..... **V**

FIGURLISTE ..... **VII**

TABELLISTE ..... **VIII**

FORKORTELSER ..... **IX**

SAMMENDRAG ..... **X**

1 INNLEDNING **1**

1.1. BAKGRUNN 1
1.2. PROBLEMSTILLING 1
1.3. AVGRENSNINGER 2
1.4. OPPBYGNING 2

2 PROTOKOLLER **3**

2.1 SESSION INITIATION PROTOCOL (SIP) 4
2.2 H.323 8
2.3 MEDIA GATEWAY PROTOCOL (MGCP) 10

3 SIKKERHETSUTFORDRINGER **11**

3.1 SNIFFING 11
3.2 TJENESTENEKTINGSANGREP (DOS ATTACKS) 13
3.3 OPPDATERING AV SIP REGISTERSERVER 15
3.4 FALSK BRUKERREGISTRERING (”REGISTRATION HIJACKING”) 17
3.5 DHCP 18
3.6 TRUSLER I FORBINDELSE MED OPPSETT AV SESJONER 20
3.7 MOTTILTAK 22

4 SIKKERHETMEKANISMER I FORBINDELSE MED SIP **23**

4.1 SECURE MIME(S/MIME) 24
4.2 IPSEC 25
4.3 TRANSPORT LAYER SECURITY (TLS) 30

5 SIKKERHETSMEKANISMER I FORBINDELSE MED H.323 ..... **31**

5.1 H.235 VERSJON 2 32
5.2 H.235 VERSJON 3 33

6 GENERELLE SIKKERHETSTILTAK **34**

6.1 SKILLE MELLOM DATA- OG TALETRAFIKK 34
6.2 NETWORK INTRUSION DETECTIONS SYSTEMS (NIDS) 35
6.3 BRANNMURER 35
6.4 NETWORK ADDRESS TRANSLATION (NAT) 36
6.5 APPLICATION LEVEL GATEWAYS (ALG) 36
6.6 SAMARBEID MELLOM PROXYSERVER OG BRANNMUR 37
6.7 ESP I ”TUNNELMODUS” 37

7 SECURE REAL TIME PROTOCOL (SRTP) **38**

7.1 AUTENTISERING 38
7.2 KRYPTERING 38
7.3 MULTIMEDIA INTERNET KEYING(MIKEY) 40

8 INFORMASJON OM NORSKE TILBYDERE **42**

8.1 NØDANROP 42
8.2 KOMMUNIKASJONSKONTROLL 45
8.3 SIKKERHETSMESSIGE ASPEKTER 47

9 KONKLUSJON 49
10 REFERANSER 50

Figurliste

Figur 2-1 ”Oppsett av en SIP sesjon med bruk av proxyserver” 6
Figur 2-2 ”Oppsett av en SIP sesjon med bruk av Redirectserver” 7
Figur 2-3 ”H.323 nettverk sammenkoblet med et PSTN/ISDN nett” modifisert fra [2] 8
Figur 3-1 ”Bruker sender en ”SIP REGISTER” forespørsel til en SIP server ” modifisert fra [1] 15
Figur 3-2 ”Utdrag fra headerinnholdet i en ”SIP REGISTER” forespørsel” modifisert fra [1] 16
Figur 3-3 ”ARP spoofing angrep” fra [32] 19
Figur 3-4 ”SDP tilleggsfelter fra en SIP INVITE melding” modifisert fra [31] 20
Figur 4-1 ”Bruk av protokoller for overføring av signaler og tale innen SIP” modifisert fra [1] 23
Figur 4-2 ”Bruk av protokoller for sikker overføring signaler og tale innen SIP” modifisert fra [1] 24
Figur 4-3 ”Overhead i forbindelse med IPsec” 27
Figur 5-1 ”Oppsett av samtale ved bruk av H.323” modifisert fra [8] 31
Figur 7.1 ”SRTP Autentisering” modifisert fra [31] 38
Figur 7.2 ”SRTP Kryptering” modifisert fra [31] 39
Figur 7.3 ”Ulike bruksområder for MIKEY” modifisert fra [16] 40
Figur 7.4 ”Oppsett av MIKEY sikkerhetsprotokoll” 41
Figur 8.1 ”Kundeinformasjon fra Telenor sine hjemmesider” fra [20] 44

Tabelliste

Tabell 2-1 ”Standarder benyttet i forbindelse med bredbåndstelefoni” fra [29] **3**
Tabell 5-1 ”Sikkerhetsmekanismer i H.323v2 Annex F” modifisert fra [8] **32**
Tabell 5-2 ”Sikkerhetsmekanismer i H.323v2 Annex D” modifisert fra [8] **32**
Tabell 5-3 ”Sikkerhetsmekanismer i H.323v2 Annex G” modifisert fra [8] **33**
Tabell 8.1 ”Informasjon om nødanrop” basert på [23]-[27] **43**
Tabell 8.2 ”Informasjon om kommunikasjonskontroll” basert på [23]-[27] **45**
Tabell 8.3 ”Informasjon om sikkerhetsutfordringer” basert på [23]-[27] **47**

Forkortelser

- AH (Authentiaction Header): Benyttes i IPsec for å sørge for integritet og autentisering av IP-pakker
- ALG (Application Level Gateway): Programvare som benyttes sammen med brannmurer for å analysere trafikken på applikasjonsnivået.
- ARP (Adress Resolution Protocol): Benyttes for å mappe adresser mellom logiske IP-adresser og fysiske MAC-adresser
- DHCP (Dynamic Host Configuration Protocol): Sørger for å dynamisk allokere IP adresser til brukere av et LAN.
- DoS (Denial of Service): På norsk brukes ofte ordet tjenestenektingsangrep. Her forsøker en angriper å nekte legitime brukere i å få tilgang til en tjeneste eller informasjon.
- ESP (Encapsulating Security Payload Protocol): Benyttes i IPsec for å sørge konfidensialitet for IP-pakker
- E.164: Navnet på den internasjonale telefonnummerplanen administrert av ITU (International Telecommunication Union). Et fullt kvalifisert E.164-nummer inneholder en landkode, en by- eller områdekode pluss et telefonnummer. I Norge inngår by eller områdekoden i selve telefonnummeret.
- IKE (Internet Key Exchange): Mye benyttet rammeverk for nøkkeldistribusjon innenfor IPsec.
- ICMP (Internet Control Message Protocol): Tillegg til IP-protokollen. Benyttes for å sende feilmeldinger.
- IPsec (Internet Protocol Security): Sikkerhetsstandard som benyttes for å sikre trafikken på nettverkslaget.
- SDP (Session Description Protocol): Format for å utveklse parameter i forbindelse med oppsett av multimediasesjoner.
- SRTP (Secure Real Time Protcol): Rammeverk som tilbyr kryptering og autentisering av RTP/RTCP meldinger.
- MIKEY(Multimedia Internet Keying): rammeverk for nøkkelutveksling som er beskrevet i RFC3830 fra IETF
- MIME (Multipurpose Internet Media Extensions) : Protokoll som ble utviklet for bruk innen e-post som gjør det mulig å overføre flere typer data enn kun tekstbasert data. Eksempler på slike data kan være grafikk, lyd, video eller andre filtyper.
- NAT (Network Address Translation): Benyttes innenfor et lokalnett slik at enhetene som er på dette nettverket deler en felles IP-adresse ut mot omverdenen
- NIDS(Network Intrusion Detections Systems): Verktøy for direkte å identifisere ulike typer angrep
- RTP (Real Time Protocol): Standard som benyttes til transport av sanntidstrafikk.
- RTCP(Real Time Control Protocol): Benyttes for å analyser RTP-trafikken.

Sammendrag

Innen utgangen av 2006 er det ventet at IP-telefoni vil ha en markedsandel på mellom 20 og 25 prosent innen markedet for fasttelefoni. I den harde kampen om markedsandeler vil det være viktig for tilbyderne å bruke ressurser på å få et billig produkt raskt utpå markedet. I en slik sammenheng kan sikkerhet bli nedprioritert fordi dette ofte ikke er den viktigste faktoren for mange kunder. Det er derfor viktig å kartlegge hvilke sikkerhetsutfordringer tilbydere og myndigheter står ovenfor i forbindelse med IP-telefoni, og hvilke muligheter som finnes for å sikre IP-telefoni på en best mulig måte.

Tilbyderne av IP-telefoni i Norge baserer seg i hovedsak på to forskjellige standarder. Dette er Session Initation Protocol (SIP) fra Internet Engineering Taskforce (IETF) og H.323 rekommandasjonen fra International Telecommunications Union (ITU). Av disse er det SIP som er mest benyttet. Grunnen til dette skyldes i hovedsak at SIP er enklere å implementere og har billigere tilhørende komponenter enn H.323.

Sikkerhet i forbindelse med IP-telefoni handler både om sikkerhet under selve samtalen, og om sikkerhet i forbindelse med oppsett av sesjoner. Real Time Protocol (RTP) benyttes for å overføre tale. Kravet om sanntid gjør at remtransmisjon av talepakker ikke har noen hensikt, derfor må RTP benyttes i kombinasjon med User Datagram Protcol (UDP). Ved selve oppsettet av en samtale stilles det ikke så strenge krav til sanntid. Det gjør at her kan Transmission Control Protocol (TCP) benyttes isteden for UDP

Fordi IP-telefoni benytter seg av IP-teknologien vil mange angrep og trusler som har vært rettet mot tradisjonelle datanettverk også være en trussel for IP-telefoni. Eksempler på dette kan være utnyttelse av svakheter i nettverket, tjenestenektingsangrep eller sniffing. Innen IP-telefoni vil dette medføre blant annet redusert opptid for selve tjenesten og risiko for avlytting av samtaler. Andre typer angrep kan være mer spesifikke for IP-telefoni. Et eksempel på et slikt angrep er ”falsk brukerregistrering” der en angriper kan kapre identiteten til en gyldig bruker. Dårlig sikkerhet i forbindelse med oppsett av sesjoner kan også være en trussel, siden det her overføres sensitiv informasjon om både brukeradresser og i en del tilfeller også krypteringsnøkler.

SIP benytter seg i stor grad av eksterne sikkerhetsmekanismer som IPsec, S/MIME eller TLS for å beskytte signaleringstrafikken. For å beskytte taletrafikken er IPsec per i dag det mest brukte alternativet. I motsetning til SIP har H.323 en egen definert standard for sikkerhetsprofiler, denne standarden kalles H.235. Denne standarden finnes i 3 ulike versjoner og med en rekke tilegg. Her beskrives det hvilke algoritmer som støttes i forbindelse med autentisering, konfidensialitet og integritet. I tillegg beskrives det mekanismer for nøkkeldistribusjon. Både H.323 og SIP er fremover forventet å benytte seg av Secure Real Time Protocol (SRTP) og Multimedia Internet Keying (MIKEY) i en stadig større grad. SRTP er en protokoll som benyttes for å beskytte taletrafikken og MIKEY er et rammeverk for nøkkeldistribusjon.

I tillegg til sikkerhetsmekanismene som benyttes av SIP og H.323 er det også en del generelle sikkerhetstiltak som kan benyttes i forbindelse med IP-telefoni. Det bør blant annet tilstrebes å skille mellom data- og taletrafikk i størst mulig grad. Et slikt skille vil som oftest realiseres ved å benytte Virtuelle Lan (VLAN) kombinert med brannmurer som er i stand til å skille mellom data- og taletrafikk. Det vil ikke være mulig å ha et komplett skille mellom data- og taletrafikk da i en del tilfeller er nødvendig med kommunikasjon på tvers av disse nettverkene.

For å belyse situasjonen hos de norske tilbyderne er det i denne oppgaven tatt med et kapittel med utgangspunkt i en høring Post– og teletilsynet sendte ut i 2004. Her gir de ulike tilbyderne sine synspunkter på en del områder innen IP-telefoni. Områdene nødanrop, kommunikasjonskontroll og sikkerhetsmessige aspekter blir gjennomgått i denne oppgaven. Fra tilbyderne kan en registrere at det fortsatt ikke eksisterer gode løsninger for opprinnelsesmarkering hvis brukerne flytter med seg IP-telefonen rundt på forskjellige steder. Tilbyderne ser derimot ut til å etter hvert kunne tilby myndighetene avlytting av samtaler. Unntaket er hvis kundene selv tar initiativ til å kryptere sine samtaler, da vil avlytting bli svært vanskelig. En kan derfor konkludere med at IP-telefoni introduserer en del nye sikkerhetsutfordringer sammenlignet med fasttelefon, men at det er mulig å gi en god beskyttelse mot disse truslene hvis arbeidet med sikkerhet tas seriøst. Ellers gjenstår det fortsatt en del arbeid før myndigheter og tilbydere har på plass fullgode mekanismer for opprinnelsesmarkering i forbindelse med nødanrop og klare instrukser for hvordan avlytting av samtaler skal gjenomføres.

1 Innledning

1.1. Bakgrunn

IP-telefoni blir en stadig mer populær form for telefoni. Tall fra Post og –teletilsynet [28] viser at det i juli 2005 var registrert 109 000 IP-telefonikunder hos ulike norske tilbydere. Hvis den positive trenden fortsetter forventes det at antallet IP-telefoni kunder passerer 340 000 innen utgangen av 2006. IP-telefoni vil da ha en markedsandel på mellom 20 og 25 prosent innen "fasttelefoni" (ISDN/PSTN/IP-telefoni). Det er derfor en hard kamp mellom ulike tilbydere for å sikre seg en størst mulig del av den nye kundemassen. For å sikre seg markedsandeler er det viktig for tilbyderne å være tidlig ute med sine løsninger og samtidig ha et produkt som oppfattes som attraktivt av potensielle kunder.

Det hersker fortsatt en del usikkerhet i forhold til sikkerhetsmessige utfordringer og regulering av IP-telefoni, og de ulike tilbyderne har i stor grad selv vært ansvarlige å sette krav til sine egne tjenester. I en slik sammenheng vil det være naturlig at sikkerhetsmessige aspektet ved et produkt blir nedprioritert i forhold til lave priser og hurtig produktlansering.

1.2. Problemstilling

For å lage et IP-telefonisystem med en høy grad av sikkerhet er det viktig å vite hvilke angrep og trulser en skal beskytte seg imot. Et av målene for denne oppgaven har derfor vært å gi en oversikt over ulike trulser og angrep som kan rettes mot et IP-telefonisystem. Det gis også en oversikt over ulike former for IP-telefoni og hvilke metoder som tilbys for å sikre disse på en best mulig måte. Oppgaven omtaler også en del utfordringer Post- og teletilsynet ser for seg i forbindelse med IP-telefoni og hvilket syn norske tilbydere har på dette.

1.3. Avgrensninger

Oppgaven settes fokus på løsninger for fullverdig IP-telefoni. Slike løsninger omtales ofte som bredbåndstelefoni. Dette er løsinger som er tilrettelagt for alle-til-alle kommunikasjon og standard telefonnumre brukes for å sette opp forbindelser mellom brukerne. I resten av oppgaven vil derfor IP-telefoni i tillegg bli omtalt som bredbåndstelefoni eller Voice Over IP (VoIP). Oppgaven er ment å gi en overordnet oversikt over ulike sikkerhetsutfordringer i bredbåndstelefoni. Dette medfører at detaljnivået i beskrivelsen av ulike løsninger i størst mulig grad lagt på ett nivå som er relevant for tilhørende eksempler.

