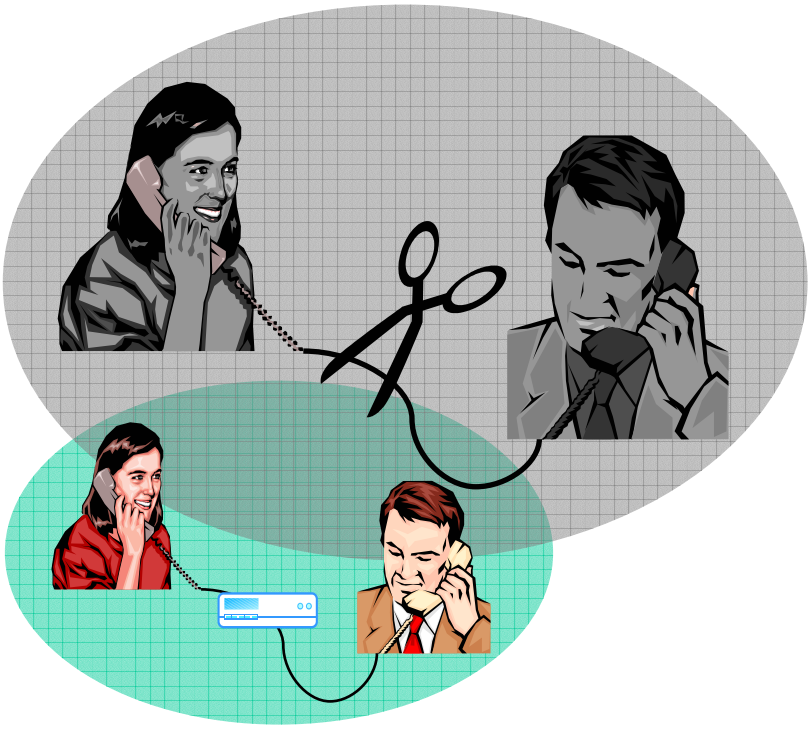
FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--1528--SE
Januari 2005
ISSN 1650-1942
Underlagsrapport

Svante Barck-Holst, Henrik Christiansson, Arne Vidström

IP-telefoni ur ett sårbarhetsperspektiv



Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Försvarsanalys
172 90 Stockholm

FOI-R--1528--SE

Januari 2005

ISSN 1650-1942

Underlagsrapport

Svante Barck-Holst, Henrik Christiansson, Arne Vidström

IP-telefoni ur ett sårbarhetsperspektiv

Innehåll

1 Inledning

1.1 Bakgrund

IP, Internet Protocol, som bärare för telefoni är under stark frammarsch. Många organisationer väljer IP-baserade telefonsystem såväl nationellt som internationellt. IP-telefoni finns även som abonnemangsform för enskilda kunder[1]. Den allt mer spridda användningen av IP-telefoni i samhället har även betydelse för totalförsvaret.

IP-telefoni baserar sig delvis på annan teknik jämfört med etablerade telefonsystem. Existerande system för kretskopplad telefoni är väl utbyggda och mycket arbete har lagts på att få dem säkra, uthålliga och tillgängliga. Byggandet av IP-nät har gått snabbt de senaste åren och IP-telefoni erbjuder nya tjänster och möjligheter, såväl ur ett drifts- och underhållsperspektiv som ur ett användarperspektiv. Tekniken för IP utvecklades ursprungligen i ett syfte att skapa förutsättningar för säkrare dataöverföring. Införandet av IP-telefoni kan därför ha såväl positiv som negativ inverkan på de elektroniska kommunikationernas robusthet och är därmed viktigt att följa ur ett samhälls- och sårbarhets-perspektiv.

Ett exempel på en incident där VoIP funktionen påverkats inträffade i slutet av 2002 och beskrivs i en rapport från Gartner.[2] Masken SQL Slammer som slog mot många datorer som körde konventionella applikationer slog också mot system vid ett call-center som använde VoIP. Användare förlorade tillgång till telefoni och svarstiden försämrades snabbt och inom femton minuter hade alla väsentliga system ”stannat”.

Allt eftersom taltjänster flyttar över till IP nätverk blir säkerhetsverktyg för dessa nätverk av stor betydelse för taltjänstoperatörer. Dessa verktyg utgörs t ex av brandväggar, system för att förhindra intrång, detektionsmodeller, virtuella privata nätverk och antivirusprogramvara.

Gartner[3] bedömer vidare i sin rapport att det är troligt att det under 2006 kommer att dyka upp virus och maskar som slår specifikt mot VoIP-specifika nätverkselement. Under 2007 bedöms kommunikation via VoIP att regelbundet utsättas för tillgänglighetsattacker. Dock underbyggs dessa bedömningar inte speciellt utförligt i rapporten.

Post & Telestyrelsen, PTS, verkar för att alla i Sverige ska ha tillgång till effektiva, prisvärda och säkra kommunikationstjänster. För att göra detta behöver PTS bland annat god kunskap om de elektroniska kommunikationernas användningsområden, egenskaper samt möjliga utvecklingstendenser för dessa.

På uppdrag av PTS har därför FOI studerat IP-telefoni och dess betydelse för samhällets funktioner ur ett sårbarhetsperspektiv.

1.2 Syfte

Denna rapport utgör en av slutprodukterna i studien ”IP-telefoni ur ett sårbarhetsperspektiv”.

---

[1] Enligt Post & Telestyrelsen fanns det 20 000 abonnemang för IP-telefoni i Sverige i juni 2003 och 56 400 abonnemang i juni 2004.

[2] R. Mogull, C. Moore, D. Fraley, R. Goodwin, A. Earley, R. DeLotto, **Strategic Planning SPA-21-3633, Gartner Reserach Note 14 January 2004**, *Predicts 2004: Critical Infrastructure Protection.*

[3] Ibid.

Ett syfte med studien har varit att identifiera trender och utveckling som är relevanta för en sårbarhetsbedömning vid en allmänt ökad användning av IP-telefoni.

Ett annat syfte med studien har varit att bidra till kunskapsuppbyggnad på PTS. Resultaten från studien skall dessutom fungera som underlag för PTS i deras arbete med säkerhets- och beredskapsfrågor inom de elektroniska kommunikationerna.

Målet med projektet har varit

- att ur ett sårbarhetsperspektiv analysera system och tekniska lösningar för IP-telefoni,
- att analysera framtida användning av systemen för IP-telefoni samt bedöma vilka konsekvenser störningar i systemen får och hur dessa kan hanteras,
- att identifiera frågeställningar inom området IP-telefoni som kräver fortsatt bevakning eller utredning.

1.3 Avgränsningar och definitioner

Med IP-telefoni menar vi i denna rapport överföring av tal mellan två punkter i realtid över nät med hjälp av IP. I detta dokument använder vi även förkortningen VoIP (Voice over IP) och menar då IP-telefoni i ovan nämnda bemärkelse.

I rapporten använder vi många gånger begreppet ”traditionell telefoni” för att beteckna kretskopplad telefoni, det vill säga telefoni som inte utgör IP-telefoni.

De systembeskrivningar som görs i dokumentet har som syfte att belysa och värdera sårbarhetsfrågor ur något perspektiv. De kan därför vara ofullständiga eller bristfälliga ur andra perspektiv.

Det kan anses att vi allt för ofta uppehåller oss vid de problem och svagheter som IP-telefoni för med sig och att vi endast i begränsad utsträckning pekar på den nya teknikens fördelar. Vi vill därför tydliggöra att syftet med den genomförda studien har varit att belysa IP-telefoni ur ett sårbarhetsperspektiv, inte att åstadkomma en heltäckande beskrivning av IP-telefoni.

Vi har i inte haft någon speciell inriktning på sårbarhetsfrågor för IP-telefoni vid höjd beredskap. Vi har inte heller beaktat frågor om fysiskt skydd.

1.4 Metod

Arbetet baserar sig på litteraturstudier, intervjuer samt egen analys. Under arbetet har vi pratat med representanter från Aerotech Telub, Avbrottsfria kraftnät UPN AB, Bredbandsbolaget, Cisco, com hem, FRA, Sjöfartsverket, SOS Alarm, Telenor, TeliaSonera, Tjänstemannaförbundet HTF.

2 Exempel på andra arbeten inom området

I detta avsnitt beskriver vi två andra exempel på arbeten som gjorts inom området och som vi anser vara av värde för våra egna studier. Utöver dessa så har ett antal andra rapporter och artiklar studerats inom ramen för projektet.

2.1 Rapport till EU-kommissionen om följderna av en övergång till VoIP

Analysföretaget Analysys levererade i januari 2004 en rapport[4] till EU kommissionen. Rapporten riktar sig till regeringar och föreskrivande myndigheter inom EU och syftar till att identifiera och förklara frågor som rör övergången från publika kretskopplade telefonisystem till IP-baserade nätverk för överföring av tal och tillhandahållande av andra tjänster.

I rapporten delas VoIP[5] in i fem olika typer eller tjänstemodeller. Förutom den rent tekniska aspekten skiljer sig varje typ åt genom att de representerar olika affärsmodeller. Varje typ/modell främjar/främjas av olika aktörer och det finns olika drivkrafter bakom varje modell. De fem olika typerna presenteras nedan:

Kunden gör det själv[6]
I denna modell är det kunderna som med egen hård- och mjukvara själva kopplar upp sig över ett befintligt nät (Internet eller eget lokalt nätverk) och pratar med varandra. Ingen tredje part är alltså direkt inblandad i uppkopplingen. I sin renodlade form innebär denna modell att man inte kan ringa till/från PSTN. Denna form kallas ibland för ”Internet-telefoni”.

Oberoende av Internetoperatör[7]
Denna modell innebär att abonnenterna tecknar avtal med en tjänsteleverantör som tillhandahåller en koppling till PSTN. Via Internet kan sedan abonnenten ansluta sig till tjänsteleverantörens koppling och på så sätt nå det publika telenätet. Abonnentens Internetleverantör är i detta fall inte samma som tjänsteleverantören. Tjänsteleverantören kan här inte ge några garantier för QoS (Quality of Service) eftersom han inte har rådighet över kundens anslutning till tjänsteleverantörens utrustning.

Tillhandahållet av bredbandsleverantör[8]
Den enda skillnaden i denna modell jämfört med den föregående är att Internetleverantören och tjänsteleverantören som tillhandahåller en koppling till PSTN är samma företag. Detta är en viktig distinktion ur ansvarssynpunkt eftersom tjänsteleverantören har rådighet över abonnentens anslutning och på så vis kan ge garantier för QoS.

Internt över företagets eget datornätverk[9]
I detta fall handlar det om företag som använder IP-baserade företagsväxlar och på så sätt kan utnyttja det egna datornätverket för att förmedla telefontrafik inom det egna företaget.

[4] IP Voice and Associated Convergent Services
[5] VoIP – Voice over IP, det vill säga ”tal över IP” alltså taltrafik som förmedlas över IP-nät.
[6] Benämningen i Analysys rapport var: Self-provided consumer.
[7] Independent of Internet access.
[8] Provided by broadband access service provider.
[9] Corporate internal use on LAN/WAN.

