IT-säkerhet i GTRS:

Riskinventering och scenarier

AMUND HUNSTAD, HENRIK KARLZÉN OCH JACOB LÖFVENBERG

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--2980--SE
ISSN 1650-1942

Underlagsrapport
April 2010

Informationssystem

Amund Hunstad, Henrik Karlzén och Jacob Löfvenberg

IT-säkerhet i GTRS:

Riskinventering och scenarier

Titel	IT-säkerhet i GTRS: Riskinventering och scenarier
Title	IT security in GTRS: Risk inventory and scenarios
Rapportnr/Report no	FOI-R--2980--SE
Rapporttyp Report Type	Underlagsrapport
Månad/Month	April
Utgivningsår/Year	2010
Antal sidor/Pages	55 p
ISSN	ISSN 1650-1942
Kund/Customer	FMV
Projektnr/Project no	E530914
Godkänd av/Approved by	Anders Törne

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

I denna rapport redovisas resultatet av FOI:s problematiserande studie rörande IT-säkerhet i Gemensamt Taktiskt Radiosystem, GTRS. Med utgångspunkt i ett antal riskfaktorer identifierade vid ett arbetsseminarium med FOI-expertis, har en riskinventeringsmodell tagits fram. Riskinventeringsmodellen relaterar de olika riskfaktorerna till varandra.

Med riskfaktorer avses aktörer, aktiviteter, sårbarheter, och de hot som bygger på dessa liksom de möjliga skadorna. Identifierade riskfaktorer redovisas med korta beskrivningar och diskussioner. Varje riskfaktor förses också med en risknivå-bedömning.

För att relatera riskfaktorer till tänkbara verksamhetssituationer som GTRS ingår i, beskrivs i scenarioform några relevanta exempel på händelsekedjor av riskfaktorer. Utöver riskfaktorer har också ett antal övergripande problemområden, av vikt att analysera inför kommande GTRS-utveckling, identifierats och tagits upp till diskussion.

Riskinventeringen utgör huvudresultatet av studien och är ett underlag för prioriteringar av vad som kräver mera ingående granskning. Resultatet av studien är likaså ett underlag för kommande arbete med en IT-säkerhetsarkitektur för GTRS.

Nyckelord: GTRS, IT-säkerhet, riskinventeringsmodell, Försvarsmaktens gemensamma riskhanteringsmodell, risk, riskfaktorer, aktörer, aktiviteter, sårbarheter, hot, skador

Summary

This report accounts for the result of a problem-oriented study performed at the Swedish Defence Research Agency (FOI) regarding IT security in the software defined radio system GTRS. A number of risk factors, identified at a workshop with FOI-expertise, were used as a starting point to produce a risk inventory model. The risk inventory model relates different risk factors to each other.

Risk factors include actors, activities, vulnerabilities and the threats based on these as well as the implied damage. The identified risk factors are accounted for by short descriptions and discussions. Each risk factor is also associated with a risk level estimate.

To relate risk factors to conceivable operational situations where GTRS is used, some relevant examples of event chains of risk factors are described in the form of scenarios. In addition to the risk factors there are also a number of general problem areas, of importance for analyzing prior to future GTRS-development, which are identified and discussed.

The risk inventory is the main result of this study and as such constitutes the basis for a prioritization of candidates for future, detailed examination. The result of this study is also a basis for future work regarding an IT security architecture for GTRS.

Keywords: GTRS, IT security, risk inventory model, Swedish Armed Forces joint risk management model, risk, risk factors, actors, activities, vulnerabilities, threats, damages

Innehållsförteckning

1 Inledning

Gemensamt Taktiskt Radiosystem, GTRS, är ett system som är under utveckling med sikte på att tillhandahålla förbättrade såväl som nya tjänster för Försvarsmakten. GTRS förväntas erbjuda betydande flexibilitet i jämförelse med dagens radiosystem. Samtidigt kan det noteras att GTRS är ett komplext system.

Balansgången mellan flexibilitet och komplexitet medför betydande IT-säkerhetsutmaningar. Inom FOI:s projektet om IT-säkerhet i GTRS ingår deluppgifter med fokus på att identifiera sårbarheter, hur hot kan utnyttja dessa och vilka risker detta medför samt att med detta som utgångspunkt formulera en IT-säkerhetsarkitektur för GTRS.