1.4. Oppbygning

Kapittel 2: Som et grunnlag for resten av oppgaven gis det her en oversikt over hvilke protokoller norske tilbydere har valgt å benytte seg av i sine implementasjoner av bredbåndstelefoni. Det vil også bli gjennomgått en del sentrale elementer i forbindelse med de ulike protokollene.
Kapittel 3: Her gjennomgås en del sikkerhetsutfordringer i forbindelse med bredbåndstelefoni.
Kapittel 4 og 5: Tar for seg hvilke sikkerhetsmekanismer som kan benyttes i sammenheng med de to mest brukte protokollene innefor bredbåndstelfoni, Session Initiation Protocol (SIP) fra Internet Engineering Taskforce (IETF) og H.323 rekommandasjonen fra International Telecommuncations Union (ITU).
Kapittel 6: Her beskrives en del ulike sikkerhetstiltak som kan benyttes for å gi best mulig sikkerhet i nettverk som skal benyttes til bredbåndstelefoni.
Kapittel 7: Inneholder en oversikt over Secure Real Time Protocol (SRTP). Dette er en forholdsvis ny protokoll som kan benyttes til å sikre taletrafikk. Kapittelet omtaler også rammeverket Multimedia Internet Keying (MIKEY) som kan benyttes for nøkkelutveksling i kombinasjon med SRTP.
Kapittel 8: Her gis det en oversikt over hvilke problemer norske tilbydere av bredbåndstelefoni ser for seg i forbindelse med nødanrop, kommuniksajonskontroll og sikkerhet.
Kapittel 9: Her gis det en konklusjon.
Kapittel 10: Inneholder en referanseliste.

2 Protokoller

Som et grunnlag for de neste kapitlene vil det her gis en gis en oversikt over ulike implementasjoner av bredbåndstelefoni. Det vil settes fokus på løsninger for fullverdig bredbåndstelefoni. Dette er løsinger som er tilrettelagt for alle-til-alle kommunikasjon og standard telefonnumre brukes for å sette opp forbindelse mellom brukerne.

I dag er det i hovedsak to former for implementasjon av bredbåndstelefoni. Den ene bygger på Session Initiation Protocol (SIP) fra Internet Engineering Taskforce (IETF) og den andre bygger på H.323 rekommandasjonen fra International Telecommuncations Union (ITU). I tillegg har vi Media Gateway Control Protocol som er en noe enklere standard enn SIP og H.323.

Våren 2005 utarbeidet Intech A.S en rapport om privatmarkedet for bredbåndstelefoni i Norge [29]. Rapporten tar for seg 11 ulike tilbydere og ble utarbeidet på oppdrag fra Post- og teletilsynet. Rapporten gir blant annet oversikt over bruk av standarder hos de ulike tilbyderne. Dette gir oss en pekepinn på hvordan de ulike tilbyderne har valgt å implementere sine løsninger.

Tabell 2-1 "Standarder benyttet i forbindelse med bredbåndstelefoni" fra [29]

Tilbyder	Standard
BKK	SIP
BlueCom	SIP
Briiz	SIP
IP24	Støtter H.323 og SIP, men baserer seg på SIP
LOS	SIP eller MGCP
Lyse	H.323, og etter hvert SIP og MGCP
NextGenTel	SIP for privatkunder, vurderer eventuelt MGCP i forbindelse med fremtidige bedriftsløsninger.
Sandefjord	H.323, og etter hvert SIP og MGCP
Telenor	SIP
TeleVoIP	SIP
Telio	SIP

Fra Figur 2-1 ser vi at implementasjoner med SIP, H.323 og MGCP også benyttes av norske tilbydere. Resten av dette kapittelet vil derfor gi en overordnet oversikt over disse tre ulike løsningene hvor hovedfokuset vil ligge på SIP.

Felles for de ulike løsningene for bredbåndstelefoni er at alle bruker Real Time Protocol (RTP) og User Datagram Protocol (UDP). Fordi det ikke har noen hensikt å benytte retransmisjon på talepakker som går tapt i nettverket benyttes UDP benyttes isteden for Transmission Control Protocol (TCP). UDP er en lettvektsprotokoll som ikke har egne mekanismer for sekvensnummerering eller tidsstempling, og IP-pakkene kan derfor ankomme mottakeren usynkronisert og i feil rekkefølge. For at talen skal spilles av for mottakeren må først disse pakkene settes i riktig rekkefølge og synkroniseres, UDP må derfor kombineres med Real Time Protocol(RTP). RTP vil bli nærmere omtalt i avsnitt 2.2.

2.1 Session Initiation Protocol (SIP)

SIP er en protokollstandard for signalering som ligger på applikasjonslaget. SIP brukes for å initiere, modifisere og terminere interaktive sesjoner.

Internet Engineering Task Force (IETF) ga ut den første SIP spesifikasjonen i 1999 (RFC 2543). I 2001 ble en ny SIP spesifikasjon utgitt (RFC 3261), og med denne var grunnlaget for SIP på plass. Allerede samme år begynte flere tilbydere å realisere SIP baserte tjenester innenfor områder som tale, video og spill. SIP er i dag sammen med H.323 den ledende signaleringsprotokollen for VoIP. Mye av SIP sin økende popularitet kan tilskrives enkel implementasjon og billige tilhørende komponenter.

SIP er en enkel ASCII basert protokoll som brukes for å etablere kommunikasjon mellom de ulike komponentene i et nettverk og for å sette opp en forbindelse mellom to eller flere endepunkter. SIP bygger på to velkjente protokoller Hyper Text Transfer Protocol (HTTP) som brukes av webapplikasjoner og Simple Mail Transfer Protocol (SMTP) som brukes til e-post. SIP har blant annet hentet elementer innen ”server-klient” arkitekturen fra HTTP og bruken av ulike headerfelter fra SMTP. Siden SIP som sagt bygger på HTTP og SMTP vil alle sikkerhetsmekanismene som kan brukes mot disse protokollene også kunne benyttes på SIP sesjoner.

For å representere adresser eller lokasjoner i Internett brukes en URL (Uniform resource locators). Denne betegnelsen brukes også om SIP adresser, men som regel brukes isteden betegnelsen URI (Uniform resource identificator) for å beskrive disse adressene. Bakgrunnen for at begrepet URI benyttes isteden for URL er at ved bruk av SIP vil en bruker kunne flytte seg rundt mellom ulike nett og dermed endre sin lokasjon.

En SIP adresse er bygd opp på samme måte som en e-post adresse med brukerID og et vertsnavn. BrukerID kan enten være et brukernavn eller en E.164 [1]adresse og vertsnavnet kan være et domenenavn eller en nettverksadresse. En SIP adresse kan derfor uttrykkes på ulike måter som for eksempel:

- sip:bruker@telio.no
- sip:73512253@telio.no

2.1.1 SIP sesjoner

Ved oppsett av SIP sesjoner benyttes to hovedkomponenter:

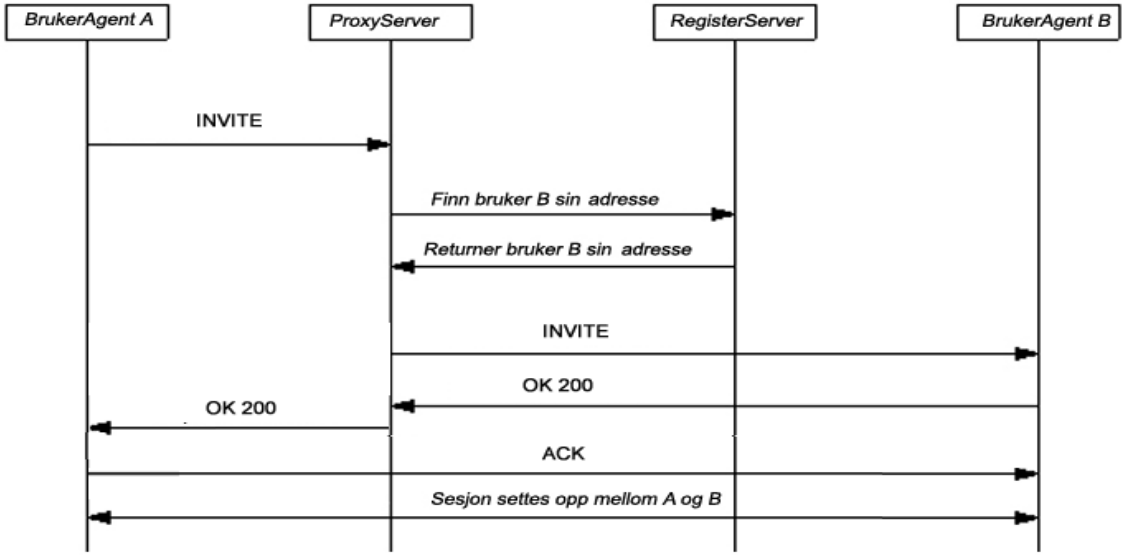
1) SIP Brukeragenter: Enheter som benyttes av brukerne i enden av en forbindelse. Brukeragentene tar imot input fra brukerne og oppfører seg som agenter på deres vegne. En brukeragent setter opp og kobler ned interaktive sesjoner med andre brukeragenter. Brukeragenter må være representert i begge ender av nettverket, for å representere brukere som ringer ut (klient) og brukere som blir oppringt (server)
2) SIP Servere: Her skiller vi mellom ulike typer servere:

[1] Post- og teletilsynet definerer E.164 slik: E.164 er navnet på den internasjonale telefonnummerplanen administrert av ITU (International Telecommunication Union). Et fullt kvalifisert E.164-nummer inneholder en landkode, en by- eller områdekode pluss et telefonnummer. I Norge inngår by eller områdekoden i selve telefonnummeret.

Proxyserver

En proxyserver tar imot forespørsler fra brukeragenten på om å etablere en sesjon med en annen brukeragent. Deretter forespørres en database om adresseinformasjon for brukeragenten som skal kontaktes. Denne databasen kalles ofte registerserver og inneholder lokasjonen til alle brukeragenter innenfor et domene.

Figur 2-1 "Oppsett av en SIP sesjon med bruk av proxyserver"

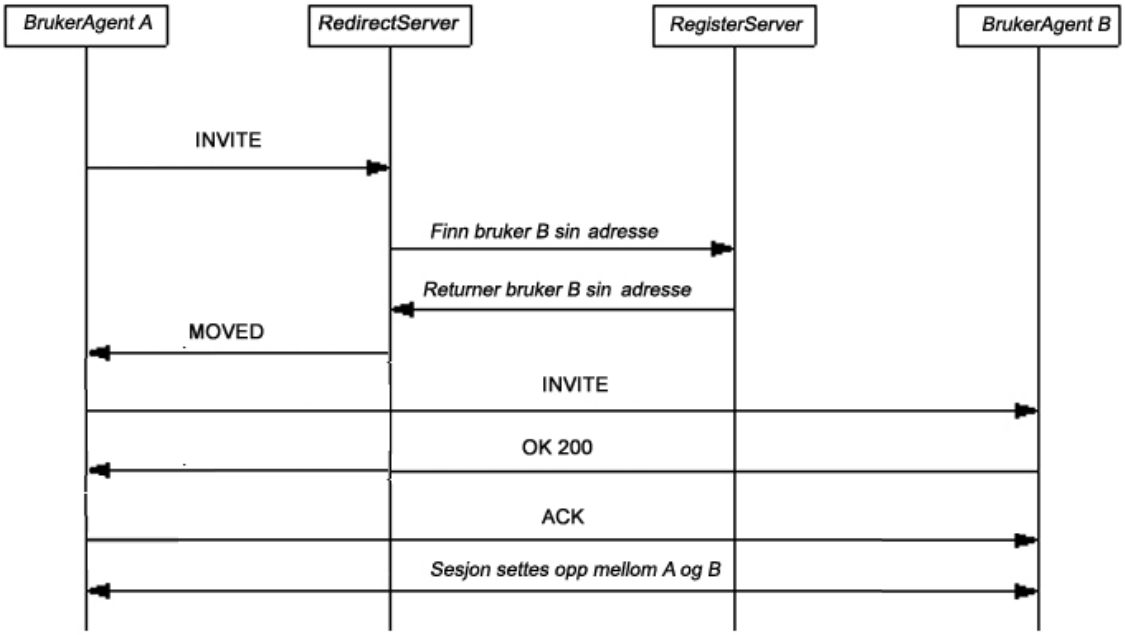


Når brukeragent A skal kontakte brukeragent B sendes det først en INVITE forespørsel til proxyserveren. Denne forespørselen inneholder informasjon om hvem og hvor det ringes fra og hvem som skal ringes opp. For at proxyserveren skal klare å videresende denne forespørselen er den avhengig av å vite brukeragent B sin IP-adresse, derfor må det gjøres et oppslag i registerserveren for å finne denne adressen. Når adressen er funnet kan proxyserveren videresende INVITE forespørselen til brukeragent B. Hvis brukeragent B godtar forespørselen svarer den proxyserveren med meldingen OK 200, denne meldingen videresendes så til brukeragent A. Brukeragent A svarer med en ACK melding for å godkjenne responsen og sesjonen mellom A og B kan så settes opp.

Redirectserver

Hvorvidt en SIP server skal fungere som en proxyserver eller en redirectserver kan bestemmes i konfigurasjon av serveren. Både proxy- og redirectservere benytter seg av registerserveren for å finne adressen til den oppringte brukeragenten. I motsetning til en proxyserver vil ikke en redirectserver videresende forespørsler på vegne av brukeragenten, men isteden sende lokasjonsinformasjonen tilbake til brukeragenten.

Figur 2-2 "Oppsett av en SIP sesjon med bruk av Redirectserver"



Her ser vi at brukeragenten får meldingen MOVED tilbake fra redirectserveren. Denne meldingen inneholder den midlertidige adressen til brukeragent B. Brukeragent A får selv ansvaret for å sende INVITE til meldingen brukeragent B.

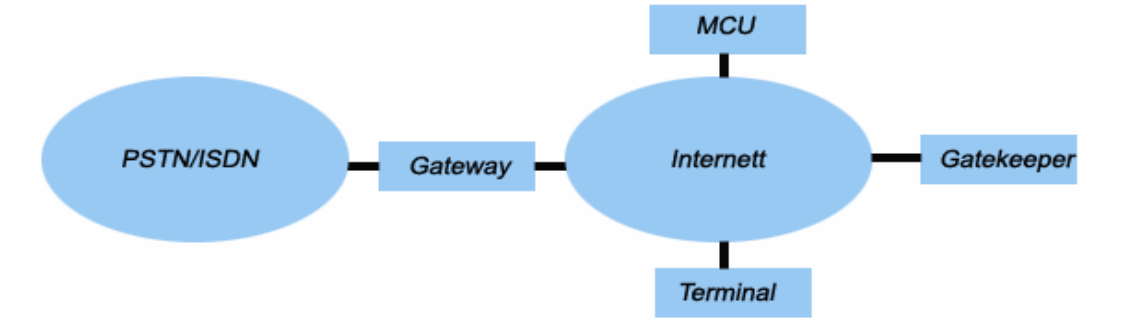
Registerserver

Database som inneholder lokasjonen til alle brukeragenter innenfor et domene. Disse serverne mottar og videresender brukeragentene sine IP-adresser og annen informasjon til proxy- og redirectserverene.

2.2 H.323

H.323 er en rekommandasjon definert av ITU-T. H.323 omtales ofte som paraply-rekommandasjon, det vil si at den omfatter flere ulike spesifikasjoner og er sammensatt av flere ulike protokoller. H.323 muliggjør sanntidskommunikasjon av lyd og bilde mellom ulike endesystemer over pakkebaserte nettverk.

Figur 2-3 "H.323 nettverk sammenkoblet med et PSTN/ISDN nett" modifisert fra [2]



H.323 benytter en gateway og tre typer endepunkter:

1) Gateway: Sørger for kommunikasjon mellom ulike nettverk som benytter seg av ulike protokoller. For å realisere dette må en gateway konvertere signaleringen og mediastrømmen mellom de ulike nettverkene. Eksempler på slike nettverk kan for eksempel være et H.323 nettverk og et ISDN nettverk.
2) Terminal: Endepunkt som brukes til sanntidskommunikasjon av video, data eller lyd med andre endepunkter. En terminal kan for eksempel være en IP-telefon, utstyr for videokonferanse eller applikasjon på en PC.
3) Gatekeeper: Har ansvaret for en samling av H.323 enheter. Skal sørge for aksesskontroll for terminaler, adresseoversettelse, autentisering og båndbreddekontroll. Kan i en del tilfeller også tilby faktureringstjenester og call management[2]. Endepunkter som er registrert hos en gatekeeper danner en såkalt H.323 sone. Alle samtaler innen denne sonen må autoriseres av gatekeeperen.

[2] Call Management: Tjeneste som gjør det mulig å håndtere innkommende samtaler etter gitte parametere, som for eksempel tidspunkt på dagen eller hvem som ringer.