Internt i teleoperatörens nät[10]
Här handlar det om att teleoperatörerna internt i sina egna stamnät går över till att använda IP istället för andra protokoll för överföring av trafik.

Denna uppdelning tydliggör ansvarsfördelningen mellan olika aktörer i varje modell. I rapporten diskuteras de olika typerna huvudsakligen ur ett struktur-, marknads- och lagstiftningsperspektiv. Man gör dock ingen djupare analys av sårbarhetsfrågor även om problem med larmnummer känslighet för elstörningar och svårigheter att geografiskt lokalisera uppringande part i telefonsamtal diskuteras.

För vårt vidkommande är den typindelning som görs i Analysys rapport av intresse. Dels för att den tydliggör vilka typer av IP-telefoni som finns. Dels för att typindelningen ger en bra bild av vilka möjliga aktörer som är involverade vid VoIP och vilket ansvar olika aktörer har.

Typmodellerna *Tillhandahållet av bredbandsleverantör* och *Internt över företagets eget datornätverk* är de modeller som idag utgör reella alternativ till den traditionella fasta telefonin, så kallad ”first-line replacement”.

2.2 Amerikanska myndigheters rekommendationer relaterade till VoIP och säkerhet

National Institute of Standards and Technology (NIST) är amerikanska Department of Commerce forsknings- och standariseringsinstitut. De riktlinjer rörande IT-säkerhet som NIST ger ut skall beaktas av civila amerikanska myndigheter. När det gäller VoIP har NIST tagit fram ett utkast till rapport med titeln *Security Consierations for Voice over IP Systems: Recommendations of the National Institute of Standards and Technology*[11] med rekommendationer avseende användningen av VoIP.

Syftet med dokumentet är att ge federala myndigheter och organisationer praktiska riktlinjer för att kunna upprätta säkra VoIP-nätverk. Dock gäller dessa riktlinjer inte för nationella säkerhetssystem (national security systems) som har högre krav. Riktlinjerna ligger också utanför de säkerhetsaspekter som är viktiga för det publika telenätet (PSTN).

I rapporten beskrivs i ett inledande kapitel VoIP på en övergripande nivå i form av vilken utrustning som krävs och hur den logiska pakethanteringen sker samt kostnader för detta och kvalité på tjänsten. Kapitlet avslutas med en diskussion kring säkerhetsfrågor. Där man påpekar att PSTN bygger på att kritisk utrustning skyddas mot fysiskt tillträde. Ett sådant skydd kan man vanligtvis inte tillhandahålla för all utrustning i ett datornätverk eftersom användarutrustningen också är kritisk vid VoIP. För att VoIP-system skall nå samma skyddsnivå som PSTN anser NIST att det krävs satsningar på tillräckligt skydd i form av IT-säkerhetslösningar.

Därefter följer ett kapitel som berör frågor om kvalitén hos VoIP vilket följs av kapitel om olika arkitekturer som H.323 och SIP. Gateways har fått ett eget kapitel.

[10] Carrier internal use.
[11] D. R. Kuhn, T. J. Walsh, S.Fries, *Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology*, NIST National Institute of Standards and Technology, DRAFT Special Publication 800-58

Identifierade IT-säkerhetsproblem diskuteras i ett kapitel med rubriken *Brandväggar, Adressöversättningar (NAT) och upprättande av Samtal* (fritt översatt) där säkerhetsproblem i dessa och mellan dessa koncept och processer.

Kryptering och IPsec har ett eget kapitel där det beskrivs hur detta påverkar kvalitén hos VoIP men också hur dålig kompatibilitet mellan IPsec och NAT påverkar VoIP.

Rapporten avslutas med två kapitel rörande förslag till lösningar på vissa problem samt hur man skall planera för ett införande av VoIP hos t ex en myndighet.

I ett appendix diskuteras risker, hot och sårbarheter i termer av konfidentialitet, riktighet och tillgänglighet (CIA)[12] vilket är de klassiska säkerhetsbegreppen i IT-säkerhetssammanhang. Man kan konstatera att en sådan indelning av de hot och sårbarheter som beskrivs inte fyller någon större funktion. Det räcker med att klargöra att om en angripare skaffar sig tillgång till systemkomponenter kan denne troligtvis uppnå effekter inom alla nämnda CIA-områden.

Nätverk som bygger på paketförmedlad trafik är ofta beroende av ett antal dynamiskt konfigurerbara parametrar exempelvis IP-adresser, default-gateway samt DNS-serveradresser. Dessutom sker mappning mellan IP-adresser och Ethernetadresser[13] dynamiskt. Dynamiska data uppdateras när nätverkskomponenter startar, börjar kommunicera med varandra, men även vid andra tillfällen. En antagonist har möjlighet att utföra olika attacker för att manipulera dynamisk uppdatering av viktiga data.

Några av de problem som VoIP-tjänsten medför på grund av det ovan nämnda och som diskuteras är att:

- Det finns ännu ingen *allmänt accepterad* standard inom området[14]vilket leder till att man bör använda flexibla komponenter som kan anpassas till de olika standarder som finns.
- Införandet av brandväggar i VoIP-nätverket komplicerar flera aspekter av VoIP men framförallt gäller det den dynamiska porthanteringen (dynamic port trafficking) och procedurerna kring uppkopplingen av samtal.
- Inom LAN används Network Adress Translation (NAT) för att öka säkerheten och för att möjliggöra att flera ändpunkter skall kunna dela på samma IP-nummer. Dock medför detta problem för VoIP-tjänsten ur ett säkerhetsperspektiv som ännu inte är helt lösta.
- För att skydda VoIP-tjänsten från t ex otillåten avlyssning använder man sig av olika kryptografiska lösningar. Dessa orsakar dock flera problem i VoIP-tjänster med avseende på till exempel kvalité på talöverföringen.

Några av de mer specifika rekommendationer som ges i rapporten är att

- Man skall separera tal och data på *logiskt* skilda nätverk.
- Vid gateways som kopplar mot PSTN skall alla VoIP-protokoll förhindras från att kommunicera direkt med datanätverket.
- Stark autenticering och accesskontroll skall användas för att koppla upp sig och administrera de flesta av komponenterna i VoIP-nätverket.
- Fysiska säkerhetslösningar är viktiga att införa i VoIP-miljöer

[12] På engelska kallas detta Confidentiality, Integrity och Availibility (CIA)
[13] All IP-trafik förmedlas inte över Ethernet. I exempelvis accessnät för kabel-TV och xDSL används andra bärare.
[14] Det finns dock många standarder exempelvis H.323, SIP, MGCP eller Megaco/H.248

- Specifika IT-säkerhetslösningar för VoIP-komponenter måste införas, anpassas och rutinmässigt testas.
- Organisationer måste införa lämpliga lösningar för att hantera problemen med E-911[15] tjänsten när man inför VoIP.

Noterbart är att endast IT-säkerhetsrelaterade frågor tas upp. Reservkraftsfrågor behandlas inte.

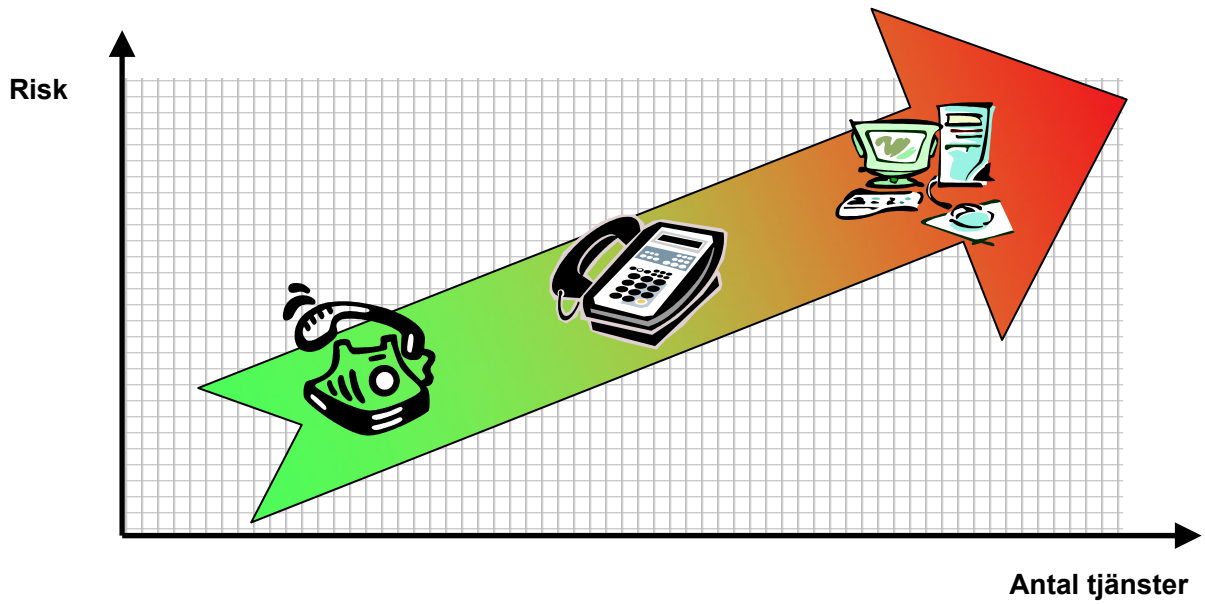
Ett liknande dokument som ger rekommendationer för organisationer inom den amerikanska försvarsmakten som använder VoIP är *Voice over Internet Protocol (VoIP) Security Technical Implementation Guide*[16]. De övergripande slutsatserna gällande sårbarheter i VoIP är likartade de som presenteras i NIST-rapporten.

[15] Motsvarar 112-funktionen för Europeiska förhållanden.
[16] DISA (Defense Information Systems Agency) Field Security Operations, *Voice over Internet Protocol (VoIP) Security Technical Implementation Guide*, Version 1, Release 1, 13 januari 2004.

3 Drivkrafter för övergång till IP-telefoni

Drivkrafterna för övergången till IP-telefoni är många gånger ekonomiska[17]. Privatpersoner kan få billigare samtals- och abonnemangskostnader. Organisationer gör besparingar genom att samutnyttja de fysiska näten för data och tele. En fara ur ett sårbarhetsperspektiv är att en ekonomisk kalkyl görs utan att man i tillräcklig utsträckning beaktar eventuella säkerhets-aspekter.

En annan viktig drivkraft är möjligheten att kunna utnyttja nya tjänster och i större utsträckning integrera telefonin med andra tjänster och applikationer som finns i en organisations IT-infrastruktur. Inom detta område finns många potentiella fördelar och möjligheter till effektivisering av verksamhet. Många gånger innebär en ökad integration av IP-telefoni med andra tjänster att man måste exponera telefonitjänsten mer i nätet och kanske avstå från metoden att logiskt separera data- och teletrafik som används för att säkerställa en hög tillgänglighet för telefoni (läs mer om detta i avsnittet *5.2.1 Typfall 1 – Lösning för en större organisation*). Här kan man konstatera att det finns en intressekonflikt som kan leda till komplicerade avvägningsfrågor.