I denna rapport belyses hur kedjan sårbarhet-hot-skada-risk påverkar dynamisk IT-säkerhetshantering i programvaruintensiva system i nätverk. För att på ett kostnadseffektivt sätt välja, förvalta och genomföra säkerhetsåtgärder krävs betydande kunskap och förståelse rörande tänkbara attacker respektive relevanta motåtgärder. En möjlig attack utgör ett hot genom att kunna utnyttja en sårbarhet i systemet och därmed ge upphov till en skada. Till varje sådan kedja kan en risk associeras.

Vilka attacker som är möjliga och praktiskt genomförbara varierar över tid, vilket ger en betydande dynamik avseende hot- och riskbild. Det krävs därmed en adekvat dynamik även i säkerhetshanteringen. För att belysa detta har vi konstruerat ett urval scenarier med tänkbara attacker mot systemet GTRS, varefter adekvata säkerhetsåtgärder identifieras och kort beskrivs.

Våra frågeställningar rör i princip GTRS som system, oberoende av vilken apparat som används. Dock är diskussionen med naturlighet präglad av Ra7201 eftersom det i dagsläget är den enda apparat som finns för GTRS. Vi kommer genomgående att använda begreppet GTRS även när det rör egenskaper som är knutna till apparaten. Detta gör vi för att slippa gränsdragningsfrågor angående vad som är systemegenskaper och vad som är apparategenskaper. Just den gränsdragningsfrågan är heller inte så betydelsefull så länge det bara finns en sorts apparat för GTRS.

Komplexiteten och flexibiliteten hos GTRS såväl som i de verksamheter där GTRS planeras ingå nödvändiggör en riskinventering. Med riskinventering avses här en översyn av vilka oönskade händelser som kan tänkas inträffa, bakomliggande faktorer som leder fram till händelserna och en risknivåbedömning av händelserna. I denna rapports inventering kategoriseras dessa bakomliggande faktorer som sårbarheter och hot. Då GTRS fortfarande är ett koncept och system under utveckling har denna inventering en övergripande karaktär.

Som start på arbetet genomfördes 2009-10-06 ett FOI-internt arbetsseminarium som närmare beskrivs i [3]. En avsikt med seminariet var att dess resultat skulle

bearbetas vidare för att konstruera IT-säkerhetsrelevanta scenarier, vilket är det arbete som beskrivs i denna rapport. Arbetsseminariet resulterade i ett relativt omfattande material av sårbarheter, hot, skador, risker och mer problematiserande säkerhetsfunderingar relaterade till GTRS.

I efterarbetet har detta material sorterats och grupperats, vilket har utmynnat i en riskinventeringsmodell för IT-säkerhetsfrågorna baserat på begreppskedjan sårbarhet-hot-skada-risk, utökad med några ytterligare delar. Utgående från bakgrundsresonemang i kapitel 2, beskrivs riskinventeringsmodellen i kapitel 3 och i kapitel 4 beskrivs de riskfaktorer som var resultatet av arbetsseminariet. I kapitel 5 presenteras och diskuteras framtagna scenarier, beskrivna i termer av riskinventeringsmodellen. Dessa scenarier eftersträvar att relatera sårbarheter, hot, skador och risker till tänkbara verksamhetssituationer där GTRS ingår. I kapitel 6 diskuteras identifierade övergripande problemområden som accentuerar centrala avvägningar inför vidare GTRS-utveckling. Kapitel 7 innehåller en sammanfattande diskussion som indikerar möjliga prioriteringar och val inför vidare utvecklingsarbete.

2. Bakgrund

I detta bakgrundskapitel ingår en genomgång av för inventeringen viktiga begrepp, en presentation av Försvarsmaktens gemensamma riskhanteringsmodell samt en kort metodikdiskussion.

2.1. Terminologi

För resonemangen i rapporten är begreppskedjan *sårbarhet – hot – skada – risk* central. Begreppen är nära relaterade till varandra och till säkerhetsmässiga resonemang och analyser.