4) Multipoint Control Unit (MCU): Støtter konferanser mellom 3 eller flere endepunkter. Kan implementeres inn i en terminal, gateway, gatekeeper eller uavhengig i en egen PC.

Under en sesjon mellom endepunkter benytter H.323 seg av ulike kanaler. Når media skal overføres må det settes opp en kanal for å sende og en for å motta data. H.323 benytter ulike standarder for å kontrollere de ulike kanalene:

- H.225: Brukes til initiering av sesjoner.
- H.245: Benyttes i hovedsak til å utveksle parametere for samtalekontroll og sette opp og lukke mediakanaler. H.245 bruker TCP som underliggende protokoll
- Q.931: Benyttes til signalering som summetone og ringesignaler.
- Real Time Protocol (RTP): Protokoll for overføring av ulike former for multimedia. I forbindelse med VoIP vil RTP legge til ett headerfelt foran de ulike talepakkene som inkluderer informasjon om hvilken talekode som brukes. I tilegg legges det til sekvensnumre og tidsstempler slik at taletrafikken kan prosesseres og presenters på en ryddig måte ovenfor mottaker.
- RTP Control Protocol (RTCP): RTCP-pakker sendes periodevis i mediastrømmen og inneholder informasjon om antall RTP-pakker som sendes, pakketap og forsinkelse av pakker. Denne informasjonen kan for eksempel benyttes til å justere overføringshastigheten.

Innenfor rammeverket H.323 finnes også flere standarder. En av disse er Registration/Admission/Stauts Protocol (RAS). RAS sørger for blant annet kommunikasjon mellom endepunkter og gatekeeper samt å oversette H.323-adresser til IP-adresser.

2.3 Media Gateway Protocol (MGCP)

MGCP er en alternativ protokoll til SIP og H.323. MGCP benytter mange av de samme mekanismene som H.323, men sørger for signaleringsmuligheter for endepunkter, for eksempel en gateway, som er mindre avanserte og billigere enn de som benyttes i H.323. Endepunkter innefor MGCP trenger ikke å inneholde alle de ulike protokollene som benyttes i H.323.

MGCP benytter seg i hovedsak av to hovedkomponenter. En MGC-server som fungerer som en ”call agent” og et MG-endepunkter som utfører kommandoer som den mottar fra MGC-serveren.

Et eksempel på bruk av MGCP er når en enhet kobler seg på taleporten til gateway. Denne enheten vil da fungere som ett MG-endepunkt. Det blir så rapportert til MGC-serveren at en ny enhet er tilkoblet. MGC-serveren gir så beskjed tilbake til enheten om hvilken tjeneste som skal tilbys, for eksempel en melding om å aktivere summetone.

MGCP tar utgangspunkt i at de ulike MG-serverne synkroniser trafikken mellom de ulike endepunktene som er koblet opp mot den. Etter at en forbindelse er satt opp vil RTP-pakker utveksles direkte mellom de ulike endepunktene. MGCP protokollen har ansvaret for å gjøre IP-adreseser og portnumre tilgjengelige for MGC-serveren.

3 Sikkerhetsutfordringer

Fordi bredbåndstelefoni benytter seg av IP-teknologien vil mange angrep og trusler som har vært rettet mot tradisjonelle datanettverk også være en trussel for bredbåndstelefoni. Eksempler på dette kan være utnyttelse av svakheter i nettverket, tjenestenektingsangrep eller sniffing. Innen IP-telefoni vil dette medføre blant annet redusert opptid for selve tjenesten og risiko for avlytting av samtaler. Andre typer angrep kan være mer spesifikke for IP-telefoni. Blant disse angrepene finner vi trusler i forbindelse med oppsett av sesjoner og falsk brukerregistrering.

3.1 Sniffing

En sniffer er programvare eller datakomponenter som overvåker trafikken som går over en nettverksforbindelse. Alle data som passerer en slik forbindelse kan i utgangspunktet overvåkes, men som regel gjøres det et selektivt utvalg på hvilke data som skal overvåkes. For å velge hvilke data som skal overvåkes benyttes det som regel pakkefiltre, disse er på forhånd konfigurert ut fra bestemte regler. Innen IP brukes ofte betegnelsen pakkesniffing om sniffing.

I [4] nevnes det fire vanlige forutsetninger og komponenter for å utføre pakkesniffing:

1) Fysisk tilgang til nettet.
2) Programvare for å fange opp pakker.
3) Minne eller annen lagringskapasitet for å lagre pakker.
4) Programvare og maskinvare for å analysere og dekode pakker.

Som tideligere nevnt vil programvaren som fanger opp pakker ha innstillinger for å filtrere disse etter ulike kriterier. Eksempler på slike kriterier kan være MAC- adresser, IP-adresser, flagg og størrelse på pakkene. Programmene som brukes til sniffing har også ofte gode metoder for dekodning slik at informasjonen blir presentert ovenfor brukeren på en forståelig måte. Informasjonen som presenteres kan være IP-adresser, informasjon om navneservere, headerinformasjon, sekvensnummer, pakkestørrelse og flagg. Innefor bredbåndstelefoni kan denne informasjonen benyttes til å finne ut hvem som snakker sammen, hvor ofte ulike personer har samtaler og hvor lenge samtalene varer.

Pakkesniffing kan brukes både til lovlige og ulovlige formål. Trafikkanalyse, overvåking av båndbredde og feilsøking er noen av de mest vanlige formene for kommersiell bruk av pakkesniffing, og pakkesniffing blir dermed et nyttig verktøy for mange nettverksadministratorer.

Men pakkesniffing kan også benyttes av angripere og kan derfor være en potensiell trussel for bredbåndstelefoni. En angriper kan tilegne seg store mengder informasjon ved å benytte seg av pakkesniffing. Informasjonen som sniffes opp kan være informasjon om brukerkonto og passord, sensitive persondata, eller annen konfidensiell informasjon. Innenfor bredbåndstelefoni vil det først og fremst være avlytting som er det mest aktuelle bruksområdet for sniffing. Denne informasjonen kan angriperen enten bruke til egen personlig vinning eller til å skade andre. Bedrifter og organisasjoner vil ofte være mer utsatt for slike angrep enn privatpersoner da samtaleinformasjon fra disse vil være mer verdifull for angriperen. Informasjonen som sniffes opp kan for eksempel benyttes til bedriftsspionasje. Også angrep fra en bedrifts egne ansatte er vanlige innen denne formen for angrep, denne typen angrep er ekstra alvorlige da angriperen i disse tilfellene har inngående kjennskap til hvilken informasjon det skal letes etter.

Siden transporten av talestrømmen i VoIP ofte ikke er kryptert vil det være mulig å lagre en samtale og deretter sette de sammen igjen slik at den kan spilles av. Det finnes i dag en del programmer fritt tilgjengelig på Internett som er i stand til å utføre sniffing og avspilling av RTP trafikk. Et eksempel på et program som gjennomfører en slik operasjon er ”Voice over misconfigured Internet Telephones” (VOMIT) [33]. Ved å benytte seg av verktøyet tcpdump på en unix plattform kan VOMIT fange opp en strøm av VoIP-pakker, disse pakkes settes deretter sammen og presenteres for brukeren som en avspillbar lydfil.

Ifølge dokumentasjonen til VOMIT støtter programmet talekoding av formatet G.711. Formatet G.711 er i dag en av de mest brukte talestandardene for bredbåndstelefoni og benyttes av de fleste norske tilbydere. Hvis trafikken ikke er kryptert vil det være mulig å for en sniffer å spille av samtaler kodet med denne standarden ved hjelp av VOMIT.

Nettverk som kombinerer VoIP trafikk sammen med vanlig IP trafikk vil være mer utsatt for angripere som ønsker å avlytte VoIP trafikken. Dette skyldes blant annet at antallet

potensielle angripere øker samtidig som da det i mindre grad vil være mulig å konkret overvåke VoIP trafikken. Tilbydere bør derfor tilstrebe i størst mulig grad å separere disse to trafikktypene. Hvordan dette kan gjøres er nærmere omtalt i kapittel 6.1.

3.2 Tjenestenektingsangrep (DoS attacks)

Det finnes mange ulike former for tjenestenektingsangrep, men generelt er det tilgjengeligheten til tjenester som brukeren vanligvis benytter som rammes. Tjenestenektingsangrep er generelt vanskelige angrep å beskytte seg imot, og er vanlige angrep innenfor IP-nettverk. I de siste årene er det blitt stadig lettere å gjennomføre slike angrep. Tideligere ble disse angrepene gjennomført av for eksempel en gruppe hackere som samarbeidet om å ramme et bestemt mål. Nå er dette blitt mulig å gjennomføre distribuerte angrep ved hjelp av programvare. Maskiner som ikke har god beskyttelse mot virus vil kunne bli infisert av programmer som kan benyttes av angripere til å gjennomføre tjenestenektingsangrep. Programvaren for å utføre slike angrep blir stadig mer tilgjengelig. Dette har redusert terskelen for angrep og dermed også økt antallet potensielle angripere. Disse angrepene vil derfor også være en stor trussel for bredbåndstelefoni. Det finnes mange forskjellige måter å nekte brukere tilgang til tjenester på. Her vil noen av de som er mest aktuelle for bredbåndstelefoni bli gjennomgått.

3.2.1 Buffer overflow

Slike angrep forekommer når en prosess eller et program laster for mye data inn i et buffer slik at bufferet blir overfylt. Dette skyldes som regel dårlig konfigurert programvare som gjør det mulig å sende større pakker enn det bufferet er konfigurert for. Når slike angrep inntreffer vil ikke enheter som rammes av angrepet lenger være tilgjengelige og systemer som er avhengige av disse maskinene vil ikke lenger fungere. Hvis dette er sentrale servere eller lignende vil et stort antall brukere kunne bli rammet. Buffer Overflow angrep kan også gi flere problemer enn kun tjenestenekting. Et eksempel på dette er når sensitive data plutselig vil bli tilgjengelige for potensielle angripere på grunn av minneproblemer i systemet. Eksempler på informasjon som da blir tilgjengelig kan være IP-adresser eller passordinformasjon.

Senter for informasjonssikring (SIS) varslet i Juli 2005 om at en Cisco Call Manager var sårbar for Buffer Overflow angrep [11]. Fra hjemmesiden deres [10] kan en lese følgende informasjon:

”Sårbarhetene er relatert til allokering og endring av minne. Det åpner for at angriper kan få utført tjenestenektingsangrep og selvbestemt kode. Sårbarhetene er ikke betegnet som kritiske, da angriperen må være på innsiden av nettverket for å kunne utnytte dem.
Et tjenestenektingsangrep vil føre til at Call Manager-serveren skrur seg av og starter opp på nytt. Når serveren er kompromittert, kan angriper omdirigere samtaler og avlytte dem. I tillegg kan han/hun oppnå tilgang til nettverk og maskiner som kjører Cisco VoIP-produkter.”

3.2.2 Tjenestenektingsangrep mot tale (RTP angrep)

Som nevnt er det RTP protokollen som benyttes til å overføre tale i forbindelse med bredbåndstelefoni. RTP protokollen er en meget enkel protokoll. Siden talen er avhengig av å leveres i sanntid og er svært følsom for forsinkelser vil RTP være sårbar for angrep der systemet oversvømmes av falske pakker. Disse pakkene blander seg med den vanlige trafikken og det vil derfor være vanskelig å skille mellom de ulike pakkene. Resultatet blir at hele eller deler av taletrafikken forsinkes eller droppes og resultatet blir at samtalen blir umulig å gjennomføre.

Mange telefoner har også dårlige mekanismer for å kontrollere trafikken de tar imot. Etter at RTP forbindelsen med en annen telefon er satt opp sjekkes ikke lenger IP-adressene på RTP strømmen som kommer inn. Det er derfor mulig å sende data til telefonene uten at denne blir oppfattet som ulovlig. Store RTP pakker på 1500 byte har også fått enkelte typer telefoner til å låse seg.

3.2.3 Tjenestenektingsangrep mot proxyservere

Ved å bruke programvare for å generere angrep kan en sende store mengder INVITE meldinger til proxyservere eller telefoner. Ved slike angrep vil en kunne blokkere trafikken og det vil ikke være mulig å etablere samtaler for gyldige brukere av disse enhetene.

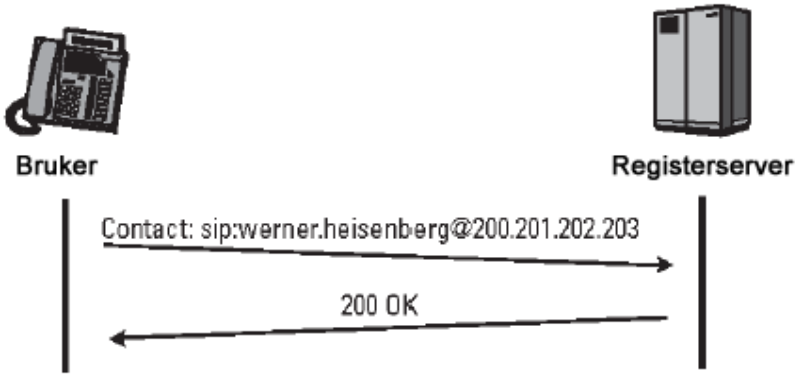
3.3 Oppdatering av SIP registerserver

Ved å studere hvordan en SIP registerserver oppdateres av en bruker som ønsker å endre sin lokasjon, kan en danne seg et bilde av hvordan noen av de ulike angrepene mot implementasjoner av SIP kan realiseres.

En registerserver har som oppgave å ta imot "SIP REGISTER" forespørsler fra brukere slik at en brukers lokasjon til enhver tid er oppdatert. Registerserveren bruker informasjonen den mottar til å oppdatere sin database, denne informasjonen blir dermed tilgjengelig for proxy- og viderekoblingsservere innefor det samme administrative domenet.
Denne lokaliseringsinformasjonen benyttes til ruting av SIP forespørsler.

En tilsvarende endring av lokasjon finnes ikke i et tradisjonelt telefonsystem, men det har en del likheter med hvordan dette gjøres innen mobiltelefoni. En mobiltelefon sender sin identitet til en basestasjon. Basestasjonen videresender så mobiltelefonens lokasjon og telefonnummer til et "home location register" (HLR). Når så "mobile switching center" (MSC) mottar en innkommende samtale forhører MSC seg med HLR for å finne posisjonen til mobiltelefonen.

Figur 3-1 "Bruker sender en "SIP REGISTER" forespørsel til en SIP server " modifisert fra [1]



I dette eksemplet hentet fra [1] skal brukeren, Werner Heisenberg, oppdatere sin lokasjon ovenfor en SIP registerserver. Det sendes da en "SIP REGISTER" forespørsel fra bruker til registerserver for å oppdatere registerserveren om brukerens lokasjon. Registerserveren godkjenner oppdateringen ved å sende en "OK" responsmelding tilbake til bruker.

Figur 3-2 ”Utdrag fra headerinnholdet i en ”SIP REGISTER” forespørsel” modifisert fra [1]

```
REGISTER sip:registrar.munich.de SIP/2.0
Via: SIP/2.0/UDP 200.201.202.203:5060;branch=z9hG4bKus19
Max-Forwards: 70
To: Werner Heisenberg <sip:werner.heisenberg@munich.de>
From: Werner Heisenberg <sip:werner.heisenberg@munich.de>
 ;tag=3431
Call-ID: 23@200.201.202.203
CSeq: 1 REGISTER
Contact: sip:werner.heisenberg@200.201.202.203
Content-Length: 0
```

Fra figur 3-2 er følgende tre felter mest relevante for vårt eksempel:

1) ”To” indikerer hvilken adresse oppdateringen gjelder. Dette vil være brukeren sin velkjente URI adresse.
2) ”From” forteller hvem som sender meldingen. I de fleste tilfeller vil ”To” og ”From” feltene være like da det som regel er brukeren selv som oppdaterer sin egen lokasjon. Men i enkelte tilfeller kan en tredjepart ha rettigheter til å gjøre endringer og feltene ”To” og ”From” vil da være ulike.
3) ”Contact” inneholder den oppdaterte adressen til brukeren.