Figur 1. Fler tjänster ger högre risk.

[17] Detta diskuteras bland annat i PTS rapport ”IP-telefoni. En teknisk marknadsbeskrivning”, PTS-ER-2003:41, 13 november 2003

4 Hotkällor

I detta avsnitt diskuteras möjliga källor till hot som kan utgöra faror för IP-telefonisystem och tal som förmedlas över IP. En vanlig uppdelning är att göra en distinktion mellan slumpmässiga och avsiktliga hot. En sådan indelning görs bland annat i FOI-rapporten ”Telekommunikationernas sårbarhet och risker för samhället”[18]. Distinktionen är viktig vid värdering av risken för att en större störning skall inträffa. För att en allvarlig störning skall uppstå krävs normalt att ett flertal händelser inträffar samtidigt. Slumpmässiga hot kan ha relativt hög sannolikhet att realiseras[19] men ger då vanligen små effekter. Avsiktliga hot karakteriseras av avsikten att störa eller påverka i syfte att uppnå ett visst mål. Den avsiktlige aktören kan därför förväntas agera så att samtidiga insatser samverkar till att uppnå önskad störning.

Många gånger är hot mot traditionell telefoni och hot mot IP-telefoni likartade. Det finns dock skillnader och det är framförallt dessa vi vill belysa i detta avsnitt.

4.1 Slumpmässiga hot

Tre huvudgrupper inom slumpmässiga hot är

- Naturkatastrofer,
- Tekniska fel och
- Felhandlingar.

När det gäller naturkatastrofer är IP-telefoni lika utsatt som många andra former av elektronisk kommunikation.

Tekniska fel utgör ett hot, framförallt de närmaste åren eftersom tekniken fortfarande är under utveckling. Det finns flera standarder inom området och även om många leverantörer följer dessa gör de ofta egna tillägg. Detta kan bland annat leda till att produkter med från olika leverantörer kan ha svårt att fungera tillsammans och att man får oväntade problem.

Man skulle kunna argumentera att IP-telefoni i jämförelse med traditionell fast telefoni behöver en betydande komplexitet i sina telefonterminaler (IP-telefoner, soft-clients och telefonadaptrar). Det skulle innebära att man har mer komplex utrustning på fler ställen och närmare abonnenterna, det finns alltså fler ställen där tekniska fel potentiellt kan uppstå. Samtidigt så är ju även dagens traditionella telefonterminaler relativt avancerade. Jämför man IP-telefoner med dagens mobiltelefoner så är mobilterminalerna av idag i många fall betydligt mer avancerade än många IP-telefoner.

Ny teknik medför naturligtvis en ökad risk för felhandlingar. Ett exempel är företag som överger sina traditionella telefoni-lösningar och går över till IP-telefoni. Dessa lägger ofta hela eller delar av driften på sin IT-avdelning. Det krävs därför att IT-avdelningen har den kompetens som behövs för att kunna hantera telefoniapplikationer. Samtidigt är tekniken relativt ny och företag har beklagat sig över att det ännu inte finns tillräckligt med kurser och utbildningar att tillgå inom området[20].

---

[18] FOI-R--1227--SE, Telekommunikationernas sårbarhet och risker för samhället, April 2004, G. Franzén, S. Barck-Holst, G. Fischer

[19] Exempelvis så grävde man under 2002 av i genomsnitt 55 kablar per dag i Sverige. *TeliaSonera Sverige*, http://www.kabelanvisning.com/kabelanvisningnew/default.asp?id=24

[20] Dataföreningen Sverige, IP-telefoni – Nytta ur ett verksamhetsperspektiv, Seminarium 18 februari, 2004.

Ur ett användarperspektiv är IP-telefonilösningar ibland mer komplexa eller i varje fall annorlunda jämförda med dagens telefonlösningar. Detta gäller till exempel soft-clients eller lösningar hos privata hushåll som ofta kräver en extra ”dosa” i form av en telefonadapter. Detta kan naturligtvis leda till fler felhandlingar. Misstag hos användare får dock konsekvenser som främst drabbar individen och inte samhället som helhet.

4.2 Avsiktliga hot

De avsiktliga hoten mot elektronisk kommunikation kännetecknas av att de skapas av en aktör som med sitt agerande har något syfte som i regel är vidare än att påverka tele-kommunikationerna i sig. Detta förhållande gäller även för IP-telefoni.

En indelning av aktörer som avsiktligt skulle kunna tänkas angripa IP-telefoni system är följande:

- Statliga aktörer
- Terrorister
- Hackers
- Kriminella med ekonomiska drivkrafter
- Insiders

Olika medel som en aktör kan tänkas utnyttja för att angripa de elektroniska kommunikationerna finns beskrivna i den tidigare nämnda rapporten ”Telekommunikationernas sårbarhet och risker för samhället”[21]. Angrepp kan ske direkt via fysisk påverkan på utrustning och kablar eller genom attacker inriktade på mjukvara. De IT-relaterade hot som diskuteras i rapporten är speciellt relevanta för IP-telefoni. När det gäller IP-telefoni kan även själva terminalen fungera som en plattform för angrepp.

[21] FOI-R--1227--SE, Telekommunikationernas sårbarhet och risker för samhället, sid. 22-25, April 2004, G. Franzén, S. Barck-Holst, G. Fischer

5 Analys

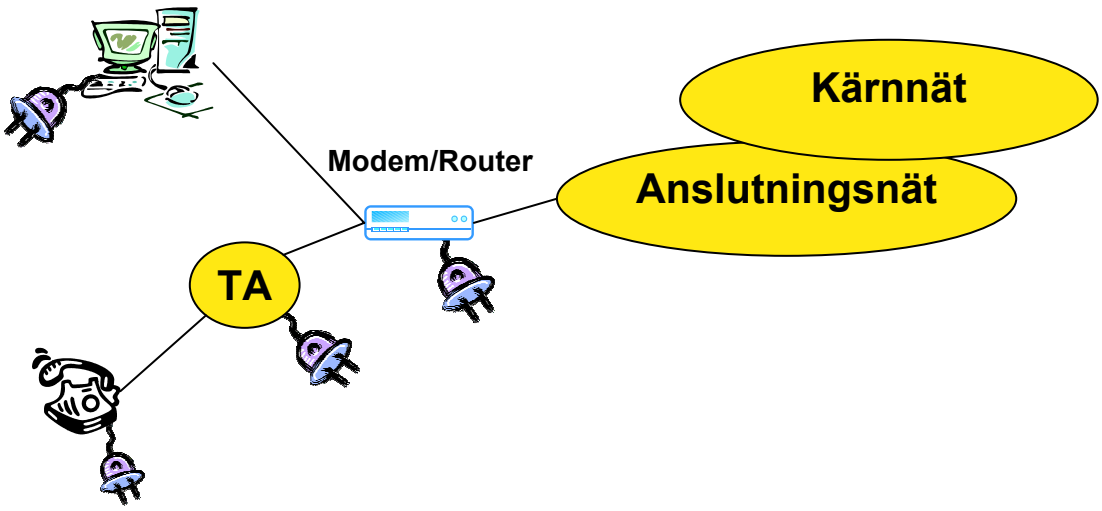
Utifrån våra studier och de intervjuer vi har gjort försöker vi i detta avsnitt göra en analys av de viktigaste sårbarhetsfrågorna.

I detta avsnitt behandlas först IP-telefonins sårbarhet med avseende på kraftförsörjning. Kraftförsörjning är grundläggande för all IP-telefoni oberoende av arkitektur. Därefter behandlas IT-säkerhetsfrågor, som utgör en stor och viktig del av sårbarhetsproblematiken kring IP-telefoni. Slutligen diskuteras IP-telefoni vid kris och extrema händelser.

5.1 Reservkraftförsörjning

En av de mer tydliga sårbarheterna när det gäller IP-telefoni är reservkraftförsörjningen. Fasta telefoner i den traditionella kretskopplade telefonin får sin el från en lokalstation eller företagsväxel via samma ledning som överför samtalstrafiken[22]. Lokalstationer liksom större delen av det traditionella stomnätet för telefoni är försett med reservkraft.

När det gäller IP-telefoni är systemen för reservkraft inte lika utvecklade. Främst gäller detta den utrustning som finns närmast abonnenterna. IP-telefoner måste vanligen strömförsörjas separat. Detta gäller datorer med soft-clients, telefonterminaler avsedda specifikt för IP-telefoni och de telefonadaptrar som används vid anslutning av vanliga telefoner. Företag och organisationer som inför IP-telefoni måste planera speciellt för en fungerande reservkraftlösning. En möjlig lösning för företag är att använda Power over Ethernet[23]. För hemanvändaren är reservkraft en kostsam lösning. En bärbar dator fungerar visserligen några timmar även vid elavbrott, men kabelmodem, ADSL-modem, bredbandsmodem och eventuella separata telefonadaptrar måste även de strömförsörjas vid avbrott.



Figur 2. Telefonterminaler och modem saknar vanligen reservkraft och slutar att fungera vid elavbrott. Nätens centralare delar är dock i större utsträckning utrustade med någon form av reservkraft. (TA = Telefonadapter)

[22] Även om det idag finns många trådlösa DECT-telefoner som kräver separat strömförsörjning för att fungera.
[23] Power over Ethernet (PoE), IEEE 802.3af är en standard för strömöverföring via Ethernetkablar. Med PoE används ethernetkabeln för tele-/datatrafik och strömförsörjning.

IP-telefoni där man använder mobilnäten för trafiköverföring (exempelvis soft-client på en laptop med GPRS-anslutning) har samma begränsningar avseende reservkraft som vanlig mobiltelefoni.

Om man ser till de nät som utnyttjas för IP-telefoni så är även reservkraftsförsörjningen i dessa idag begränsad. Stadsnätsföreningens rekommendationer för anslutningsnoder som saknar reservkraftverk är UPS-drift i en timme[24]. Men många bredbandsanslutningar saknar reservkraft och slutar fungera vid elavbrott.

Kabel-TV-näten är utrustade med reservkraft i viss utsträckning, exempelvis med fast reservkraft eller batteribackup i viktigare noder med många anslutna hushåll. Vilka noder som utrustas med reservkraft motiveras utifrån affärsmässiga grunder. Mindre noder och eventuella noder i fastighetsägarnas nät saknar i många fall reservkraft.

Vad gäller anslutning via ADSL är intrycket att det varierar från fall till fall. Från vissa leverantörer och för vissa anslutningar klarar uppkopplingen elavbrott om modemet är strömförsörjt. Det finns även lösningar för ADSL-anslutningar som medför att man vid elavbrott kopplar om till att använda det fasta telenätet. Möjligheter och problem rörande ADSL är något som kan undersökas närmare.

På lång sikt är reservkraftsproblematiken för IP-telefoni störst ute hos abonnenten.

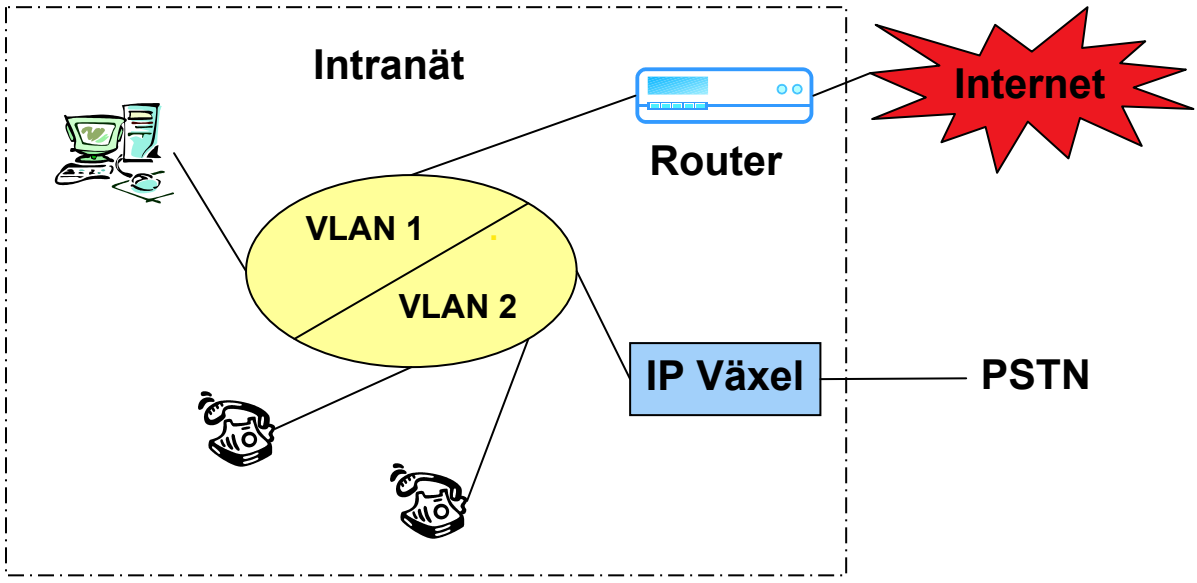
5.2 IT-säkerhetskonsekvenser för olika typfall

I det följande presenteras ett antal typfall som beskriver olika arkitekturer för IP-telefoni. Typfallen är framställda på ett sådant sätt att IT-säkerhetsaspekter skall kunna belysas och värderas. Typfall 1 behandlar lösningar för större organisationer medan typfall 2 och 3 är inriktade på privatpersoners eller mindre organisationers telefonilösningar.

5.2.1 Typfall 1 – Lösning för en större organisation

Typfall 1 beskriver de sårbarheter som finns för det som idag betraktas som en relativt säker lösning för IP-telefoni för en organisation.

[24] Robusta noder – Svenska stadsnätsföreningen



Figur 3. Typfall 1 - Relativt säker lösning för en större organisation.

I detta typfall är IP-telefoninätet ur ett logiskt perspektiv helt internt hos organisationen i fråga. Rent fysiskt kan det dock sträcka sig över nät som ägs och drivs av en annan part för att kunna omfatta flera separata platser, men då i form av ett VPN kombinerat med någon form av prioritering, eller i form av hyrda länkar. Genom att nyttja VLAN separeras på en logisk nivå det vanliga kontorsnätet från IP-telefoninätet, trots att bägge rent fysiskt utgör ett gemensamt nät. Inom det logiska IP-nätet sker ingen form av kryptering.

Ett angrepp mot denna form av IP-telefoninät kan på grund av nätets begränsade omfattning enbart få direkta konsekvenser för organisationen i fråga. Däremot kan det självklart få indirekta konsekvenser för andra parter som är beroende av organisationen.

5.2.1.1 Angrepp som slår mot tillgängligheten

En angripare som befinner sig någonstans på Internet skulle kunna utföra en DDoS-attack mot VPN-förbindelsen mellan organisationens delar. Med tillräckligt effektiv teknik för prioritering samt robusta nätverksnoder skulle inte detta få någon effekt på IP-telefonin. Om angriparen lyckas överbelasta eller på annat sätt slå ut viktiga nätverksnoder i sig, vilket skulle kunna vara tänkbart, så skulle IP-telefonitrafiken slås ut trots att den är prioriterad. En angripare som på något sätt har åtkomst till intranätet befinner sig i en liknande position.

Om angriparen befinner sig inom det logiska IP-telefoninätet blir det sannolikt mycket enklare att utföra diverse angrepp som slår mot tillgängligheten.

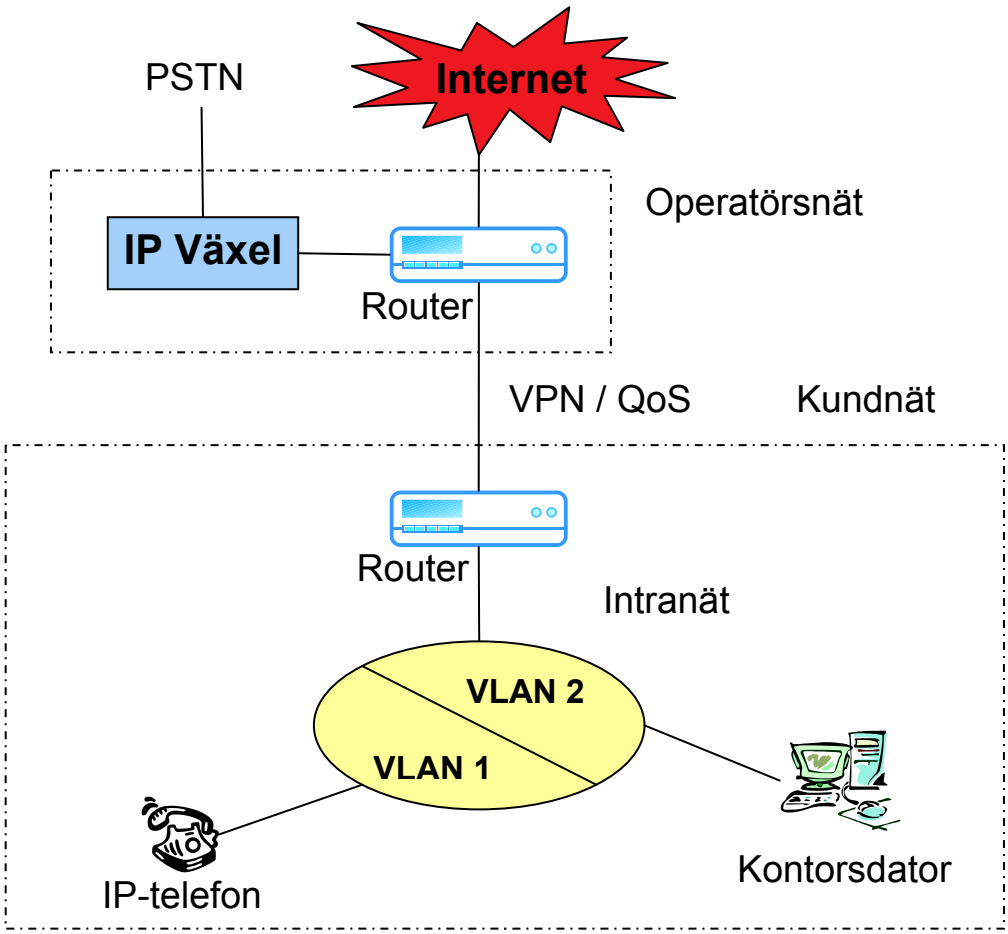
Att uppnå logisk separation i nätverk kan antas vara ett relativt enkelt problem att lösa jämfört med många andra problem inom IT-säkerhetsområdet på grund av att komplexiteten hos lösningen kan hållas relativt låg. Detta betyder inte att säkerheten hos denna typ av lösningar alltid är god i praktiken. Det finns till exempel brister i specifika implementationer av logiskt separerade nät som det möjligt att få trafik att hoppa mellan olika VLAN. Man bör dock vara medveten om att den totala mängden kända brister av den typen är många gånger mindre än den totala mängden kända brister i diverse operativsystem och applikationsmjukvara. Under projektets gång har vi kunnat konstatera att det tycks finnas ett stort behov av närmare studier av tekniker för logisk separation och prioritering av trafik för att kunna avgöra dess robusthet i praktiken.

5.2.1.2 Angripare som försöker avlyssna samtal

Passiv avlyssning från utsidan av det logiska IP-telefoninätet ska förhindras genom att VPN och VLAN används. Tillförlitligheten hos VPN får anses vara relativt hög ur ett IT-säkerhetsperspektiv. En angripare som befinner sig inom det logiska IP-telefoninätet kan dock sannolikt med relativ enkelhet utföra många olika typer av angrepp för att avlyssna samtal.

5.2.1.3 Jämförelse med PSTN

Utan att utföra en djupare analys tycks inte skillnaden i säkerhetsnivå mellan den här typen av IP-telefonilösning och PSTN vara så stor i allmänhet så länge lösningen i detalj implementeras på ett bra sätt. En av de viktigaste skillnaderna är dock de stora möjligheter till angrepp som finns *inom* ett logiskt IP-telefoninät om inga speciella säkerhetsåtgärder vidtagits. Medvetenhet om vilka angrepp som är genomförbara är viktigt för att inte användarna av IP-telefoni ska få ett felaktigt förtroende för tjänsten. I samband med detta är det också önskvärt med någon form av adekvat sektionering mellan olika delar av ett större logiskt IP-telefoninät. Dessa bägge punkter bör studeras ytterligare. En annan stor skillnad mellan PSTN och IP-telefoni är att en relativt tekniskt outbildad person som kommit över verktyg för att utnyttja eventuella brister hos en viss IP-telefonilösning skulle kunna avlyssna samtal på distans, utan att någonsin befunnit sig i närheten av de parter som avlyssnas. När det gäller PSTN får det anses vara mycket få personer som är kapabla till motsvarande sorts avlyssning. Där är det största hotet att någon fysiskt kopplar in sig direkt på ledningarna till en viss abonnent.

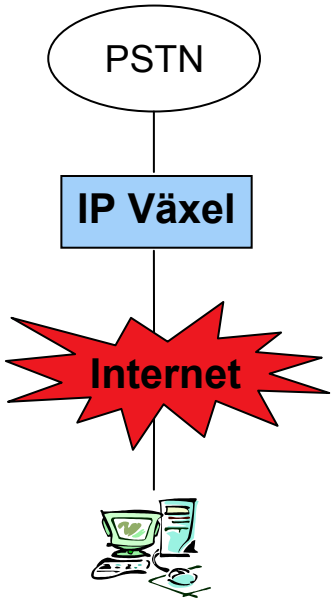


Figur 4. Modifierat typfall 1 - IP-växeln har placerats i operatörens nät.