Forbindelsen mellom Heisenbergs velkjente adresse i ”To” feltet og den oppdaterte adressen i ”Contact” feltet lagres nå i registreringsserveren sin database. Når en proxyserver nå gjør en forespørsel mot databasen for å lokalisere Heisenbergs URI vil den motta URI’en tilhørende Heisenbergs ”Contact” adresse.

Denne type oppdatering foregår vanligvis automatisk ved installasjon av en SIP enhet og deretter i bestemte tidsintervaller satt opp av registerserveren.

Bakgrunnen for at denne mekanismen i utgangspunktet utgjør en sikkerhetsrisiko er at er at de ulike headerfeltene kan modifiseres av brukeren, og dermed også av potensielle angripere. Et eksempel på et slikt angrep er ”registration hijacking” som vil beskrevet i neste kapittel.

3.4 Falsk brukerregistrering (”registration hijacking”)

Falsk brukerregistrering gjør det mulig for en angriper å kapre brukeridentiteten til en gyldig bruker. Kapring av brukeridentitet kan føre til at innkommende anrop fanges opp av en angriper isteden for den tiltenkte mottakeren av samtalen. Hvis slike angrep er vellykket vil angriperen ha mulighet til å blokkere, avlytte eller manipulere samtaler.
Det er også mulig å blokkere trafikken inn til en gateway, og konsekvensen kan da bli enda større siden dette gir muligheter for å ramme flere brukere samtidig.

Hvis et angrep av denne typen skal realiseres må en først angriperen finne gyldige SIP adresser som kan utnyttes. For en intern angriper, som kjenner en bedrifts adressestruktur, vil dette være ganske trivielt. En ekstern angriper som på forhånd ikke kjenner disse adressene må søke etter disse ved hjelp av en såkalt skanner. En skanner generer SIP forespørsler til ulike adresser, responsen på disse forespørslene avgjør om adressen er gyldig.

Når en adresse har blitt identifisert kan et angrep utføres ved at en angriper sender en modifisert ”SIP REGISTER” forespørsel til en SIP registerserver. Målet med denne modifiserte forespørselen er å fjerne brukeren sin gyldige adresse slik at ”Contact-URI” ikke lenger inneholder noen oppdatert adresse.

I neste fase sender så angriper en ny ” SIP REGISTER” forespørsel hvor ”Contact-URI” nå er erstattet med angriperen sin adresse. Dermed vil all trafikk og forespørsler inn til den gyldige brukeren i stedet bli videresendt til angriperen.

For å sikre seg på best mulig måte mot slike angrep er det viktig å implementere sterk autentisering. Autentiseringsmekanismer i SIP vil bli nærmere omtalt i kapittel 4. Det bør også settes begrensinger på hvilke brukere som har behov for å registrere seg fra eksterne nettverk, men denne løsningen vil også fjerne en del av brukervennligheten som SIP representerer. Det er også tvilsomt om det i dag finnes gode mekanismer for å gjennomføre dette. SIP mobilitet regnes som en av de foretningsmessige fortrinnene ved SIP og ved å blokkere denne muligheten vil en gjøre SIP mindre attraktivt for kommersielle formål som for eksempel bredbåndstelefoni over trådløs nettverk.

3.5 DHCP

Dynamic Host Configuration Protocol (DHCP) brukes i dag ofte for å gjøre IP nettverk mer skalerbare. DHCP sørger for å dynamisk allokere IP adresser til brukere av et LAN. Et potensielt sikkerhetsproblem er at angripere kobler seg på et nettverk som benytter DHCP. En angriper kan fysisk koble seg på ledige porter på en svitsj eller benytte virusprogramvare på maskiner som allerede er koblet på nettverket. Angripere kan i sin enkleste form være personer som kobler til en IP-telefon på et bedriftsnettverk for å sikre seg gratis telefoni, eller mer ondsinnede angripere som ønsker å ramme eksisterende brukere.

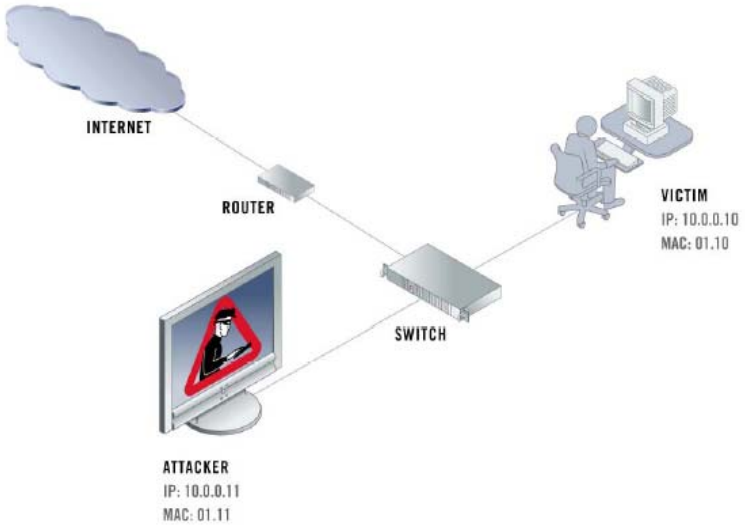
Ett eksempel på et DHCP angrep er at angriper kobler seg på nettverket og setter opp en falsk DHCP server, serveren gir en falsk DHCP respons tilbake til IP-telefonen og angriperen vil dermed være i stand å blokkere trafikken ved å manipulere adressene eller ved at angriperen overvåker trafikken ved å fungere som en mellommann.

3.5.1 Adress Resolution Protocol (ARP)

Adress Resolution Protocol (ARP) benyttes for å mappe adresser mellom logiske IP-adresser og fysiske MAC-adresser. En svitsj sender ut broadcast meldinger med en IP-adresse og alle enheter må da kontrollere om denne IP-adressen tilhører dem. Den enheten som er eier denne IP-adressen må svare med å oppgi sin MAC-adresse. Et angrep kan nå foretas i tre faser:

1) Ved å svare ukorrekt på slike broadcast- meldinger vil en angriper være i stand til å sette seg selv opp som mottaker av trafikk den egentlig ikke er tiltenkt. Enheten som egentlig skulle ha tatt imot denne trafikken vil nå ikke være i stand til å motta pakker.
2) Angriperen sender så falske ut nye falske meldinger som gjør at enheten som er utestengt videresender sin utgående trafikk til angriperen. Angriperen mottar nå inngående og utgående trafikk som er tiltenkt den andre enheten.
3) Angriperen videresender alle denne trafikken og enheten som er angrepet vil oppfatte alt som normalt. Angriperen har derimot plassert seg mellom enheten og den utgående svitsjen og vil dermed kunne avlytte trafikken.

Figur 3-3 ”ARP spoofing angrep” fra [32]



Ved et ARP-Spoofing angrep vil en angriper med IP-adresse 10.0.0.11 svare på vegne av IP-adresse 10.0.0.10 når svitsjen sender ut broadcast meldinger. Meldinger som er sendt til 10.0.0.10 vil da havne på MAC-adresse 01.11 som tilhører angriperen.

Et sikkerhetstiltak for å hindre en angriper i å ulovlig koble seg på et LAN er å tildele lovlige brukere statiske IP-adresser koblet opp mot MAC-adressen til disse brukerne sine IP-telefoner. Hvis en enhet med en ukjent MAC-adresse kobler seg på nettverket vil ikke denne enheten automatisk motta noen IP-adresse, men vil derimot kun få benytte IP-adressen som er assosiert med den aktuelle MAC-adressen . Hvis MAC-adressen ikke er registrert vil brukeren ikke bli tildelt noen IP-adresse. En slik løsning krever derimot en del ekstra ressurser i forbindelse med nettverksadministrasjon og vil dessuten ikke være helt sikker mot mulige angrep. Hvis en angriper klarer å avlytte trafikken og lese av en gyldig MAC-adresse vil angriperen være i stand til å statisk tildele sin egen maskin denne MAC-adressen og dermed få tilgang til nettet, men denne operasjonen er mer komplisert og dermed utgjør den en mindre fare.

3.6 Trusler i forbindelse med oppsett av sesjoner

Under oppsett av en SIP sesjon, slike som vist i kapittel 2.1.1, benyttes det i tillegg en Session Description Protocol (SDP). SDP informasjonen sendes sammen med INVITE, OK og ACK meldingene som transporters mellom brukeragenten via proxyserverene. SDP informasjonen overføres ved at SIP meldingene benytter en såkalt MIME[3] Body. SDP inneholder en rekke parametere vedrørende SIP sesjonen som skal settes opp. Informasjon om IP-adresser, portnummer, mediatype og koding er standardfelter. I tillegg kommer en rekke tilleggsfelter som brukeragentene som setter opp sesjonen fritt kan benytte.

Figur 3-4 "SDP tilleggsfelter fra en SIP INVITE melding" modifisert fra [31]

```
o=alice 3157331353 3157331353 IN IP4 160.85.170.139
c=IN IP4 160.85.170.139
k=clear:910bc4defa71eb6190008762fca6ae2f1d959e87cdf3c0c5c5076ad38ee8
m=audio 10000 RTP/AVP 0
```

1) Owner("o"): Indikerer hvem som eier sesjonen. Eier av sesjonen vil være den brukeragenten som initierer sesjonen.
2) Contact Information ("c"): Når INVITE meldingen kommer fram til mottaker vet mottaker at avsender skal kontaktes på denne IP-adressen.
3) Key ("k"): Felt for å utveksle krypteringsnøkler. Dette vil som regel være symmetriske nøkler. I figuren over ser vi at vi at metoden "clear" er valgt. Det vil si at nøkkelen overføres direkte under oppsettet av sesjonen. SDP tilbyr også andre metoder for å overføre nøkler, blant annet "Prompt" der nøkkelen overføres etter at sesjonen er satt opp.
4) Media Session ("m"): Forteller hvilken type media som skal overføres og med hvilken protokoll.

[3] MIME (Multipurpose Internet Media Extensions) : Protokoll som ble utviklet for bruk innen e-post som gjør det mulig å overføre flere typer data enn kun tekstbasert data. Eksempler på slike data kan være grafikk, lyd, video eller andre filtyper.

SDP kan altså benyttes til nøkkeldistribusjon, men siden SDP ikke selv tilbyr kryptering av trafikken må sikker nøkkeldistribusjon med SDP baserer seg på underliggende sikkerhetsmekanismer som S/MIME, TLS eller IPsec. Disse metodene vil bli nærmere omtalt i kapittel 4.

Når brukeragenter sender forespørsler i forbindelse med oppsett av en sesjon blir disse sendt via en eller flere proxyservere. Fra brukere som deltar i en sesjon vil det være viktig å være klar over hvilke sikkerhetsbestemmelser som skal gjelde for disse proxyserverene, og om disse proxyserverene er til å stole på.

Serverne må være i stand til å videresende meldinger, men i mange tilfeller er det ønskelig at innholdet i selve meldingen skal holdes hemmelig for serveren. Dette skyldes at ulike angripere vil være i stand til å utnytte innholdet i SIP meldingene. Som det er vist i figur 3-4 inneholder meldingene både adresseinformasjon og eventuelt en krypteringsnøkkel. Begge deler er interesant for eventuelle angripere. Mellomliggende proxyservere vil derfor være et attraktivt sted for ulike angripere og dårlig sikring av proxyservere muliggjør flere typer angrep.

En angriper vil potensielt være i stand til å utnytte innholdet i meldingene under oppsettet av en sesjon ved å skaffe seg nøkkel og adresseinformasjon. Angriperen vil dermed kunne påvirke trafikken mellom de to brukeragentene. En mulighet er at angriper endrer adresseinformasjonen og fungerer som en mellommann, det vil si at angriperen opptrer som brukeragent A ovenfor brukeragent B og motsatt. Hvis trafikken er ukryptert eller angriperen klarer å utnytte krypteringsnøkkelen til å dekryptere den kommende trafikken i sesjonen som er satt opp mellom de to endepunktene vil det åpne seg da muligheter for manipulering av samtalen:

- Angriperen kan endre adresseinformasjonen og rute trafikken via et punkt i nettverket som angriperen har adgang til. Angriperen kan være i stand til å sniffe trafikken og avlytte samtalen.
- Angriperen kan sende en ”Re-INVITE” melding på vegne av den ene brukeragenten med for eksempel nye sikkerhetsparametere som gjør at trafikken ikke lenger skal krypteres.

- Angriperen kan sende falske meldinger og rive ned forbindelsen. Et eksempel på dette er hvis angriperen sender en ”BYE” forespørsel til den ene brukeragenten. Brukeragenten vil da oppfatte dette som et ønske om å avslutte samtalen og samtalen kobles dermed ned.

Det er derfor viktig at informasjonen som overføres mellom to brukeragenter ikke kan utnyttes i mellomliggende servere. Det vil være viktigst å sikre selve meldingsinnholdet, men siden proxyservere er avhengige av visse deler av headeren er det ikke ønskelig at alle feltene i headeren skal beskyttes med ende-til-ende kryptering.

3.7 Mottiltak

Det finnes flere mottiltak mot de truslene som nå er omtalt, noen av de viktigste er:

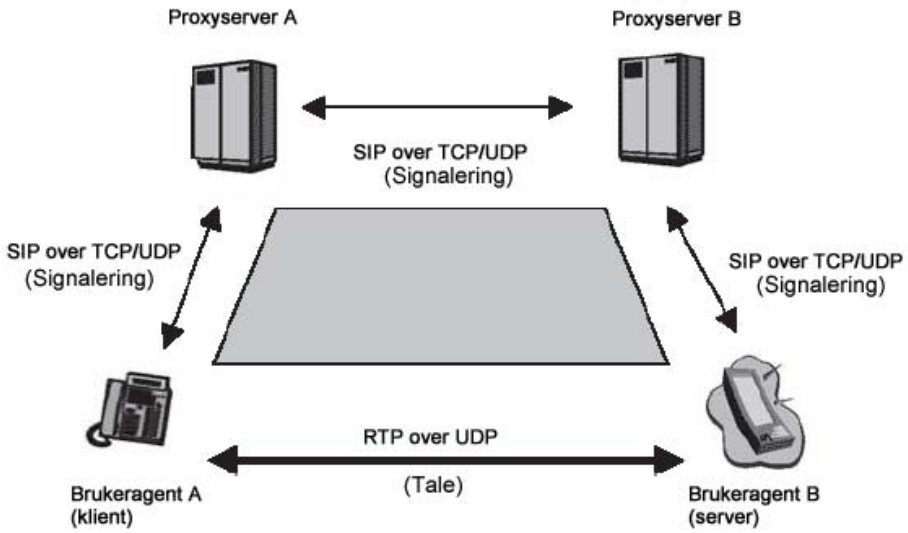
- Sterk autentisering ved brukere som ønsker å initiere samtaler.
- Benytte moderne brannmurer kombinert med verktøy som er i stand til å overvåke og analysere trafikken og eventuelt skille mellom data og taletrafikk.
- Prioriter trafikk fra kjente kilder.

Disse metodene vil bli nærmere omtalt i kapittel 4, 5 og 6.