I ett något modifierat fall av det tidigare beskrivna har IP-växeln placerats i operatörens nät istället för hos den egna organisationen. Detta utgör i princip inte någon skillnad mot vad som beskrivits tidigare. Men det är viktigt att lägga märke till att om flera kunders IP-telefonitrafik blandas på ett olämpligt sätt i operatörsnätet uppstår helt nya säkerhetsproblem.

5.2.2 Typfall 2 – IP-telefoni oberoende av Internetoperatör

I detta typfall ringer privatkunder direkt över Internet via sin vanliga bredbandsanslutning med hjälp av IP-telefoni. Ingen kryptering av trafiken utförs[25].



Figur 5. Typfall 2 - IP-telefoni oberoende av Internetleverantör.

5.2.2.1 Angrepp som slår mot tillgängligheten

En angripare som befinner sig någonstans ute på Internet kan mycket enkelt utföra en lyckad DDoS-attack mot en enskild kund eftersom det varken sker någon fysisk eller logisk separation mellan vanlig Internettrafik och IP-telefonitrafik. En utomstående angripare skulle dessutom kunna tänkas utföra en DDoS-attack mot IP-växeln. Även tillgänglighetsattacker genom utnyttjande av säkerhetsbrister i mjukvara hos IP-växeln eller kundens dator får ses som sannolika vid denna typ av lösning.

5.2.2.2 Angripare som försöker avlyssna samtal

Eftersom trafiken inte ens krypteras är den möjlig att avlyssna mellan kunden och IP-växeln. Även om trafiken vore krypterad är det mycket svårt för en vanlig kund att skydda sin dator mot intrång och därigenom mycket svårt att skydda sig mot avlyssning. Även IP-växeln kan vara svår att skydda med hög tillförlitlighet. Risken för angrepp bör betraktas som mycket stor eftersom all utrustning befinner sig mer eller mindre direkt ute på Internet.

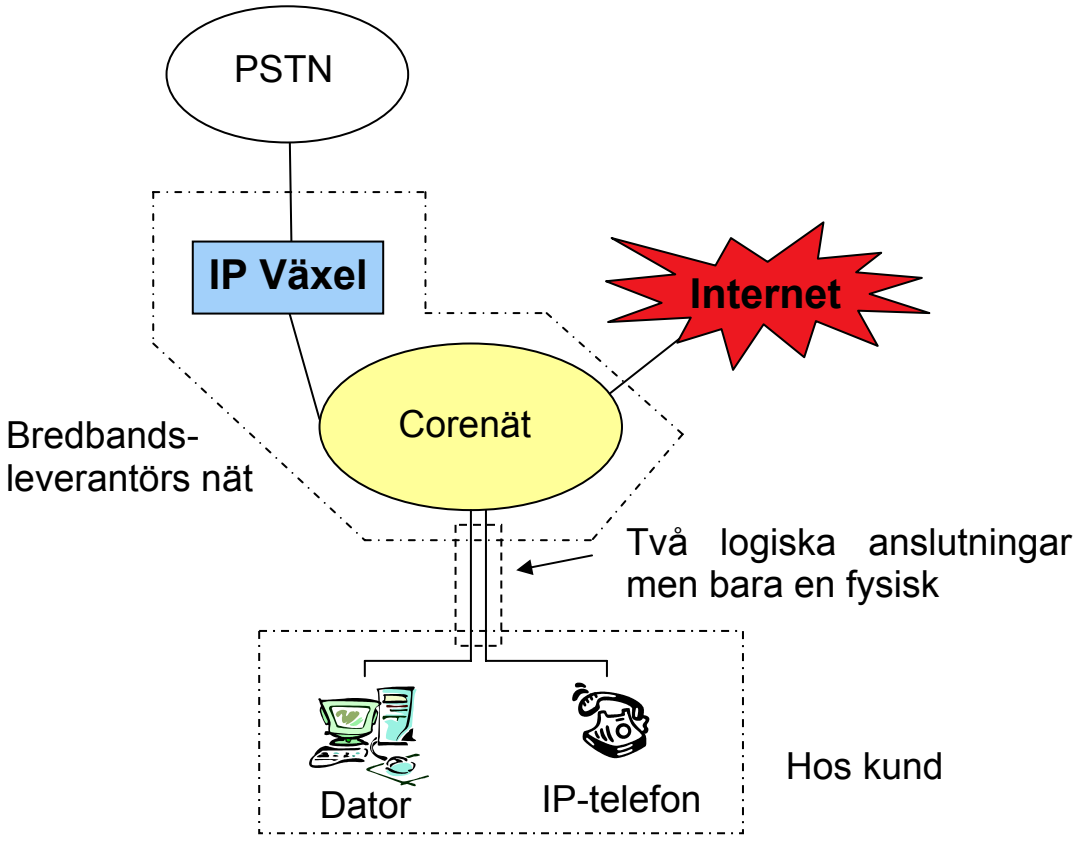
[25] Detta är en förutsättning i detta typfall. Det finns dock tjänsteleverantörer som krypterar trafiken, exempelvis Skype med SkypeOut.

5.2.2.3 Jämförelse med PSTN

Möjligheten att lyckat och utan risk för påföljder utföra angrepp mot tillgänglighet eller avlyssna samtal är mycket stor jämfört med PSTN. Denna typ av lösning utan kraftiga modifikationer bör absolut inte ses som en ersättning för PSTN.

5.2.3 Typfall 3 – IP-telefoni tillhandahållet av bredbandsleverantör

Denna lösning har mycket gemensamt med typfall 1, men är inriktad på tillämpning för privatpersoner.



Figur 6. Typfall 3 - IP-telefoni tillhandahållet av bredbandsleverantör

IP-telefoni och Internet utgör två logiskt separerade nät. Hotbilden ser dock annorlunda ut i detta fall eftersom användarna består av ett mycket stort antal privatpersoner. Risken för angrepp inom IP-telefoninätet är utan speciella åtgärder potentiellt lika stor som i Typfall 2. För att uppnå en god säkerhetsnivå måste ett antal kriterier vara uppfyllda. Den lista som presenteras här skall *inte* betraktas som fullständig utan bara som exempel på kritiska punkter.

- Mjukvaran i IP-växeln måste vara tillräckligt robust med avseende på intrång
- Mjukvaran i IP-telefonerna måste vara tillräckligt robust med avseende på intrång
- Den logiska separationen av trafik måste vara tillräckligt tillförlitlig
- Lösningen för prioritering av IP-telefonitrafik måste vara tillräckligt tillförlitlig

5.3 Kommunikationer vid kriser och extrema händelser

Vid terroristattentaten den 11 september 2001 användes VoIP som ett alternativ när den kretskopplade telefonin hade slagits ut.[26] Dock var den totala mängden av denna typ av samtal liten jämfört med mängden samtal som gick i det kretskopplade nätet. Vid denna tidpunkt var användandet av VoIP inte särskilt utbrett.

En effekt som terroristattackerna fick som relaterar till detta är att det amerikanska näringslivsdepartementet identifierade att man inte kunde larma sina anställda vid denna typ av incident.[27] Detta har fått konsekvensen att man på detta departement har installerat en applikation i kombination med departementets VoIP-nätverk som larmar via högtalarfunktionen på VoIP-telefonerna.

Inom ramen för de pågående militära operationerna i Irak och Afghanistan används VoIP på flera olika nivåer och med olika syften. Den tysk-holländska militära styrkan som opererar i Afghanistan använder VoIP i sin nätverksinfrastruktur *Theatre Independent Tactical Army and Air Force Network* (TITAAN). [28] Det amerikanska försvarsdepartementet använder VoIP i vissa av sina verksamheter i Irak och Afghanistan. Cisco Systems anger att de har installerat fler än 130 VoIP-nätverk över hela världen för amerikanska försvarsdepartementets räkning.[29] Den kanadensiska försvarsmakten använder VoIP för att låta sina soldater ringa hem från Afghanistan till en låg kostnad.[30]

En fördel med IP-telefoni i en krissituation är att det är relativt lätt att flytta med sitt telefonnummer till en alternativ placering, exempelvis i en krisledningscentral.

IP har en egenskap i form av ”graceful degradation” som även VoIP kan dra nytta av. Vid skador i nätverken omdirigeras trafiken automatiskt till alternativa vägar om sådana finns. Dessutom kan talkvaliten justeras ner och på så sätt minskas bandbreddsbehovet.

IP-nätverk är relativt enkla att bygga upp på lokal nivå. Utrustningen är i stor utsträckning standardiserad. Vid skador i nätverk och under uppbyggnadsskeden så drar man även fördel av VoIP genom att data och teletjänster byggs ut samtidigt i en gemensam fysisk nätverksinfrastruktur.

Hur mycket och på vilket sätt taltrafiken komprimeras styrs av vilken codec[31] som valts för en viss IP-telefonilösning. I en situation då stora nätskador uppstår skulle man kunna tänka sig att den tillgängliga bandbredden blir begränsad. Genom att byta codec skulle det då vara möjligt att få bättre kompression (till priset av sämre talkvalitet) och på så sätt förmedla fler samtal. Detta är kanske framförallt av intresse vid skador i trådlösa nät där exempelvis utslagning av ett antal basstationer reducerar kapaciteten, men täckningen vanligen i huvudsak finns kvar.

---

[26] National Research Council, *The Internet Under Crisis Conditions: Learning from 11 september*, sidan 47, 2002 (ISBN 0-309-08702-3)
[27] Alan, Joch, *VOIP's second act*, Federal Computer Week, 19 juli 2004, http://www.fcw.com/fcw/articles/2004/0719/feat-voip-07-19-04.asp
[28] Royal Netherlands Army, *TITAAN State-of-the-Art Networking for Military Mobile Environments* http://www.ce.areur.army.mil/pages/netherland/TITAAN_.pdf
[29] B. Brewin, F. Tiboni, DISA: Shift communications to IP, Federal Computer Week, 6 september 2004, http://www.fcw.com/fcw/articles/2004/0906/news-dodcomm-09-06-04.asp
[30] Soldiers in Afghanistan phone home with VoIP, 4 juli 2004, http://www.tmcnet.com/usubmit/2004/jul/1053607.htm
[31] Codec – Compressor/Decompressor

För nödsamtal finns det dock i dagsläget problem som uppkommit på grund av IP-telefoni. Det ena gäller tillgången till nödnummer. Vissa former av Internettelefoni tillhandahåller inget nödnummer, exempelvis Skype och Net Meeting. Detta kan visa sig vara ett problem om personer väljer att överge alla andra former av telefoni. I nuläget är dock denna typ av Internet-telefoni mest att betrakta som ett komplement till annan telefoni. Det är heller inte helt oproblematiskt att möjliggöra nödsamtal via Internet-telefoni. En potentiell fara skulle kunna vara en överbelastningsattack där en stor mängd Internet-telefoni-klienter samtidigt ringer 112 och på så sätt överbelastar larmcentralerna. Det finns även en oro hos SOS Alarm att IP telefoni skall leda till en ökad mängd fel- och okynnesringningar.

Ett annat problem rörande nödsamtal är lokalisering. För Internettelefoni förväntas användarna själva ofta ange var de ringer ifrån, vilket kan vara lätt att slarva med. Dessutom saknas standarder för att förmedla positioneringsinformation för IP-teletelefoni. Det kan innebära att larmcentralen tvingas ställa extra frågor till den nödställde för att säkerställa att man får rätt position eller att man helt enkelt inte får rätt uppgift om en nödställds position. Räddningsinsatser riskerar att försenas eller att skickas till fel ställe, vilket är mycket allvarligt då det i de flesta situationer är viktigt att hjälp kommer så snabbt som möjligt. Liknande problem kan uppstå för företag med lokalkontor på olika orter då SOS Alarm kan vilseledas att tro larmet kommer från den ort där IP-växeln står[32]. Detta kan dock undvikas med en riktigt konfigurerad IP-telefonilösning. För IP-telefoni *tillhandahållet av bredbands-leverantör*[33] bör lokalisering inte vara ett problem eftersom bredbandsleverantören har kontroll över sina nät och vet var kunderna ansluter sig geografiskt.

[32] Detta problem är inte specifikt för IP-telefoni utan kan även inträffa med traditionella växlar.
[33] Se avsnitt 2.1.

6 Scenarier

Ett av studiens mål är att bedöma vilka konsekvenser övergången av IP-telefoni kan få för samhället. I detta avsnitt görs detta med hjälp av tre olika scenarier.

Dessa scenarier utgör inga prognoser och gör inga anspråk att beskriva den faktiska framtiden utan skall ses som ett underlag för en diskussion kring sårbarhetsaspekter rörande IP-telefoni. Där det har funnits faktiska exempel på redan existerande sårbarheter eller hot har det refererats till dessa.

6.1 Scenario 1- Användande av IP-telefonimask för utpressning

Året är 2010 och majoriteten av alla svenska hushåll har gått över till IP-telefoni. Operatören TalaIP AB är näst störst i landet med cirka 700 000 anslutna abonnenter. TalaIP har infört ett antal åtgärder för att höja säkerhetsnivån i sin lösning.

Alla IP-telefoner sitter på ett nät som är logiskt separerat från det nät som kunderna har sina datorer anslutna till (Se Figur 6 från Typfall 3). Brandväggsfunktioner i accessnätet ser till att ingen som helst trafik släpps igenom direkt mellan två kunders IP-telefoner utan att ett samtal först kopplats upp. Dessutom tillåts ingen signalering direkt mellan IP-telefonerna utan denna går enbart via en central IP-växel. Den enda trafik som tillåts mellan två IP-telefoner är själva talströmmen.

Vidare kontrollerar alla anslutna IP-telefoner med automatik regelbundet efter nya uppdaterade versioner av mjukvaran. Om en uppdatering upptäcks laddas den ner och installeras utan att användaren märker det. För att en uppdatering ska vara giltig krävs att den är digitalt signerad av tillverkaren.

TalaIP har också ett kombinerat system för fraud prevention and intrusion prevention. Detta system spärrar automatiskt kunder som försöker utföra intrång av kända typer via nätet, eller som exempelvis ringer ett stort antal andra abonnenter i snabb följd.

Den 7:e maj upptäcker en medlem i den framgångsrika brasilianska hackergruppen HastaLaHacka att det finns ett allvarligt säkerhetshål i den modell av IP-telefon som används av TalaIP. Hålet utgörs av en s.k. stack based buffer overrun[34] i den programkod som tolkar protokollet för överföring av talströmmar. Genom att skicka speciellt utformade IP-paket kan en antagonist ladda in nya programinstruktioner i den befintliga mjukvaran i telefonens arbetsminne och aktivera dessa. Denna typ av attack kringgår helt den säkerhetsmekanism baserad på digitala signaturer som finns i telefonerna. En annan medlem i hackergruppen konstruerar under den nästföljande veckan ett s.k. exploit - ett litet program som skickar de speciellt utformade paket som krävs för att ta kontrollen över en IP-telefon.

Den 20: e maj träffas en medlem i HastaLaHacka och en medlem i den svenska kriminella hackergruppen LamboCrew på en internationell chattkanal för kriminella hackers. LamboCrew har kommit över en lista med kompletta uppgifter för runt 1000 kreditkort. De

[34] För exempel och beskrivning på denna typ av angrepp se exempelvis: Paul A. Henry *Buffer Overrun Attacks*, CyberGuard Corp. http://www.rootsecure.net/content/downloads/pdf_downloads/buffer_overruns.pdf

båda medlemmarna gör upp om ett byte - exploitet mot kontokortsuppgifterna. Redan den 25: e maj har LamboCrew lyckats skapa en IP-telefonimask[35] som bygger på det köpta exploitet.

Sent på eftermiddagen den 27: e maj ansluter LamboCrew en dator till ett IP-telefoniuttag i TalaIP:s nät. Masken väljer på ett intelligent sätt ut tre nya abonnenter och ringer automatiskt upp dessa. Så fort ett samtal kopplats upp får masken en fri väg till den mottagande IP-telefonen och infekterar denna. Därefter ringer varje infekterad telefon upp ytterligare tre telefoner. Eftersom det rör sig om relativt få samtal från varje enskild abonnent och säkerhetshålet inte är känt sedan tidigare så hindras inte masken av vare sig fraud prevention eller intrusion prevention. Inom en timme har masken infekterat nästan alla TalaIP:s 700 000 abonnenter. Efter totalt två timmar går masken in i fas två - den låser alla IP-telefoner totalt på ett sätt som gör att de måste skickas in till en reparationsverkstad för ominstallation. Ungefär 700 000 abonnenter är nu fullständigt utslagna och TalaIP tvingas efter ett par timmar att gå ut via massmedia med uppmaningen att lämna in telefonen till verkstad. Samtidigt tar en medlem kontakt med den största operatören av VoIP, nämligen StörstIP och kräver 5 miljoner kronor för att inte släppa lös en mask som kommer att slå lika skoningslöst mot StörstIP:s system som den andra masken gjort mot TalaIP.[36] Dessa betalar eftersom ingen analys av masken har genomförts och man vågar inte gå på linjen att LamboCrew bluffar.

För TalaIP innebär det genomförda angreppet en mycket hög arbetsbelastning eftersom det rör sig om så stora mängder telefoner. Dessutom krävs omfattande analys hos företaget som tillverkat IP-telefonerna för att hitta säkerhetshålet. På grund av detta uppstår långvariga leveransförseningar innan kunderna slutligen får tillbaka sina telefoner. Efter ytterligare ett halvår hör LamboCrew av sig till TalaIP igen och påstår sig ha en ny mask som är ännu effektivare än den förra. Den här gången vill man ha 10 miljoner kronor av TalaIP för att inte släppa ut den…

[35] R. Mogull, C. Moore, D. Fraley, R. Goodwin, A. Earley, R. DeLotto, **Strategic Planning SPA-21-3633, Gartner Reserach Note 14 January 2004**, *Predicts 2004: Critical Infrastructure Protection.* Gartner bedömer att det är troligt att det under 2006 kommer att dyka upp virus och maskar som slår specifikt mot VoIP-specifika nätverkselement.
[36] W. Knight, *Zombie networks fuel cybercrime*, New Scientist, 6 november 2004.

6.2 Scenario 2 - Elavbrott till följd av oväder

Året är 2008 och nästan 90 procent av Sveriges abonnenter har bredband i någon form. Framförallt är det bredband över DSL-anslutningar som har fått stort genomslag[37]. Men även för andra accessformer har antalet abonnenter ökat kraftigt. En viktig förklaring till det stora genomslaget har varit teknikövergången till IP-telefoni, men även ökande efterfrågan på tillgång till bredbands-TV och Video-on-demand. Tjänsten IP-telefoni ingår numera som standard i de flesta bredbandserbjudanden, varför i princip alla bredbandskunder har tillgång till IP-telefoni och ca 80 % har övergett den traditionella telefonin.

På privatmarknaden började traditionell fast telefoni redan i början av 2006 att få stark konkurrens från IP-telefoni över kabel-TV-nät, elnät och olika fibernät. Vissa lokala telestationer hade slutligen extremt få abonnenter anslutna då de flesta abonnenter hade övergått till bredband med IP-telefoni över andra accessformer. TeleStort oroades av kunderna övergav sina fasta teleabonnemang och för att locka tillbaka kunderna erbjöd man ett kombinerat bredbands- och telefoniabonnemang över DSL, som dock förutsatte att kunden använde sig av IP-telefoni. På så sätt kunde man avveckla den traditionella kretskopplade telefoniutrustningen i många mindre telestationer och hålla nere kostnaderna.

Den statliga satsningen på bredband har lett till en snabb utbyggnad av bredbandsnät i Sveriges kommuner[38]. Det ekonomiskt fördelaktiga att använda dessa nät för IP-telefoni stod snart klart för många kommuner och år 2008 har 70 % av landets kommuner helt eller delvis växlat över till IP-telefoni för sin verksamhet.

X kommun i Västsverige var definitivt inte först med att kasta ut sina gamla växlar. Men när man såg vilka ekonomiska vinster det fanns att göra gick det undan. Sedan beslutet fattades i maj 2007 har man på ett halvår fått den nya lösningen på plats. Kommunens säkerhetssamordnare har pekat på att reservkraftsförsörjningen inte är tillfredsställande. Man har därför påbörjat ett arbete för att förbättra detta, tanken är att besparingarna det nya telesystemet genererar under 2 år skall användas till att åtgärda reservkraftsproblemen. Man prioriterar då först de centrala delarna och kritisk verksamhet.

Måndag morgon den 24 november 2008 drar ett kraftigt snöoväder in över södra och västra Sverige[39]. De flesta yrkesarbetande har hunnit bege sig till sina arbeten och skolveckan har börjat. Det snöar kraftigt och blåser i medeltal 28 m/s – i vindbyarna upp till 45 m/s. Under förmiddagen leder saltbeläggningar till kortare avbrott i elförsörjningen. Vid 13-tiden rasar två ledningsstolpar och en 400 kV-ledning över Göta älv i den kraftiga stormen. Vid 14-tiden är Göteborg, Kungsbacka, Mölndal, Borås, Alingsås, Kungälv, Stenungsund, Uddevalla och Lysekil med omgivande områden – totalt 800 000 människor – strömlösa. Stormen och den tunga snön på träden slår vidare ut stora delar av eldistributionsnätet på landsbygden. Vid 16-tiden är ca 40 000 hushåll, jordbruk och mindre industri- och service-företag utanför

[37] Lars Anders Karlberg, *Ericssons magiska låda ger adsl till alla*, Ny Teknik 041118 http://www.nyteknik.se/art/37685, ”Telia bygger nu ut sina telestationer i en rasande fart och lovar att 90 procent av alla svenska hushåll ska ha tillgång till 8 megabit bredband till jul. Hemligheten är Ericssons lilla adsl-låda som gör det lönsamt att bygga in adsl även i små telestationer.”