4 Sikkerhetmekanismer i forbindelse med SIP

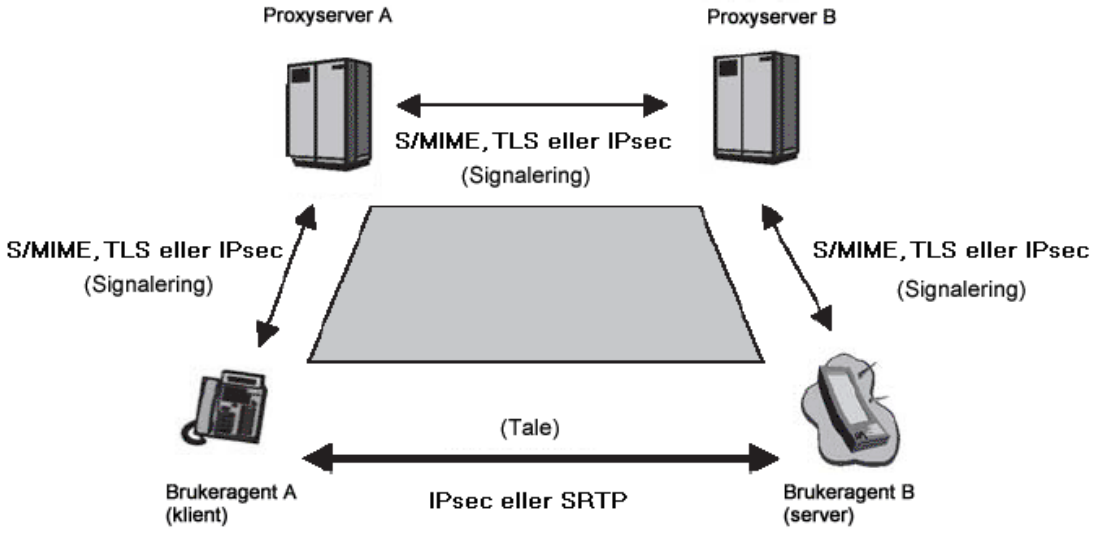
SIP protokollen i seg selv gir ikke noen muligheter for å kryptere data. Som tideligere omtalt benyttes RTP for å transport av mediastrømmen innenfor VoIP implementasjoner.

Figur 4-1 "Bruk av protokoller for overføring av signaler og tale innen SIP" modifisert fra [1]



Fra figuren ser vi at SIP meldinger benyttes til signalering mens RTP meldinger benyttes til tale .Den eneste sikkerhetsmekanismen som tilbys i RTP er konfidensialitet. Med konfidensialitet menes det at bare den tiltenkte mottakeren av en melding skal være i stand til å lese innholdet i meldingen. For andre enn mottakeren vil altså ikke meldingen inneholde noen nyttig informasjon. For å sikre konfidensialitet av en melding må det benyttes kryptering. For å kryptere trafikken benytter RTP seg av standarden Data Encryption Standard (DES). Fordelen med DES er at det er en rask algoritme, men den tilhørende ulempen er at den ikke lenger regnes som noen sikker algoritme. Algoritmen kan derfor brukes som en slags nødløsning for kryptering av mediastrømmen mellom to SIP enheter hvis andre tyngre krypteringsalgoritmer gir så mye forsinkelse av pakker at det går utover kvaliteten på samtalen.

Figur 4-2 ”Bruk av protokoller for sikker overføring signaler og tale innen SIP” modifisert fra [1]



Fra figuren ser vi at IPsec eller SRTP kan benyttes for å beskytte taletrafikken, mens S/MIME, TLS eller IPsec kan benyttes for å beskytte signaleringstrafikken. S/MIME, TLS og IPsec vil nå bli nærmere omtalt mens SRTP vil bli omtalt i kapittel 7.

4.1 Secure MIME(S/MIME)

I den første versjonen av SIP kunne Pretty Good Privacy (PGP) benyttes til å autentisering og kryptering av innholdet i SIP-meldinger, men fra og med versjon 2 ble PGP erstattet av S/MIME. Som sagt fraktes innholdet i SDP meldingene inne i MIME bodies. S/MIME tilbyr mekanismer både for å signere og kryptere slike meldinger. Disse mekanismene har felles betegnelsen public-key cryptography specifications(PKCS) og er gjort tilgjengelig for S/MIME fra RSA laboratoriet.

- Kryptering: Her tilbys det både ende til ende kryptering eller kryptering mellom hver enkelt node. S/MIME tilbyr kryptering ved å benytte Enveloped Data. Det vil si at det benyttes en symmetrisk nøkkel for å kryptere innholdet i meldingen. Deretter krypteres denne symmetrisk nøkkelen av mottaker sin offentlige nøkkel. Den krypterte sesjonsnøkkelen, informasjon om mottakers offentlige nøkkel (X.509) og informasjon om hvilken algoritme som brukes oversendes til mottaker.

- Signering: Her benyttes enten algoritmene SHA1 eller MD5 til å generere et vedlegg. Dette vedlegget signeres så av avsender sin private nøkkel. Dette sendes til mottaker sammen med informasjon om avsenders offentlige nøkkel (X.509) og informasjon om hvilken algoritme som er brukt.

S/MIME er et godt alternativ for sikkerhet i forbindelse med oppsett av sesjoner. Ved å benytte S/MIME fra ende-til-ende kan en som sagt både sørge for både autentisering og kryptering. SDP innholdet vil dermed bli utilgjengelig for mellomliggende servere, mens headerinnholdet vil fortsatt være tilgjengelig og dermed kan forespørslene videresendes. Bruk av S/MIME forutsetter implementering av ett rammeverk for offentlig nøkkeldistribusjon, siden X.509 sertifikater benyttes i forbindelse med både autentisering og kryptering.

4.2 IPsec

IPsec er anvendelig innenfor bredbåndstelefoni siden det både kan tilby beskyttelse av selve taletrafikken og beskyttelse av SIP-meldinger i forbindelse med oppsett av sesjoner.

IPsec er en samling av sikkerhetsprotokoller og krypteringsalgoritmer som tilbyr metoder for å beskytte IP pakker som fraktes over nettverket mot uautoriserte brukere. IPsec sørger for ulike sikkerhetsfunksjoner, autentisering og kryptering på IP-laget. IPsec fungerer sammen med både Ipv4 eller Ipv6, men i Ipv6 er Ipsec innebygd i protokollstakken. Ipsec er derfor i utgangspunket en mekanisme som burde er godt egnet for å kombinasjon med VoIP trafikk, men en implementasjon av Ipsec i et VoIP nettverk byr på en del utfordringer.

Før IPsec trafikk kan passere gjennom et nettverk er en avhengig av å etablere systemer for utveksling av nøkler. Hver ruter, brannmur eller server må være i stand til å identifisere identiteten til sin nærmeste node. IPsec er altså avhengig av nøkkeldistribusjon.

Det finnes ingen definerte retningslinjer på hvordan IPsec skal kombineres med SIP. Dette gjelder både nøkkeldistribusjon og hvilke mekanismer IPsec mekanismer som skal benyttes. Det rammeverket som er mest benytter for nøkkeldistribusjon er Internet Key Exchange (IKE). IKE benytter seg av tre ulike metoder for nøkkeldistribusjon

- Internet Security Association and Key Management Protocol (ISAKMP).

- Oakley Key Determination Protocol
- Secure Key Exchange Mechanism for the Internet (SKEME).

Kort sagt så benyttes Oakley og SKEME til nøkkelutveksling innenfor rammeverket ISAKMP.

IPsec baserer seg på to ulike metoder:

1. Encapsulating Security Payload Protocol (ESP): En sikkerhetsprotokoll som sørger for datakonfidensialitet ved å benytte kryptering. ESP tilbyr også metoder for autentisering og ESP kan benyttes alene eller sammen med Authentication Header (AH). ESP sørger med dette også for beskyttelse mot ulike typer angrep.
2. Authentication Header (AH): Kan benyttes alene eller sammen med ESP. AH sørger for pakkautentisering ved å benytte kryptografiske sjekksummer.

ESP og AH kan benyttes i to forskjellige typer overføring. I transportmodus krypteres nyttedata og headerfelter fra øvre lag. En angriper som fanger opp en slik pakke vil altså ikke være i stand til å lese av innholdet i pakken, men derimot hvor pakken skal sendes. Transportmodus gir dermed ingen beskyttelse mot ulike former for trafikkanalyse. Innenfor bredbåndstelefoni vil altså være mulig for en angriper å finne ut av hvem som ringer hverandre og hvor lenge de ulike samtalene foregår.

I tunnelmodus krypteres den originale IP-pakken. Den originale IP-pakken benyttes så som innhold i en ny IP-pakke. Dermed vil det ikke lenger være mulig å bestemme hvem som er mottaker av den originale IP-pakken.

En ulempe med IPsec i forbindelse med SIP er at mellomliggende servere mellom de to brukeragentene er nødt til å kjenne innholdet i SIP headeren. IPsec kan derfor ikke benyttes i ende-til-ende forbindelser når sesjoner skal settes opp, men isteden må det settes opp nye tunneler mellom hver enkelte node. IPsec forbindelser kan settes opp permanent eller ved behov. Ved bruk av permanente forbindelser slipper brukeragenten å sette opp en ny forbindelse hver gang en sesjon skal etableres.

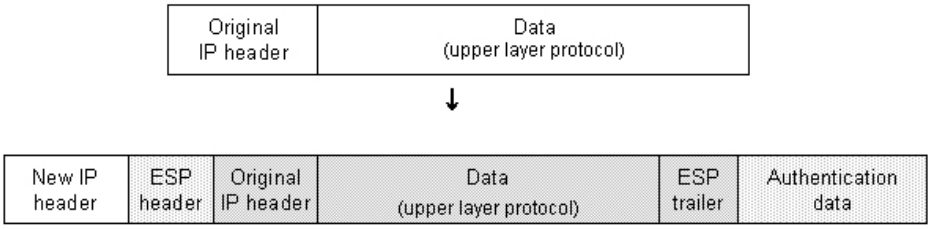
Sikkerhet i VoIP er ment å beskytte både selve innholdet i samtalen og informasjon om hvem som deltar samtalen. IPsec kan gi i utgangspunktet beskyttelse mot begge disse to delene hvis

den benyttes sammen med ESP i "Tunnelmodus". ESP benyttes for å sikre begge endepunktene i samtalen og talen som overføres vil gis beskyttelse mot trafikkanalyse, "man-in-the-middle" angrep og pakkesniffing. Men i det siste er det kommet fram at IPsec som kun benytter ESP i ”tunnelmodus” uten integritetskontroll av meldingene er utsatt for angrep. Det anbefales derfor å kombinere ESP med AH for å sørge for integritet i IPsec.

4.2.1 Utfordringer i forbindelse med IPsec og bredbåndstelefoni

Taletrafikk er spesielt følsom for forsinkelser og dette kan bli et problem når man kombinerer taletrafikk og IPsec. Det største problemet vil være at ved å benytte ESP vil en generere mye overhead på hver enkelt IPsec pakke og dermed vil det stilles større krav til båndbredden og forsinkelse vil kunne oppstå. Hvor mye overhead som genereres er avhengig av hvordan krypteringen utføres..

Figur 4-3 ”Overhead i forbindelse med IPsec”



Figuren viser hvordan pakkestørrelsen øker ved å benytte ESP. Ved benyttelse algortimen 3DES vil overhead kunne bli:

- ESP header, 8 bytes
- Initieringsvektor, 8 bytes
- ESP trailer, 2-9 bytes
- Autehentication data, 12 bytes

Det må derfor nøye planlegges hvor i nettverket IPsec skal implementeres. Det kan settes opp IPsec tunneler ut til endepunktene eller oppgaven kan overlates til rutere eller brannmurer som kan være endepunkter på et LAN. Et problem med å legge krypteringsfunksjonaliteten i for eksempel i en ruter er at VoIP pakkene kan forsinkes. I en vanlig datastrøm av pakker som passerer gjennom en ruter vil det vanligvis bare være en liten del av disse som skal krypters. Det har derfor ikke vært sett på som en nødvendighet fram til nå å implementere mekanismer for skille mellom ulik trafikktyper i krypteringsmotorene siden den krypterte trafikken aldri har vært noen flaskehals. Med kryptering av VoIP trafikk er dette derimot blitt et problem. Hvis en skal kryptere en VoIP samtale vil det være store mengder data som er nødt til å krypteres Talepakker må derfor konkurrere med datapakker om de samme ressursene og resultat kan bli forsinkelser for talepakkene.

En mulig løsning på dette problemet er å legge krypterings- og dekrypteringsfunksjonaliteten ut til endepunktene på nettverket. Dette krever at de ulike endepunktene har nok prosesseringskraft til å håndtere kryptering og samtidig levere talepakkene rask nok slik at det ikke går utover kvaliteten på samtalen. Nye og bedre adaptere eller telefoner gjør at dette i stadig større grad er en mulighet. Hvis telefonene ikke kan håndtere krypteringen vil en annen mulighet være å legge krypteringen ved en gateway eller en brannmur inn til det lokale nettverk slik at trafikken innad i nettverket er ukryptert mens trafikken som går over Internett krypteres.

4.2.2 Sårbarhet i forbindelse med enkelte implementasjoner av IPsec

I mai 2005 sendte ”the National Infrastructure Security Co-ordination Centre” (NISCC) ut en advarsel om svakheter i forbindelse med IPsec som benytter ESP i ”tunnelmodus” [13]. Det beskrives tre ulike implementasjoner som kan være utsatt for slike angrep:

- Encapsulating Security Payload (ESP) i tunnelmodus uten integritetsbeskyttelse.
- Systemer som kun benytter integritetsbeskyttelse fra et høyere lag i protokollstakken.
- Autehentication Header (AH) i end-til-ende forbindelser satt opp i transportmodus inne i en ESP tunnel.

På grunn av at en del IPsec implementasjoner benytter seg av Cipher Block Chaining (CBC)[4] vil det være mulig for angripere å benytte såkalte bit-flipping angrep på kryptere bitstrømmen for å ende innholdet på bestemte deler i den originale teksten. Normalt sett vil slike angrep ikke føre til at noen kan klare å lese av den krypterte teksten, men på grunn av en svakhet i forbindelse med Internet Control Message Protocol (ICMP) meldinger kan dette nå la seg gjøre ved visse implementasjoner av IPsec.

Bakgrunnen for dette er mellomliggende rutere som prosesser innholdet av ESP-pakkene. Innholdet av disse pakkene vil være tilgjengelige i klartekst under denne prosesseringen. Denne informasjonen vil ikke være tilgjengelige for angripere i selve ruteren, men informasjonen kan gjøres tilgjengelig ved å manipulere ruteren til å sende ICMP-pakker. På grunn av måten ICMP er konfigurert vil ICMP-pakkene inneholde informasjon om headerfeltene og nyttedata i den originale meldingen.

For at slike angrep skal være mulige å gjennomføre er angriperen avhengig av å ha verktøy for sniffe trafikken mellom de ulike enhetene som benytter IPsec, angriperen er også avhengig av å sortere ut de riktige ICMP-pakkene. Det gis ingen konkret beskrivelse på hvordan bit-flippingen gjennomføres, men NISCC nevner tre ulike angrepstyper som kan rettes mot IPsec:

1) Forandre mottakeradresse
    - En angriper forandrer mottakeradressen i den indre delen ved å benytte ”bit-flipping” på den ytre delen.
    - Ruteren dekrypterer pakken og videresender pakken i henhold til den nå modifiserte indre delen av pakken.
    - Hvis angrepet er vellykket ankommer den indre delen av pakken til adressen bestemt av angriperen.
2) Forandring av headerfelt og avsenderadresse
    - En angriper forandrer lengden på headerfeltet og avsenderadressen i den indre pakken ved å benytte bit-flipping på den ytre delen.
    - Endringene vil mest sannsynlig føre til at ruteren som mottar pakken vil generere en ICMP melding som den sender til den falske avsenderadressen.

[4] Cipher block chaining (CBC): Krypteringsmekanisme som benyttes mot blokker av data. Bruker mekanismer som gjør at krypteringen og dekrypteringen av en blokk er avhengig av den foregående blokken. Den første blokken er avhengig av en initieringsvektor (IV)for å kunne krypteres/dekrypteres. IV må også være tilgjengelig for den som skal dekryptere teksten.

- Ved å studere innholdet i ICMP pakken kan nå angriperen finne ut innholdet i den originale meldingen.

3) Endring av protokollfelt og avsenderadresse
    - En angriper forandrer protokollfeltet og avsenderadressen i den indre pakken ved å benytte bit-flipping.
    - Ruteren videresender pakken til den originale mottakeren
    - Når mottakeren av pakken inspiserer pakken og oppdager feilen i protokollfeltet genereres det en ICMP ”protocol unreachable” melding som sendes til den falske avsenderadressen.
    - Og på samme måte som i eksemplet over kan nå angriperen lese av innholdet i den originale meldingen.