[38] Utbyggnaden av bredband med statligt stöd har passerat halvtid, Projektet ”Samverkan kring IT-infrastruktur” http://www.orebrolan.se/asp/fncShowDoc.asp?key=intraslj@739

[39] Idéerna till elavbrottet i detta scenario är hämtade ur delscenario 1 i SOU 1995:20 ”Utan el stannar Sverige”

tätorterna i Bohuslän, Dalsland, Västergötland och Halland strömlösa. Tisdag morgon har vinden avtagit och det har slutat snöa, men det är nu mycket kallare än tidigare.

Utvecklingen i X kommun under elavbrottet
På landsbygden i X kommun blir många hushåll strömlösa redan på förmiddagen den 24 november när träd faller över kraftledningar. Efter klockan 14 är dock hela kommunen strömlöst.

De av kommunens hushåll som bara har IP-telefon över bredband kan då inte längre använda denna eftersom bredbandsmodemen är strömlösa. Mobiltelefonerna fungerar fortfarande. Kapaciteten i mobiltelenäten är dock försämrad eftersom de flesta 3G-basstationerna är utslagna. Många är oroliga och ringer via mobiltelefon till anhöriga eller SOS Alarm. Det är svårt att komma fram och man får ibland försöka ringa flera gånger innan man får signaler att gå fram.

På kommunens huvudkontor är man överraskad. Reservkraftaggregatet gick igång som planerat och telefonerna fungerar, men man kan ändå bara ringa internt. Kommunens IT-avdelning jobbar på att spåra problemet. Mobiltelefonerna används flitigt.

Även ute i kommunens skolor är man hänvisad till mobiltelefoner. Här fanns ingen reservkraft och deras IP-telefoner står alla tysta. På Skogåsens lågstadieskola har man beslutat att stänga skolan. Många barn bor dock långt från skolan. Man försöker kontakta föräldrarna för att få dem att hämta barnen. Ett problem är att servern med alla klasslistor och adressuppgifter gått ner och skolpersonalen har därför svårt att få fram telefonnummer till föräldrarna.

De flesta mindre vägar är oframkomliga på grund av det ymniga snöfallet eller nedblåsta träd och annat bråte. De större vägarna lyckas man hjälpligt hålla farbara med hjälp av plogning. På många håll kan man dock se övergivna fordon som kört fast i snön.

Vid 16-tiden är det nästan omöjligt att komma fram ens med mobiltelefon. Batterierna i radiobasstationerna har laddat ur även för GSM-näten. Ett fåtal stationer fungerar då de får ström från reservkraftsaggregat. Reparationspersonal har även placerat ut mobila reservkraftsaggregat vid en del basstationer. Men kapaciteten i mobilnäten är ändå allt för låg och få samtal blir faktiskt uppkopplade.

Ett flerfamiljshus står i brand efter att någon försökt få liv i sitt ADSL-modem med hjälp av ett bilbatteri. Lägenhetsinnehavaren ringde SOS Alarm med sin mobiltelefon men samtalet bröts innan han hann berätta vilken adress han ringde ifrån. Från larmcentralen försökte man flera gånger ringa tillbaka men utan framgång. Lyckligtvis hade man påbörjat utplacering av polis och räddningsfordon i kommunen för att kunna få in eventuella larm när telefonitjänsterna började svikta[40]. En polisbil hade då upptäckt branden och lokaliserat den till Vikomberga. Men det tog lång tid innan den första brandbilen kom till platsen.

I kommunhuset har man lokaliserat problemet med telefonerna. Batterier i en UPS-anläggning hade varit urladdade och därför hade den externa kopplingen gått ner i det glapp som uppstod

[40] Utplacering av polis och räddningsfordon på grund av omfattande teleavbrott gjordes vid teleavbrottet i Uppsala i oktober 2002. Se exempelvis ”Teleavbrottet i Uppsala 2002 – Infrastrukturell sårbarhet”, Anna Hedin Ekström, Crismart 2004

innan reservkraften kopplades på. Felet är snabbt åtgärdat. IT-avdelningen kan dock konstatera att man har kontakt ut från kommunen och med andra enheter som är anslutna till kommunhuvudnoden. Områdesnäten och anslutningsnäten[41] i kommunen har dock delvis upphört att fungera då UPS-aggregaten vid noderna laddat ur och man på många håll inte hunnit få fram reservkraftsaggregat.

Under kvällen fortsätter ovädret med något avtagande styrka. Reparations- och räddningsarbeten pågår på många håll i kommunen. Även om man via RAKEL-systemet[42] kan koordinera insatserna från krisledningsplatsen i kommunhuset är man plågsamt medveten om att 65 % av hushållen saknar fungerande telefon och att det även är så att vissa byar och mindre samhällen helt saknar telefonförbindelser då den lokala telestationens batterier laddat ur eller att det helt enkelt inte finns några hushåll med traditionella telefonabonnemang kvar i dessa områden.

[41] Se Svenska Stadsnätsföreningens ”Robusta Noder : Rekommendation” för information om reservkraft i bredbandsnät.
[42] Enligt Krisberedskapsmyndighetens faktablad om RAKEL ”Vad händer hösten 2004?” är driftstart i Västra Götaland planerad till 2006. För mer om RAKEL se:
http://www.krisberedskapsmyndigheten.se/default____176.aspx

6.3 Scenario 3 - Misslyckad tillgänglighetsattack mot IP-telefoni

Året är 2008 och den nystartade Myndigheten för Gift- och Läkemedelsinformation, MGL, har infört IP-telefoni. MGL hjälper bland annat sjukvården med information vid allvarliga akuta förgiftningar av ovanliga substanser där enbart myndigheten besitter tillräcklig kompetens.

Telefonitrafiken till MGL går i en VPN-tunnel över myndighetens vanliga Internetförbindelse till en IP-växel placerad hos operatören. Operatören använder sig av teknik som garanterar VPN-tunneln en minsta tillgängliga bandbredd.

En politisk extremistgrupp beslutar sig för att sabotera samhällsviktiga funktioner och som en del av detta slå ut myndighetens telefoni. Gruppen sprider en trojan via mass-mailutskick till hundratals Internetanvändare. Trojanen kan fjärrstyras, och den 8 oktober 2008 beordras alla aktiva trojaner att skicka så mycket trafik som möjligt till MGL:s brandvägg[43]. Detta ger upphov till en trafikmängd som är ca 25 gånger högre än bandbredden hos myndighetens Internetanslutning.

Eftersom VPN-tunneln som transporterar IP-telefonitrafiken har en garanterad minsta tillgängliga bandbredd får attacken ingen som helst effekt på telefonin. Däremot slås all åtkomst till och från Internet ut totalt för myndigheten. Detta leder bland annat till att viktiga databaser som sjukvården använder inte kan nås. Eftersom det fortfarande är möjligt att nå MGL via telefon går det ändå att få ut kritisk information så länge attacken pågår.

[43] Fredrik Söderblom, XPD Systems AB, gav under Internetdagarna 2004 en beskrivning av DDoS attacker i sitt föredrag *Storskaliga attacker mot infrastruktur - hot - attack – åtgärd,*
http://www.iis.se/Internetdagarna/2004/23-robust/id04-23-fredriksoderblom.pdf

7 Områden att fortsatt bevaka

7.1 Reservkraft

För den traditionella kretskopplade telefonin har det funnits relativt enkla och förhållandevis kostnadseffektiva lösningar för reservkraftsförsörjning vilket också har utnyttjats. Detta medför en förväntan i samhället att telefonen skall fungera även vid strömavbrott.

För IP-telefoni är reservkraftsförsörjningen inte lika självklar. För att garantera fungerande IP-telefoni vid elavbrott krävs speciella lösningar.

På sikt är det troligt att de centralare delarna av näten kommer att vara väl försedda med reservkraft. Utslaget per abonnent blir kostnaden inte så hög och det är därför affärsmässigt möjlig att räkna hem denna typ av investering för nätägarna. Man riskerar inte att lokala elavbrott får störningar för många abonnenter.

Längre ut i näten blir det dock allt svårare att få en affärsmässig kalkyl att gå ihop. Abonnenternas och accessnätens elförsörjning kommer därför att utgöra en sårbarhet när det gäller IP-telefoni under lång tid framöver. Att få en lika robust lösning som den som existerar för dagens kretskopplade telefoni är troligen svårt och i vilket fall mycket kostsamt.

Av kostnadsmässiga kommer troligen såväl operatörer som abonnenter i framtiden att föredra IP-telefoni framför den traditionella kretskopplade fasta telefonin. Som illustreras i avsnitt *6.2 Scenario 2 - Elavbrott till följd av oväder* kan det finnas en risk att vi får ett samhälle där telefonitjänsterna i stor utsträckning slås ut vid större elavbrott. Denna utveckling är viktig att bevaka och det finns även skäl att utreda möjliga strategier för att motverka att samhället hamnar i en situation där man står utan fungerande telefoni vid ett elavbrott. Lösningen behöver inte vara att satsa på en fullt reservkraftsförsedd IP-telefoni och alla former av telefoni behöver kanske inte vara lika tillgängliga vid elavbrott. Det är dock viktigt att användare av telefoni känner till om de kan ringa vid elavbrott med den telefonilösning som de har tillgång till.

7.2 IT-säkerhet

En observation är att säker IP-telefoni kräver nät som är logiskt separerade från annan trafik i nätet. Dessutom bör man ha god kontroll på terminalerna för att garantera att de är säkra och pålitliga och inte manipuleras. Trafiken från ett sådant nät kan sedan slussas till andra telenät via PSTN. I framtiden kommer man att vilja koppla samman IP-nät för telefoni utan att gå via PSTN.

En stark drivkraft bakom IP-telefoni är att kunna integrera telefoni med andra tjänster. Detta kräver mer avancerade terminaler. Ju mer avancerade terminalerna blir desto sårbarare blir dessa för manipulation och skadlig kod.

Det är mycket viktigt att vara medveten om att säkerhetsproblem *inte* går att lösa enbart genom införskaffande av diverse säkerhetsprodukter som till exempel brandväggar och intrångsdetekteringssystem. Speciellt när det gäller sårbarheter i mjukvara handlar det snarare om utformningen av hela utvecklingsprocessen hos tillverkaren, införandeprocessen hos operatören, samt om omfattande och detaljerad kravställning samt testning utförd direkt av eller på uppdrag av någon aktör som har ett genuint intresse av att slutkunderna får en tillräckligt god IT-säkerhet.

Problematiken runt säkerhet när det gäller IP-telefoni skall *inte* betraktas som ett tecken på att IP-telefoni i sig aldrig kan bli säker och aldrig kan ersätta PSTN. Det vore att dra för långtgående slutsatser av den tillgängliga kunskapen. Däremot är det viktigt att vara medveten om att det finns potentiellt mycket stora och allvarliga säkerhetsproblem som måste belysas i detalj och därefter hanteras på ett korrekt sätt.

Ett exempel på sådant som för tillfället tycks vara för oklart och bör studeras närmare är frågan om hur säkra dagens lösningar för logisk separation och prioritering av trafik egentligen är.

7.3 Kris och extrema händelser

Elektroniska kommunikationer och då framförallt taltrafik är extremt viktiga i krissituationer. Samordning av insatser och annat ledningsarbete kräver tillgängliga, tillförlitliga och uthålliga kommunikationskanaler. Den enskilde som råkar i nöd bör ha tillgång till tele-kommunikationer för att kunna påkalla hjälp.

Utvecklingen avseende nödsamtal och lokalisering är ett område som fortsatt bör bevakas. Det vore olyckligt om det skulle bli så att delar av befolkningen väljer telefonitjänster som inte erbjuder fungerande funktioner för nödsamtal. Det är dock viktigt att poängtera att de lösningar som idag erbjuds som ersättning till traditionella telefonabonnemang (*First-Line Replacement)* erbjuder nödsamtal med fungerande positionering.

I avsnitt *5.3 Kommunikationer vid kriser och extrema händelser* redovisas även egenskaper hos IP-telefoni som bör vara attraktiva under och efter olika krissituationer. Dessa egenskaper bör man ha i beaktande vid framtida satsningar på ökad robusthet i de elektroniska kommunikationerna.

Ordlista

ADSL	Asymmetrical Digital Subscriber Line
Codec	Compressor/Decompressor. En codec är en algoritm för komprimering och dekomprimering av tal och data. Val av codec påverkar hur omfattande kompressionen blir och hur kvaliteten på data påverkas.
PSTN	Public Switched Telephony Service
QoS	Quality of Service
Soft-client	IP-telefoner behöver inte se ut som ”vanliga” telefoner. En soft-client är programvara som kan körs på en vanlig PC och som erbjuder telefonfunktionalitet. Datorn behöver även lämpligt ljudkort och headset eller mikrofon och högtalare.
Telefonadapter	För att använda en traditionell analog telefon som terminal vid IP-telefoni krävs en telefoniadapter som sköter signalering och konverterar taltrafik till/från IP.
VLAN	Virtual Local Area Network
xDSL	xDSL benämner en familj av DSL-tekniker (Digital Subscriber Line) för överföring av data på koppartråd.

Referenser

P. A. Henry, **Buffer Overrun Attacks**, CyberGuard Corp.
http://www.rootsecure.net/content/downloads/pdf_downloads/buffer_overruns.pdf

Ericssons magiska låda ger adsl till alla, Artikel i Ny Teknik, 2004-11-19,
http://www.nyteknik.se/art/37685

Final Report for the European Commission: **IP Voice and Associated Convergent Services**, Analysys, 28 januari 2004.
http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/studies_ext_consult/ip_voice/401_28_ip_voice_and_associated_convergent_services.pdf

IEEE 802.3af,
http://www.ieee802.org/3/af/

R. Granberg, M. Peterson, **IP-telefoni. En förstudie**, Examensarbete, Elektroingenjörs-programmet, Umeå Universitet, 2003.

IP-telefoni. En teknisk marknadsbeskrivning, PTS-ER-2003:41, 13 november 2003

Oskar Bergquist, Magnus Sjöstedt, **IP Telephony: A Swedish Perspective**, KTH, M.Sc. Thesis, 27 juni 2003.

Jason Halpern, SAFE: **IP Telephony Security in Depth**, White Paper, Cisco Systems, 2003
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf

P. Hochmuth, **Is VoIP vulnerable?,** Network World, 24 juni 2002,
http://www.nwfusion.com/news/2002/0624voip.html

Kabelanvisning.com,
http://www.kabelanvisning.com

Svenska stadsnätsföreningen, **Robusta noder: rekommendationer. Utformning av fysisk säkerhet i noder i öppna neutrala bredbandsnät. Regionala noder, kommunhuvudnoder, ortsnoder och anslutningsnoder**, Februari 2002.

D. R. Kuhn, T. J. Walsh, S. Fries, **Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology**, NIST National Institute of Standards and Technology, DRAFT Special Publication 800-58

B. Brewin, F. Tiboni, DISA: **Shift communications to IP**, Federal Computer Week, 6 september 2004, http://www.fcw.com/fcw/articles/2004/0906/news-dodcomm-09-06-04.asp

Soldiers in Afghanistan phone home with VoIP, 4 juli 2004,
http://www.tmcnet.com/usubmit/2004/jul/1053607.htm

Fredrik Söderblom, XPD Systems AB, **Storskaliga attacker mot infrastruktur - hot - attack – åtgärd**, föredrag Internetdagarna 2004,
http://www.iis.se/Internetdagarna/2004/23-robust/id04-23-fredriksoderblom.pdf

I. Lekteus et al. **Tekniska och ekonomiska förutsättningar för IP-telefoni vid FOI**, FOI-D—0171--SE, mars 2004

A. Hedin Ekström, **Teleavbrottet i Uppsala 2002 : infrastrukturell sårbarhet**, CRISMART, Försvarshögskolan, 2004

National Research Council, **The Internet Under Crisis Conditions: Learning from 11 september**, 2002 (ISBN 0-309-08702-3)

O. Arkin, **The Trivial Cisco IP Phones Compromise, Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960**, September 2002.

SOU 1995:20, **Utan el stannar Sverige**

SOS Alarm, **Riktlinjer för Nödtrafik, 112 i Sverige**, 1999-06-16.

R. Mogull, C. Moore, D. Fraley, R. Goodwin, A. Earley, R. DeLotto, **Strategic Planning SPA-21-3633, Gartner Reserach Note 14 January 2004**, *Predicts 2004: Critical Infrastructure Protection.*

S. Williamson, **Svensk telemarknad första halvåret 2003,** Post & Telestyrelsen, PTS-ER-2003:42, december 2003.

S. Williamson, F. Öst, **Svensk telemarknad första halvåret 2004,** Post & Telestyrelsen, PTS-ER-2004:43, december 2004.

G. Franzén, S. Barck-Holst, G. Fischer, **Telekommunikationernas sårbarhet och risker för samhället**, FOI-R--1227--SE, April 2004

Royal Netherlands Army, **TITAAN State-of-the-Art Networking for Military Mobile Environments** http://www.ce.areur.army.mil/pages/netherland/TITAAN_.pdf

Utbyggnaden av bredband med statligt stöd har passerat halvtid, Kommunförbundet, Landstingsförbundet, projektet "Samverkan kring IT-infrastruktur", 2004-02-26 http://www.orebrolan.se/asp/fncShowDoc.asp?key=intraslj@739

Vad händer hösten 2004?, RAKEL, Faktablad Krisberedskapsmyndigheten.

J. M. Eldridge, **Voice and Data Network of Convergence and the application of Voice over IP**, Sandia Report SAND 2000-2857, november 2000.

Alan, Joch, **VOIP's second act**, Federal Computer Week, 19 juli 2004, http://www.fcw.com/fcw/articles/2004/0719/feat-voip-07-19-04.asp

DISA (Defense Information Systems Agency) Field Security Operations, **Voice over Internet Protocol (VoIP) Security Technical Implementation Guide**, Version 1, Release 1, 13 januari 2004

O. Arkin, **Why E.T. Can’t Phone Home? Security Risk Factors with IP Telephony based Networks**, November 2002

W. Knight, **Zombie networks fuel cybercrime**, New Scientist, 6 november 2004

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--1528--SE	Underlagsrapport
Försvarsanalys	**Forskningsområde**	
172 90 Stockholm	1. Analys av säkerhet och sårbarhet	
	Månad, år	**Projektnummer**
	Januari 2005	E1895
	Delområde	
	13 Stöd till säkerhet och beredskap	
	Delområde 2	

Författare/redaktör	Projektledare
Svante Barck-Holst	Svante Barck-Holst
Henrik Christiansson	**Godkänd av**
Arne Vidström	Staffan Molin
	Uppdragsgivare/kundbeteckning
	PTS
	Tekniskt och/eller vetenskapligt ansvarig
	Svante Barck-Holst

Rapportens titel

IP-telefoni ur ett sårbarhetsperspektiv

Sammanfattning (högst 200 ord)

Denna rapport redovisar resultatet av en utredning för Post & Telestyrelsen i vilken IP-telefoni studeras ur ett sårbarhetsperspektiv. Syftet med projektet har varit att göra en sårbarhetsanalys av IP-telefoni och därur identifiera vilka eventuella konsekvenser en övergång till IP-telefoni kan få för samhället. Ett syfte har även varit att identifiera frågeställlningar inom området som kräver fortsatt bevakning eller utredning.

Inom studien har i huvudsak tre områden behandlats reservkraft, IT-säkerhet och nödsamtal.

Den traditionella fasta kretskopplade telefonin har varit väl utrustad med reservkraft och har därför i stora delar fungerat även vid elavbrott. IP-telefoni är dock sårbarare för avbrott i strömförsörjningen.

IP-telefoni kan ses som en tjänst bland andra i datanäten. Med detta följer även att IP-telefoni är exponerat för IT-hot på samma sätt. Ett sätt att skydda IP-telefonitrafiken är att logiskt separerar den från annan datatrafik i näten.

Alla IP-telefonitjänster erbjuder inte nödsamtal och lokalisering av nödsamtal är ibland problematiskt.

I rappporten redovisas tre scenarier som syftar till att konkretisera möjliga konsekvenser för samhället vid övergång till IP-telefoni.

Nyckelord

IP-telefoni, sårbarhet, konsekvenser, samhälle, scenarier, IT-säkerhet, reservkraft, kris,

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 33 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	FOI-R--1528--SE	Base data report
	Programme Areas 1. Security, safety and vulnerability analyses	
	Month year January 2005	**Project no.** E1895
	Subcategories 13 Support to Security, Safety and Preparedness	
	Subcategories 2	

Author/s (editor/s)	Project manager
Svante Barck-Holst Henrik Christiansson Arne Vidström	Svante Barck-Holst
	Approved by Staffan Molin
	Sponsoring agency PTS
	Scientifically and technically responsible Svante Barck-Holst

Report title (In translation)

A Vulnerability Perspective on VoIP

Abstract (not more than 200 words)

This report presents the results of a project, for the National Post and Telecom Agency (PTS), in which VoIP is studied from a vulnerability perspective. The aim of the project has been to study vulnerabilities of VoIP and the possible consequences for society that the transition to VoIP will have. Another goal has been to identify issues in the area that needs further attention or deeper studies.

Within the project three main areas were studied; power reserves, information security and emergency calls.

The traditional circuit-switched telephony has been well provided with power reserves and has therefore largely been available also during power black-outs. However, VoIP is more vulnerable to power black-outs.

VoIP can be seen as a service among others in computer networks. This also means that VoIP is exposed to electronic attacks. A way of protecting VoIP traffic is to separate it logically from other data traffic in the network.

Not all VoIP services offer emergency call services and localization of emergency calls is sometimes problematic.

Three scenarios are also presented; the purposes of the scenarios are to illustrate possible consequences of a transition to VoIP.

Keywords

VoIP, vulnerability, consequences, scenarios, information security, power reserve, crisis

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 33 p.
	Price acc. to pricelist