For å sikre seg mot slike angrep lanserer NISCC tre alternative mottiltak:

1) Sørg for å benytte ESP både til beskytte konfidensialitet og integritet.
2) Benytt AH til integritetsbeskyttelse, men unngå varianten med (AH) i ende-til-ende forbindelser satt opp ”transport mode” inne i en ESP tunnel.
3) Konfigurer systemet slik at ICMP meldinger ikke benyttes, eller filtrere bort disse meldingene i brannmurer eller rutere.

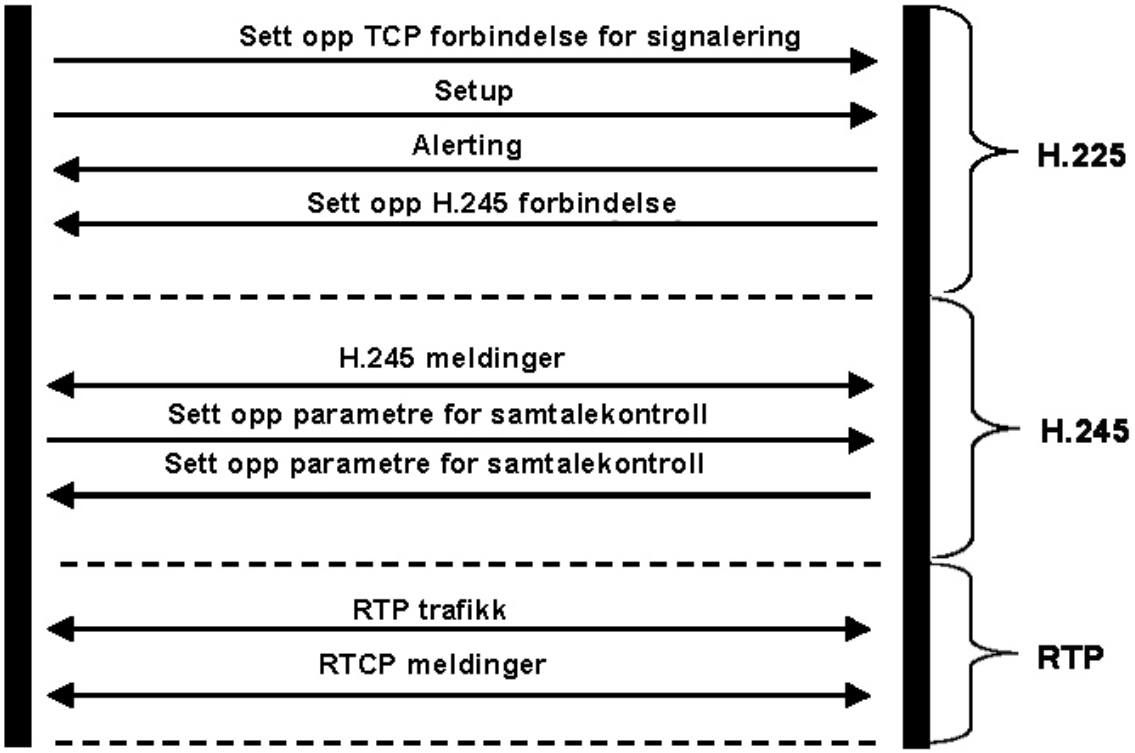
4.3 Transport Layer Security (TLS)

IETF omtaler i RFC3261 TLS som den foretrukne mekanismen for signalering mellom proxyservere, registerservere og for å beskytte SIP signaleringen. Ved å benytte TLS sikrer en konfidensialitet og integritet for signaleringstrafikken. Det anbefales også at det settes opp TLS forbindelser ut til brukeragentene. Hvis brukeragent A sender en SIP INVITE der det kreves bruk av TLS må forbindelsen settes opp med TLS helt ut til brukeragent B. Fordi de mellomliggende nodene kan være nødt til å modifisere innholdet i headerfeltene kreves det at det settes opp TLS forbindelser mellom hver enkelt av de ulike nodene. Det er altså ikke mulig å benytte en enkelt TLS forbindelse ende-til-ende. En ulempe med TLS i forbindelse med SIP er at den må kjøres over TCP forbindelser og at offentlig nøkkeldistribusjon må benyttes. TLS er kanskje mest kjent for å være benyttet i forbindelse med http protokollen, da vil sikker http spesifiseres med https. En lignende notasjon finner en i forbindelse med SIP der en kan indentifisere TLS ved at sip beskrives som sips i headerfeltet til sip meldingene.

5 Sikkerhetsmekanismer i forbindelse med H.323

Siden de aller fleste norske tilbydere benytter seg av SIP, vil denne gjennomgangen av sikkerhetsmekanismene i H.323 bli noe mindre omfattende. H.323 fra ITU-T har et egen definert standard for sikkerhetsprofiler, denne standarden har fått navnet H.235. Siden den første utgaven i ble utgitt 2000 har det kommer to nye versjoner og en rekke tillegg til hver av disse versjonene.

Figur 5-1 "Oppsett av samtale ved bruk av H.323" modifisert fra [8]



Figuren viser oppsett av en H.323-samtale. Her ser vi at protokollene H.225, H.245, og RTP benyttes. Disse er nærmere beskrevet i kapittel 2.2. Sikkerhetsprofilen H.235 definerer anbefalte sikkerhetsmekanismer for hver enkelt av disse protokollene. Her vil hovedvekten ligge på versjon2, da versjon 3 fortsatt ikke er fullt tatt i bruk.

5.1 H.235 Versjon 2

H.235v2 Annex D – Baseline Security Profile
Denne versjonen baserte seg bruken av symmetriske nøkler for å sørge for autentisering og meldingsintegritet. Dette gjorde den lite skalerbar for større nettverk siden det fordi det ikke fantes noen gode mekanismer for hvordan passordene skulle distribueres. Denne versjonen er derfor egnet for mindre nettverk der det er mulig å kontrollere alle H.323-enhetene.

H.235v2 Annex E – Signature Security Profile
Her benyttes det asymmetriske nøkler. Sertifikater og digitale signaturer benyttes for å sørge for autentisering og meldingsintegritet. På grunn av det nå baseres på offentlig nøkkeldistribusjon isteden for forhåndsdelte nøkler vil denne modellen være mer skalerbar for større globale miljøer.

Tabell 5-1 "Sikkerhetsmekanismer i H.323v2 Annex F" modifisert fra [8]

	H.225	H.245	RTP
Autentisering	SHA1/MD5, digitale signaturer	SHA1/MD5, digitale signaturer	
Integritet	SHA1/MD5, digitale signaturer	SHA1/MD5, digitale signaturer	
Nøkkeldistribusjon	PKI	PKI	

H.235v2 Annex D - Voice Encryption Option
Hovedpoenget med dette tillegget var å definere muligheter for å kryptere tale.

Tabell 5-2 "Sikkerhetsmekanismer i H.323v2 Annex D" modifisert fra [8]

	H.225	H.245	RTP
Integritet			56 bit DES, RC2, 168-Bit 3DES, AES
Nøkkeldistribusjon	Diffe-Hellmann	Distribuering av sesjonsnøkler	

Her utveksles det en hovednøkkel under oppsettet av sesjonen ved hjelp av H.225 protokollen. Fra denne hovednøkkelen deriveres det sesjonsnøkler som utveksles under samtalekontroll meldingene i H.245. Det er altså mulig å kryptere taletrafikken(RTP) ved hjelp de ulike algoritmene i tabellen over.

H.235v2 Annex G – Hybrid Security Profile

Tabell 5-3 ”Sikkerhetsmekanismer i H.323v2 Annex G” modifisert fra [8]

	H.225	H.245	RTP
Autentisering	RSA digitale signaturer, SHA1	RSA digitale signaturer, SHA1	
Konfidensialitet			
Integritet	RSA digitale signaturer, HMAC-SHA1-96	RSA digitale signaturer, HMAC-SHA1-96	
Nøkkeldistribusjon	Sertifikat allokering, Diffie-Hellmann	Sertifikat allokering, Diffe-Hellmann	

I tillegg til tideligere mekanismer benyttes her asymmetriske metoder for autentisering og integritet realisert ved bruken av RSA. I tillegg benyttes HMAC-SHA1-96 som gir en bedre integritet enn tideligere algoritmer.

Som en ser finnes det ingen egne mekanismer for konfidensialitet i forbindelse med signalering i H.323. I likhet med SIP vil det derfor være en mulighet til å benytte TLS i forbindelse med oppsett av sesjoner for å sikre konfidensialitet av trafikken.

5.2 H.235 versjon 3

Dette er et rammeverk som er under utvikling med tanke på å forbedre blant annet problemene som oppstår når H.323 skal kombineres med NAT og brannmurer. Versjon 3 tar også opp implementasjon av SRTP kombinert med MIKEY. Dette vil bli nærmere omtalt i kapittel 7.

6 Generelle sikkerhetstiltak

I dette kapitelet beskrives en del sikkerhetstiltak som kan benyttes i tillegg til mekanismene som ble nevnt i kapittel 4 og 5 i forbindelse med H.323 og SIP. Tiltakene som her beskrives går mer inn på hvordan et nettverk som skal benytte bredbåndstelefoni bør settes opp.

6.1 Skille mellom data- og taletrafikk

Det er mange gode argumenter for at data- og taletrafikk bør håndteres på to logiske ulike nettverk. Blant disse faktorene er Qualtiy of Service (QOS), skalerbarhet, håndterbarhet og sikkerhet. Ved å logisk skille data og taletrafikk vil en altså oppnå økt sikkerhet. Det vil være en lite sannsynlig og sannsynligvis en kostbar affære for de ulike tilbydere å bygge ulike fysiske nettverk for å skille ut mellom disse to ulike trafikktypene. Isteden benyttes det derfor en del ulike teknikker for å segmentere trafikken. Eksempler på dette er implementasjon av Virtuelle LAN (VLAN)og brannmurer med tilstandskontroll. På denne måten blir det mulig å skille trafikken på IP-laget. VLAN er i seg selv ingen garanti for sikkerhet innen VoIP, men er et godt alternativ for å skille trafikk uten å benytte to ulike fysiske nettverk. Innenfor området sikkerhet er dette ønskelig for å redusere faren for angrep. Dessuten vil en få mindre forsinkelser i nettverket når talepakkene slipper å konkurrere med datapakkene om båndbredde og ressurser i svitsjer og brannmurer.

Når en har klarte å skille data og taletrafikk vil det fortsatt være en del tifeller der trafikk mellom IP og datanettverket er nødvendig. Eksempler på dette kan være:

- Når telefonbrukeren i VoIP segmentet skal kontakte servere med talepostkasser i datanettverket enten for å legge igjen beskjeder til andre eller lytte på egne beskjeder.
- Når proxyserveren i VoIP segmentet skal hente oppdateringer eller kommunisere med servere som ligger plassert i datanettverket.
- Når IP telefoner må kontakte servere i datanettverket for å sette opp samtaler.

For å ha kontroll på trafikken mellom data og talenettet kan mulige alternativer være å benytte såkalte Network Intrusion Detections Systems (NIDS) eller å bruke brannmurer.

6.2 Network Intrusion Detections Systems (NIDS)

NIDS er et verktøy for direkte å identifisere ulike typer angrep [7]. NIDS inneholder mekanismer for å varsle et system mot angrep for deretter å isolere angrepet slik at systemet blir beskyttet. I motsetning til tradisjonelle brannmurene som inspiserer en og en pakke vil NIDS overvåke et større spekter av både innkommende og utgående pakker. Siden talerafikk er sensitiv ovenfor forsinkeleser i trafikken er NIDS mer gunstig enn brannmurer med tanke på at den kun overvåker trafikkmønsteret og dermed ikke forsinker trafikken som kan være tilfelle ved bruk av brannmurer.

NIDS vil typisk plasseres i svitsjer og er ment som et supplement til brannmurer, ikke et alternativ. NIDS bør plasseres mellom data og trafikknettverket. Ved å studere trafikken forsøker NIDS å finne kjennetegn på mulige angrep. Slike kjennetegn omtales ofte som angrepssignaturer. Hvis NIDS oppdager at trafikken fra en gitt kilde inneholder kjennetegn på angrep vil all trafikk fra denne kilden blokkeres. Virkemidler for å blokkere slike angrep kan være å koble ned TCP forbindelser som er satt opp eller å blokkere UDP trafikken mellom tale og datanettverket.

NIDS er et verktøy som er utviklet med tanke på datatrafikk og mangler derfor en del sikkerhetsmekanismer for direkte bruk for å beskytte taletrafikk. NIDS er derfor foreløpig best egnet til å beskytte mot angrep som har felles signaturer både for data og taletrafikk, eksempler på slike angrep er tjenestenektingsangrep og utnyttelser av protokoll svakheter.

6.3 Brannmurer

Brannmurer gir en del utfordringer når de kombineres med implementasjon av bredbåndstelefoni. Dette gjelder spesielt i forbindelse med etablering av sesjoner og trafikk som skal traverser gjennom porter som er dynamisk satt opp.

Som vist i kapittel 2 vil RTP trafikken som transporterer tale benytte seg av UDP. UDP benytter dynamiske partall som portnummre i intervallet [1024-65534], så det vil medføre en sikkerhetsrisiko hvis brannmuren tillatter trafikk på alle disse ulike portnummrene inn mot et nettverk. En mulig for å løse dette problemet er å bruke brannmurer med tilstandskontroll. Ved å plassere bredbåndstelefoner bak en slik brannmur vil en altså få muligheter til å sortere

trafikken på andre premisser en kun portnummre. En vil dermed være bedre sikret mot ulike angrep, som for eksempel tjenestenektingsangrep.

6.4 Network Address Translation (NAT)

Network Address Translation (NAT) benyttes innenfor et lokalnett slik at enhetene som er på dette nettverket deler en felles IP-adresse ut mot omverdenen. En slik løsning har flere fordeler, blant annet gir det en bedre utnyttelse av adresserommet. Dette er en fordel fordi det er knapphet på IPv4 adresser. NAT gir også bedre sikkerhet innenfor et lokalnettverk siden det kun er en IP-adresse som kan angripes og at alle angrep må gå gjennom en sentral node. NAT har åpenbart mange fordeler, men bredbåndstelefoni kombinert med NAT er har endel utfordringer som må løses. Detter gjelder spesielt i forbindelese med innkommende anrop og samtalekvalitet på grunn av forsinkelser.

For at innkommende samtaler skal komme gjennom et system som benytter NAT og en brannmur må det åpnes flere porter som potensielt kan bli et sikkerhetsproblem. En ekstern enhet som prøve å kontakte en telefon i et slikt system må vite både den eksterne IP-adressen og portnummeret i brannmuren.

Et annet problem er at tale er sensitiv for forsinkelse. Og dette kan bli et problem når all trafikken må sendes gjennom en sentral node. Når NAT er nødt til å inspisere pakkene og oversette adressene medfører dette en høy prosesseringsbelastning. , og dette kan utnyttes av programvare som ønske å sabotere trafikken ut eller inn fra nettverk. Selv om båndbredden inn til nettverket er bra vil en stor mengde av små RTP pakker gjøre at det blir en så stor belastning på brannmuren at taletrafikken forsinkes.

6.5 Application Level Gateways (ALG)

ALG benyttes i brannmurer for å analysere trafikken på applikasjonsnivået. Ved å implementer ALG blir det mulig å inspisere trafikken og dermed dynamisk åpne og lukke de nødvendige portene. I forbindelse med taletrafikk som skal benyttes sammen med NAT og Brannmurer er ALG nødt til å modifisere innholdet i headerfeltet og meldingskroppen til SIP eller H.323 meldingene. På denne måten kan ALG forandre den eksterne IP-adressen til den korrekte IP-adressen på det interne nettverket. Ulempen ved å benytte ALG er at dette kan bli en flaskehals i nettverket siden all trafikken må inspiseres.

6.6 Samarbeid mellom proxyserver og brannmur

Denne løsningen benytter proxyserveren til å foreta mange av de samme oppgavene som ALG. Proxyserveren er en egen enhet som befinner seg utenfor brannmuren i motsetning til ALG som befinner seg i brannmuren. En slik løsning vil innebære ett tett samarbeid mellom proxyserveren og brannmuren. Proxyserveren sitter inn med data om hvilke enheter bak brannmuren som er i samtaler eller har initiert samtaler. Proxyserveren formidler denne informasjonen til brannmuren vil brannmuren har ha mulighet for å slippe gjennom trafikk til enheter som befinner seg i samtaler og samtidig blokkere ulovlig trafikk inn mot enheter som ikke har registrerte samtaler.

6.7 ESP i ”tunnelmodus”

Ved å benytte implementasjoner av IPsec vil det være mulig for trafikken å passere gjennom NAT i begge retninger. Selv om denne løsningen vil medføre en del overhead kan den benyttes sammen med taletrafikk.

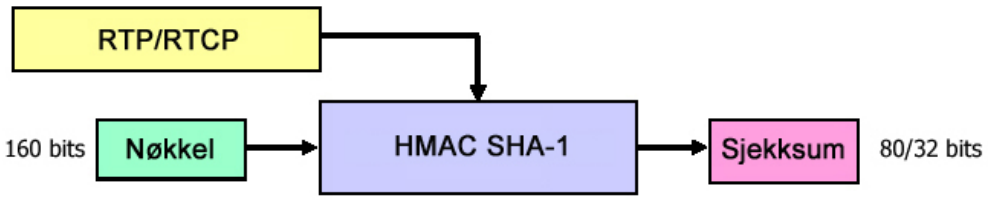
7 Secure Real Time Protocol (SRTP)

SRTP er et forholdsvis nytt rammeverk som tilbyr kryptering og autentisering av RTP/RTCP meldinger og sørger dermed også for konfidensialitet og integritet for RTP trafikken. SRTP skal også gi muligheter til å periodisk bytte ut nøkler og oppgradere algoritmer slik at systemet blir mindre utsatt for å knekkes av potensielle angripere.

7.1 Autentisering

SRTP benytter seg av en kryptografisk sjekksum for å autentisere RTP pakker. Denne sjekksummen beregnes fra både headerinnholdet og hoveddelen av RTP pakken. Vanligvis settes det av 10 byte til autentisering i en SRTP melding, men denne størrelsen kan reduseres.

Figur 7.1 "SRTP Autentisering" modifisert fra [31]

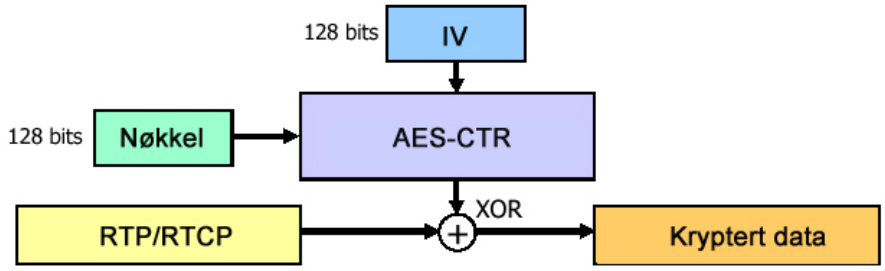


Her ser vi hvordan en SRTP danner et autentiseringsstempel ved å kombinere RTP/RTCP pakker med en hemmelig nøkkel og en krypteringsalgoritme. Resultatet blir en sjekksum som henges på som et vedlegg i SRTP pakken. Denne autentiseringen vil hindre at ikke autoriserte brukere ubemerket kan endre på pakkene som sendes. Algoritmen HMAC-SHA-1 er standardalgoritmen for SRTP autentisering, men andre algoritmer kan benyttes.

7.2 Kryptering

SRTP setter ingen begrensinger på hvilken krypteringsalgoritme den kan brukes sammen med. Men Advanced Encryption Standard in Counter Mode (AES-CTR) er definert som en standard og vil mest sannsynlig bli den mest brukte algoritmen.

Figur 7.2 ”SRTP Kryptering” modifisert fra [31]



Figur 7.2 gir viser hvordan AES-CTR kryptering gjennomføres. Algoritmen kombinerer en 128 bits initieringsvektor og en 128 bits nøkkel med innholdet i RTP/RTCP pakken for å danne en kryptert datastrøm. Ved bruke av AES-CTR vil den krypterte datastrømmen være av typen ”stream cipher” og har to klare fordeler:

- Den krypterte datastrømmen trenger ikke å deles opp i blokker og vi slipper dermed å legge inn ekstra byte i datastrømmen for å skille mellom disse blokkene.
- Mye av prosesseringen kan gjøres unna før vi kjenner innholdet av RTP/RTCP pakkene.

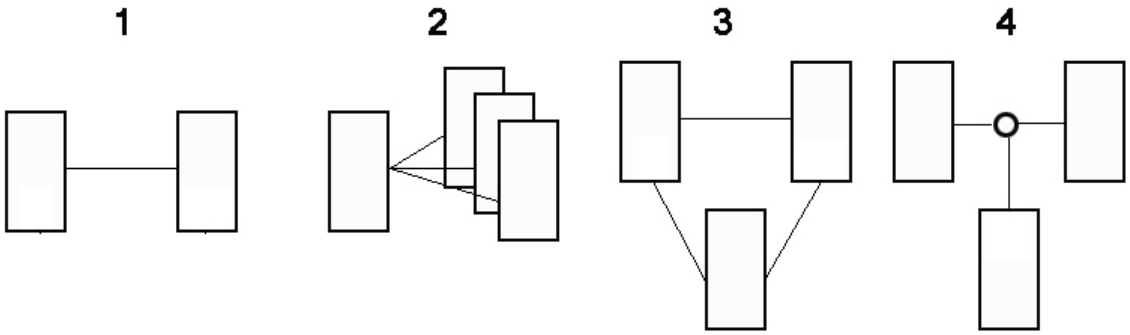
SRTP benytter seg av symmetriske nøkler både til kryptering og autentisering, det vil si at både mottaker og avsender er nødt til å oppbevare den samme nøkkelen. Disse symmetriske nøklene genereres fra en felles hovednøkkel som på forhånd er distribuert ut til deltakerne i en sesjon.

SRTP er ikke bundet opp mot noen spesielle standarder for håndtering av nøkler, men SRTP er tiltenkt å benyttes i kombinasjon med Multimedia Internet Keying(MIKEY) som IETF nå jobber med å standardisere. Session Description Protocol (SDP) har mekanismer for å overføre nøkler til SRTP sesjoner, men SDP meldingene er ikke krypterte. I påvente av MIKEY rammeverket kan derfor SDP over en kryptert forbindelse, satt opp med S/MIME, TLS eller IPSEC, benyttes til å overføre SRTP sesjonsnøkler.

7.3 Multimedia Internet Keying(MIKEY)

MIKEY er et nytt rammeverk for nøkkelutveksling som er beskrevet i RFC3830 fra IETF. MIKEY har en del til felles med Internet Key Exchange (IKE) som benyttes i forbindelse med IPsec, men MIKEY er tilpasset sanntidsapplikasjoner. Bakgrunnen for et nytt system er at det er ønskelig med et enklere system med mindre forsinkelse i forbindelse med nøkkelutveksling eller nøkkeloppdatering. MIKEY skal kunne benyttes sammen sanntidsapplikasjoner eller andre former for multimediaapplikasjoner, men er først og fremst tiltenkt å benyttes sammen med SRTP. Det beskrives det fire ulike bruksområder hvor MIKEY nøkkelutveksling kan benyttes:

Figur 7.3 "Ulike bruksområder for MIKEY" modifisert fra [16]



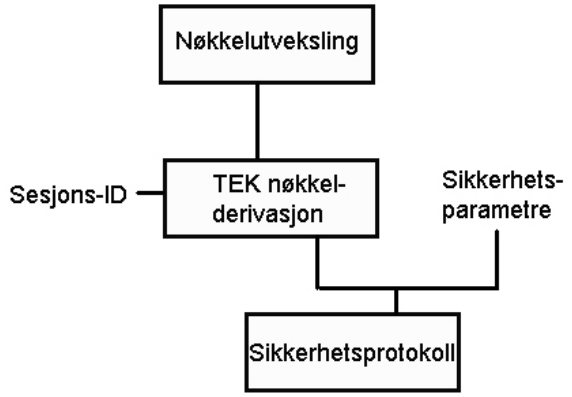
1) "Peer-to-Peer" (Unicast): Her defineres sikkerheten etter en felles avtale mellom to entiteter som ønsker å kommunisere. Det er også mulig at hver entitet selv definerer hvilke sikkerhetsparametere som skal gjelde for sin egen utgående mediastrøm.
2) "En til mange" (Multicast): Her er det senderen som er ansvarlig for sikkerheten.
3) "Mange til mange": En løsning der medlemmer innenfor små grupper setter opp sine egne sikkerhetsparametere for sin utgående mediastrøm.
4) "Mange til mange med en sentralisert kontrollenhet": For større grupper der en enhet fungerer som en kontrollenhet som setter opp sikkerhetsparametere for de andre deltakerne i gruppen

MIKEY støtter oppsett av ulike kryptografiske nøkler og sikkerhetsparametere for en eller flere sikkerhetsprotokoller. Dette er spesielt nyttig for SRTP der det kan være behov for å benytte ulike sikkerhetsparametere for RTP og RTCP pakkene.

MIKEY støtter ulike metoder for utveksling av nøkler og sikkerhetsparametere:

1) Delte sesjonsnøkler.
2) Bruk av offentlig nøkkeldistribusjon.
3) Diffie-Hellman.

Figur 7.4 "Oppsett av MIKEY sikkerhetsprotokoll"



Det benyttes en traffic-encrypting key (TEK) for hver krypteringssesjon. Denne deriveres fra TEK Generation Key (TGK) som partene på forhånd har utvekslet. TEK danner sammen med de ulike sikkerhetsparametrene og sesjons-ID en sikkerhetsprotokoll. Hele denne operasjonen kan gjentas flere ganger. De ulike sikkerhetsprotokollene danner da en Session Bundle (SB).

SRTP pakkene som ankommer mottaker inneholder en Master Key Indentifier (MKI). MKI peker på hvilken sikkerhetsprotokoll som er gjeldende for den aktuelle sesjonen. På mottakersiden vet en da hvilke nøkkel og sikkerhetsparametere som er brukt for å kryptere SRTP trafikken.

8 Informasjon om norske tilbydere

Oktober 2004 sendte Post- og Teletilsynet (PT) ut et høringsbrev til tilbydere av bredbåndstelefoni i Norge [22]. Bakgrunnen for denne høringen var at PT ønsket å hente informasjon fra de ulike tilbyderne om deres implementeringer av bredbåndstelefoni. På denne måten skulle PT skulle være bedre i stand til å se hvilke krav som måtte stilles til tilbyderne med hensyn på regulering. I dette kapittelet vil en del av svarene fra de ulike tilbyderne bli gjennomgått. Svarene danner et visst bilde av hvordan situasjonen for bredbåndstelefoni er i dag og særlig informasjonen om nødanrop og kommunikasjonskontroll er nyttig. Dette er områder det ellers har vært vanskelig å finne konkret informasjon om, da de ulike norske tilbyderne er noe tilbakeholdne på å gi ut detaljer om sine løsninger for bredbåndstelefoni. Høringen fra PT inneholder mange punkter men i dette kapittelet vil det bli fokusert på nødanrop, kommunikasjonskontroll og sikkerhetsmessige aspekter fra de fem tilbydere Telio [26], Tele2 [27], Telenor [25], NexGenTel [23] og Lyse Tele [24].

8.1 Nødanrop

Denne tjenesten omtales i Ekomloven og her er noen av kravene som stilles denne tjenesten:

- Ekomloven forutsetter at bruker av offentlig telefontjeneste skal kunne foreta anrop til nødnumre fra sin telefon.
- Slike anrop skal formidles vederlagsfritt.
- Nødanrop skal i utgangspunktet formidles til den nødmeldingssentralen som har ansvar for å besvare anrop fra den kommunen det ringes fra. Dette gjøres ved at nødnummer 110, 112 og 113 konverteres til vanlig 8-sifret nummer som benyttes for videre dirigering av anrop til Telenor som formidler disse til nødmeldesentralen.
- Anrop til nødnummer skal kunne skje på en slik måte at nødmeldesentralen som anropes også mottar informasjon om hvilket nummer det ringes fra, hvilken adresse (fasttelefon) eller hvilket geografisk område (mobiltelefon) det ringes fra. Denne funksjonen kalles opprinnelsesmarkering og skal bidra til at nødmeldesentralen kan dirigere hjelp til korrekt adresse, selv om oppringer ikke klarer å gi informasjon om dette selv.

Tabell 8.1 ”Informasjon om nødanrop” basert på [23]-[27]

Tilbyder	Informasjon om nødanrop
Telio	For mobile/nomadiske VoIP tjenester vil man på kort sikt ikke kunne overføre korrekt opprinnelsesmarkering. Som et midlertidig alternativ anbefales det at kunden gjøres oppmerksom på at opprinnelsesmarkeringen ikke vil være korrekt når man benytter tjenesten utenfor fast adresse. Man kan også legge inn info i opprinnelsesmarkeringen om at samtalen kommer fra en mobil/nomadisk tjeneste.
Tele2	Når kunden kan benytte IP-telefonitjenesten fra andre steder enn den faste adresse som kunden har oppgitt til operatør, finnes det ingen løsning i dag, etter det Tele2 er kjent med. En operatør vil kunne oppgi den faste adressen til nødsentralene, men kan ikke garantere at kunden kun vil ringe fra denne adressen. Kundene må bli informert om at opprinnelsesmarkering til nødsentralene ikke vil fungere dersom tjenesten benyttes andre steder enn den faste adresse som er oppgitt til tilbyder.
Telenor	Det er som kjent ingen gode kortsiktige løsninger for opprinnelsesmarkering ved alle typer av IP-telefoni.
NextGentel	Det er ingen fundamentale egenskaper ved IP-baserte telefonitjenester som skulle være til hinder for å tilby opprinnelsesmarkering i henhold dagens regelverk.
Lyse Tele	Dette lar seg realisere, og det er kun snakk om økonomiske midler. En bør tilstrebe en mer operatørvennlig måte å håndtere dette på enn dagens, men dette er jo et arbeid som pågår.

Som vi ser av tabellen blir opprinnelsesmarkering først et problem når kunden tar med seg adapteret for IP-telefoni til en annen adresse en den som er oppgitt hos tilbyder. Dette kalles nomadisk bruk av bredbåndstelefoni. Dette er ikke et veldig utbredt fenomen i dag da de fleste brukere ser på bredbåndstelefoni som en erstatning for fasttelefoni dermed kun benytter telefonen innenfor sin egen husstand. Men problemet blir økende med flere tilgjengelige tilknytningspunkter for bredbåndsaksess. Økning av trådløse hotspots kombinert med trådløse bredbåndstelefoner vil sannsynligvis gi en kraftig økning i nomadisk bruk av bredbåndstelefoni. Det kan selvsagt diskuteres om det er naturlig at en bruker skal kunne forlange at nødsentralen skulle kunne være i stand til å finne ut hvor kunden ringer fra hvis kunden forflytter seg rundt på forskjellige steder med IP-adapteret sitt. Men PT mener uansett at dette er et problem som må håndteres av de ulike tilbyderne.

PT har foreløpig gitt tilbyderne dispensasjon fra kravet om opprinnelsesmarkering i påvente av at de ulike partene blir enige om en teknisk løsning for dette. For at tilbyderen skal innvilges dispensasjon stilles det imidlertid visse krav fra PT, noe forenklet er de som følger:

- Tilbyderne skal kunne dokumentere at det konkret jobbes med å finne løsninger på utfordringene i forbindelse med nødanrop og nomadisk bruk av bredbåndstelefoni.
- Tilbyderne er pliktige til å informere sine kunder om problemet med nødanrop ved nomadisk bruk av bredbåndstelefonen.
- Tilbyderne skal registrere sine kunders hjemmeadresser og formidle denne informasjonen til nødmeldesentralen ved nødanrop.

Den løsningen som går igjen fra tilbyderne sin side er at nødsentralene får opplysniger om adressen til eieren av nummeret, men tilbyderne kan altså ikke garantere at samtalen kommer fra denne adressen. Foreløpig ser det derfor ikke ut til at noen tekniske løsninger for opprinnelsesmarkering ved nomadisk bruk av bredbåndstelefoni. Derfor blir det viktig for de ulike tilbyderne å tydelig informere sine kunder om dette problemet. Dette utdraget fra Telenor sine hjemmesider [20] illustrer dette:

Figur 8.1 "Kundeinformasjon fra Telenor sine hjemmesider" fra [20]

Du har ikke lov til å bruke din tilgang til bredbåndstelefoni fra andre adresser enn den vi har registrert for ditt Online ADSL-abonnement. Nødetater skal kunne identifisere adressen du ringer fra, og med bredbåndstelefoni foregår dette ved at Telenor utleverer opprinnelsesmarkering basert på den adressen som til enhver tid er registrert på deg. Dersom du skal flytte vennligst kontakt kundeservice på 05000.

Her legger Telenor inn restriksjoner på nomadisk bruk av bredbåndstelefoni ovenfor sine kunder. Fra dette vil det være naturlig å tolke at Telenor ikke har noen tekniske løsninger på hvordan en skal hindre nomadisk bruk av bredbåndstelefoni.

8.2 Kommunikasjonskontroll

Ifølge PT har tilbydere plikt til å tilrettelegge for kommunikasjonskontroll. Begrepet kommunikasjonskontroll omfatter tilgang til informasjon om hvem som prater sammen, når samtalen foregår, hvor de ulike samtalepartene befinner seg og innholdet i samtalen. Alle tilbydere av bredbåndstelefoni plikter å tilby slik kommunikasjonskontroll.
Som nevnt i forrige kapitel om nødanrop kan det være vanskelig å eksakt bestemme lokasjonen til deltakerne i en samtale, men dette er ikke den største utfordringen innen kommunikasjonskontroll. Hovedutfordringen innen kommunikasjonskontroll dreier seg i hovedsak om å være i stand til å tilby avlytting av samtaler.

Tabell 8.2 "Informasjon om kommunikasjonskontroll" basert på [23]-[27]

Tilbyder	Informasjon om kommunikasjonskontroll
Telio	Det vil være mulig å gjennomføre kommunikasjonskontroll for VoIP tjenester som omfatter transport av elektronisk kommunikasjon. For tjenester der dette ikke er en del av tjenesten vil det ikke være mulig å gjennomføre kommunikasjonskontroll fullt ut. Sluttbrukere som ønsker å sikre seg mot kommunikasjonskontroll vil med enkle midler kunne gjøre dette på eget initiativ.
Tele2	Kravspesifikasjon fra politiet mangler foreløpig. Det kan bli benyttet koding av samtaler noe som vil vanskeliggjøre kommunikasjonskontrollen. Ansvaret mellom ISP og tilbyder av IP-telefoni bør klarlegges i forhold til kommunikasjonskontroll. Etter Tele2s syn ligger ansvaret for kommunikasjonskontroll av IP-telefoni på operatøren av IP-telefoni og ikke på ISPen.
Telenor	Det er fremdeles uklart hvordan kravene skal praktiseres. Det er viktig at man velger hensiktsmessige tekniske løsninger.
NextGenTel	Dette vil i stor grad avhenge av hvilken implementering man velger for sin IP-baserte telefonitjeneste. Det er teknisk mulig – men ingen selvfølge – at man sørger for at alle samtaler settes opp via sentrale node i nettet for å sikre muligheter for kommunikasjonskontroll. Utover det har IP-baserte tjenester i prinsippet de samme muligheter og begrensninger som ISDN.
Lyse Tele	For avlyttingsformål er det også i utgangspunktet mulig å realisere, men vil kreve ikke ubetydelige økonomiske midler for operatøren å realisere et slikt behov. Det er helt klart behov for en "standardisering" i forhold til en slik funksjon, da dette i mange sammenhenger kan være plattformspesifikt. Det vil også kunne være utfordringer knyttet enkelte protokoller og kryptering av disse, som gjør at kommunikasjonskontroll vanskeliggjøres, sågar umuliggjøres.

Skal en tolke svarene fra de ulike tilbyderne kan det konkluderes med at det ennå ikke foreligger noen konkrete krav fra Post- og teletilsynet om hvordan kommunikasjonskontroll skal gjennomføres. Dette er også avhengig av hvilke metoder for kryptering de ulike tilbyderne benytter. Hvis trafikken kun kjøres som ukryptert RTP trafikk vil dette ikke være noe problem for tilbyderne å tilby kommunikasjonskontroll, da tilbyderne selv bestemmer hvilken talekoding som skal brukes og tilbydere har også tilgang til servere eller gatekeepere. Problemet med RTP er da at det også vil være tilsvarende enkelt for mulige angripere å avlytte samtalen.. Hvis det benyttes kryptert trafikk som SRTP eller IPsec for å beskytte RTP-pakkene vil det være naturlig å anta at tilbyderen har kjennskap til hvilke nøkler og algoritmer som benyttes av de ulike brukerne. Ved for eksempel å ha et register over disse vil tilbyderne være i stand til å avlytte en samtale.

Et annet problem i forbindelse med kommunikasjonskontroll som blant annet nevnes av Telio er at brukerne selv kan ta initiativ til å kryptere samtalen. Dette vil helt klart gjøre det vanskelige eller umulig å avlytte samtalen da bruken av krypteringsalgoritmer og nøkler ikke er kjent for tilbyderen.

Hvor tilbyderne velger å legge krypteringsfunksjonaliteten og hvilke nett samtalen foregår på vil også spille en vesentlig rolle i forbindelse med avlytting. Voice over Public Internet (VoPI) er en benevnelse som beskriver varianten der taletrafikken sender over det Internett og ikke i tilbyderen sine egne nettverk. Ved å benytte seg av VPN tunneler på denne delen av samtalen over vil tilbyderen kunne tilby en sikker overføring av samtalen for kunden samtidig med at avlytting av samtalen fortsatt er mulig for tilbyderen. Slike løsninger vil være enklere for tilbydere som fungerer både som tilbyder av bredbånd og bredbåndstelefoni da de selv har kontroll på linjene. Det er imidletid klart at overgangen til bredbåndstelefoni har gjort kommunikasjonskontroll mer komplisert.

8.3 Sikkerhetsmessige aspekter

Her ble de ulike tilbyderne spurt om hva slags sikkerhetsutfordringer de oppfattet som de mest relevante for bredbåndstelefoni.

Tabell 8.3 "Informasjon om sikkerhetsutfordringer" basert på [23]-[27]

Tilbyder	Sikkerhetsutforinger
Telio	• Ikke enig i at bredbåndstelefoni er mer sårbar enn tradisjonell fasttelefoni med hensyn med hensyn på urettmessig innsyn, driftsforstyrrelser eller urettmessig avlytting. • Det som er forskjellig fra tradisjonell teknologi er hva som må/kan sikres og metodene som benyttes for å gjennomføre slik sikring. • Faktum er at VoIP kan være mer sikkert enn tradisjonelle tjenester på grunn av at det faktisk eksisterer metoder for sikring av tilgang, signalering og kommunikasjon. Dette er ett eksempel på nye egenskaper ved VoIP som er nyttig både for sluttbruker og leverandør.
Tele2	Ingen bemerkninger
Telenor	• Tjenestenektingsangrep(DoS og Distribuert DoS) • Virus/Trojanere • Tilgjengelighet • Ulovlig bruk av nettet til samtaler
NextGenTel	For sentrale funksjoner er IP-baserte løsninger samelignbare med dagens ISDN-løsninger. Begge er basert på teknologi som kan angripes (hackes) av uvedkommende dersom sikring er for dårlig. Generell sikring og herding av servere, brannmurer og lignende er her nøkkelfaktorer. I forhold til kommunikasjonslinjer på aksessnivå kan disse selvsagt avlyttes fysisk både i ISDN- og IP-baserte løsninger. Teknologi for dette er kjent og kommunikasjonsprotokoller er kjent. På stamnettnivå vil dette være mer komplisert og i de fleste tilfeller ikke praktisk mulig
Lyse Tele	For Lyse Tele sitt vedkommende er telefonistrukturen atskilt fra internett tjenestene, blant annet for å ivareta de sikkerhetsmessige og kvalitetsmessige aspekter ved tjenesten. Dette betyr at tjenesten ikke fremstår som utpreget sårbar og gir heller ikke noen lettvinte metoder for avlytting. Dersom en bruker internett som bærer vil dette fortone seg vesentlig annerledes, og kan gi uønskede effekter. Det bør derfor klart skilles mellom systemer som bruker og som ikke bruker "internett" som bærer.

Fra tabellen ser en at de ulike tilbyderne har litt ulike innfallsvinkler på hva som sikkerhetsutfordringene for bredbåndstelefoni, Tele2 har for eksempel ikke listet opp en eneste sikkerhetsutfordring og Telio mener at VoIP kan gjøres mer sikkert tradisjonelle tjenester. Lyse Tele har skilt bredbåndstelefoni fra de andre datatjenestene, noe som tideligere er nevnt i denne oppgaven som en mulighet for å bedre sikkerheten for brukerne av taletjenestene. Ellers ser det ut til å være enighet om at tradisjonelle angrep mot et IP-nettverk som Virus, avlytting(pakkesniffig) og tjenestenektingsangrep også oppfattes som reelle truser mot bredbåndstelefoni. Det vil derfor være like viktig å beskytte de ulike delene av nettverket mot disse angrepene i forbindelse med bredbåndstelefoni som med vanlige IP-tjenester.

9 Konklusjon

Innenfor området datasikkerhet vil det alltid være en kamp mellom nye trusler og tilsvarende beskyttelse mot disse, dette kan også sies å gjelde for sikkerhet innen bredbåndstelefoni. En vil aldri kunne garantere at et system er ett hundre prosent sikret mot fremtidige angripere og trusler. Til tross for dette er det uansett viktig å ha beskyttelse mot de truslene som allerede finnes, og vite hva som skal til for å i størst mulig grad sikre et system mot potensielle angripere. I denne oppgaven har derfor hoveddelen av arbeidet gått ut på å kartlegge de ulike sikkerhetsutfordringene i forbindelse med bredbåndstelefoni.. I kombinasjon med dette har det også vært gjennomgått ulike teknologier for å implementere bredbåndstelefoni og sikkerhetsmekanismer i forbindelse med disse teknologiene. Oppgaven har samtidig tatt for seg ulike generelle løsninger som i dag finnes for å sikre et nettverk som benyttes til bredbåndstelefoni på en beste mulig måte.

I tillegg til det som nevnes over inneholder rapporten også noe informasjon om norske tilbydere sitt syn på sikkerhet innen bredbåndstelefoni. På bakgrunn av dette er det er vanskelig å komme med noen entydig konklusjon på hvor bra sikkerheten er hos de ulike tilbyderne. På generelt grunnlag kan det sies at det fortsatt er et noe uklart regelverk som tilbyderne må forholde seg til. Det er derfor viktig å få på plass klare retningslinjer for blant annet kommunikasjonskontroll og nødanrop slik at tilbyderne vet hva de har å strekke seg mot. På denne måten blir det lettere for tilbyderne å implementere hensiktsmessige løsninger med tanke på sikkerhet.

Denne rapporten har i stor grad vært utført som et teoretisk studium. En slik tilnærming har vært nyttig i forbindelse med å kartlegge trusler, angrep og tilsvarende mottiltak. Som en påbygging av denne oppgaven kunne det vært interessant og utført en del praktiske tester som et supplement til den teoretiske delen. Et eksempel på en slik test kan være å benytte programmet VOMIT for å se hvor godt ulike former for bredbåndstelefoni er sikret mot avlytting. I tillegg til dette kunne det vært aktuelt og gått mer i dybden på de ulike protokollene og eventuelt utført ulike stresstester mot for eksempel SIP protokollen.

10 Referanser

[1] Alan B. Johnston, SIP: Understanding the Session Initiation Protocol, Second Edition , Artech House Books, 2003

[2] James F. Kurose, Keith W. Ross, Computer Networking, A top-down approach featuring the Internet, Addison Wesley Longman Inc., 2001

[3] William Stallings, Network security essentials, Applications and Standards, Second Edition, Pearson Education, 2003

[4] James F. Ransome, John W. Rittinghouse, VoIP Security,
Elsevier Science & Technology Books, 2004

[5] Elin Wedlund, Henning Schulzrinne: Mobility Support using SIP
http://www.cs.columbia.edu/~hgs/papers/Wedl9908_Mobility.pdf

[6] SecureLogix Corporation: Voice Over IP (VoIP) Denial of Service (DoS)
http://download.securelogix.com/library/dos.pdf

[7] Cisco: IP Telephony Security in Depth
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf

[8] National Institute of Standards and Technology (NIST): Security Considerations for Voice Over IP Systems
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[9] SecureLogix Corporation: Voice Over IP and Firewalls
http://download.securelogix.com/library/voice_over_ip_firewalls_050105.pdf

[10] Senter for informasjonssikring (SIS): Ciscos VoIP-komponent CallManager sårbar for tjenestenektingsangrep
http://www.norsis.no/details.php?type=sarbarheter&id=564

[11] Cisco: Cisco CallManager Memory Handling Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a00804c0c26.shtml

[12] Senter for informasjonssikring (SIS): Sårbarheter i noen IPsec-løsninger
http://www.norsis.no/details.php?type=sarbarheter&id=519

[13] The National Infrastructure Security Coordination Centre: Vulnerability Issues with IPsec Configurations
http://www.uniras.gov.uk/niscc/docs/re-20050509-00385.pdf?lang=e

[14] Protocols.com: Voice over IP Reference Page
http://www.protocols.com/pbook/VoIP.htm

[15] Cisco: Security in SIP-Based networks
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml

[16] Internet Engineering Taskforce (IETF): MIKEY: Multimedia Internet KEYing
http://www.ietf.org/rfc/rfc3830.txt

[17] Packetizer.com: Voip Information Site:
http://www.packetizer.com/voip/

[18] Internet Engineering Taskforce (IETF): SIP: Session Initiation Protocol
http://rfc.net/rfc3261.html

[19] Internet Engineering Taskforce (IETF): The Secure Real-time Transport Protocol (SRTP)
http://rfc.net/rfc3711.html

[20] Telenor: Før du bestiller bredbåndstelefoni
http://privat.telenor.no/telefoni/abonnement/bredbandstelefoni/fordubestiller.go

[21] Cisco: Supported VPN Standards
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278d.html

[22] Post– og teletilsynet: Høring – regulatoriske utfordringer ved IP-telefoni
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/ip-telefoni-brev.pdf

[23] Post– og teletilsynet: Høringssvar fra NextGenTel AS
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/NextGenTel_AS.pdf

[24] Post– og teletilsynet: Høringssvar fra Lyse Tele AS
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/Lyse_Tele_AS.pdf

[25] Post– og teletilsynet: Høringssvar fra Telenor ASA
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/Telenor_ASA.pdf

[26] Post– og teletilsynet: Høringssvar fra Telio AS
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/Telio_AS.pdf

[27] Post– og teletilsynet: Høringssvar fra Tele2 Norge AS
http://www.npt.no/pt_internet/venstremeny/hoeringer/IP/Tele2_Norge_AS.pdf

[28] Post- og teletilsynet: IP-telefoni
http://www.npt.no/iKnowBase/FileServer/ip-telefoni.pdf?documentID=31004

[29] Post- og teletilsynet: Undersøkelse av egenskaper ved bredbåndstelefoni
http://www.npt.no/iKnowBase/Content/rapport.pdf?documentID=44849

[30] Post- og teletilsynet: Regulering av bredbåndstelefoni
http://www.npt.no/iKnowBase/FileServer/prinsipp_bredband.pdf?documentID=44246

[31] Security Group Zürcher Hochschule Winterthur: SIP Security
http://security.zhwin.ch/DFN_SIP.pdf

[32] Foundstone Security: Protecting your network from ARP Spoofing-Based Attacks
http://www.foundstone.com/resources/perspectives/AskTheExpert-200406.pdf

[33] Monkey.ORG : voice over misconfigured internet telephones
http://vomit.xtdnet.nl/