Det är inte ovanligt att säkerhetsrelaterade begrepp används inkonsekvent vilket leder till missförstånd, oklar analys och felaktiga beslut. Sårbarhet, hot och risk definieras i SIS HB 550 [6] som:

- *Sårbarhet:* Kritiskt beroende av en tillgång (eng.: vulnerability)
- *Hot:* Möjlig, oönskad händelse med negativa konsekvenser för verksamheten (eng.: threat)
- *Risk:* Kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad (eng.: risk)

Begreppet svaghet är nära relaterat till sårbarhet och med samma engelska översättning definierar SIS HB 550 [6] begreppet svaghet som:

> *Svaghet:* Brist i skyddet av en tillgång exponerad för hot (eng.: vulnerability)

Det kan noteras att Försvarsmaktens gemensamma riskhanteringsmodell (FGR) [2] använder begreppen sårbarhet, hot och risk och med referens till SIS HB 550 [6][1]. Dock definieras sårbarhet i FGR som ”Brist i skyddet av en tillgång exponerad för hot”. Med andra ord används definitionen av begreppet svaghet, från SIS HB 550, för att definiera sårbarhet. Definitionen av sårbarhet, enligt SIS HB 550, utgår ifrån en aktörs eller verksamhets beroende av en tillgång, vilket här innebär ett beroende av GTRS eller funktionalitet i GTRS. Definitionen av svaghet enligt FGR utgår däremot ifrån tillgångens perspektiv genom att beakta brister i dess skydd, vilket här innebär att GTRS eller funktionalitet i GTRS har sina brister. Dessa brister kan en hotaktör utnyttja för att i nästa steg åstadkomma skada.

[1] I bilaga 15 i FGR [2] listas begrepp och förkortningar som riskhanteringsmodellen använder. Denna lista refererar flera gånger vidare tydligt till definitionerna enligt SIS HB 550 [6]. I FGR i övrigt används delvis andra begreppsreferenser, men med samma beskrivningar av innebörd.

Med tanke på GTRS planerade användande inom FM är det rimligt att eftersträva att använda FM:s terminologi. Att samma standardiserade terminologi används är en tydlig fördel vid vidare resonemang. Dessutom är användning av begreppet sårbarhet i FGR mer relevant för det arbete som beskrivs i denna rapport. Med andra ord, med en tyngdpunkt på teknisk analys är det lättare att utgå ifrån vad som brister i skyddet, än på vad som kan utgöra ett kritiskt beroende.

Begreppet skada definieras inte i SIS HB 550, däremot definieras där begreppet konsekvens som resultat av en händelse med negativ inverkan. FGR har en delvis annan definition av konsekvens som betonar värdet av den negativa inverkan. För att undvika begreppskonflikt väljer vi att införa begreppet skada för att beskriva de negativa resultat som kan uppstå i form av direkta, konkreta, resultat i system respektive i berörda verksamheter, det vill säga det som SIS HB 550 kallar konsekvens. Vilka hot i form av möjliga skadliga aktiviteter som kan leda till de identifierade skadorna är också av intresse att identifiera. Riskresonemang associerar sannolikheter till hoten och skadekostnader till de relaterade skadorna. Skador i GTRS-sammanhang är dels direkta skador i GTRS, dels skador för verksamheten i vilken GTRS ingår som system. Skador i verksamheten är i allmänhet av störst vikt att hantera. Direkta skador i GTRS kan tänkas vara omfattande och allvarliga, men om de inte medför skador i verksamheten, är problemen ändå klart avgränsade. Detta innebär att det är rimligt att fokusera på risken för skador i verksamheten och se skadorna i GTRS snarast som en startpunkt för verksamhetsskador.

Utgående ifrån ovan formulerade definitioner utgör hot möjliga händelser, vilka kan realiseras genom nyttjande av att sårbarheter i GTRS och resultera i skador. Sårbarheter är inneboende brister i GTRS, som en hotaktör kan utnyttja för att realisera ett hot. För att kunna realisera hot är hotagenter därmed beroende av att det existerar brister, det vill säga sårbarheter, i GTRS som går exploatera. Teoretiskt är det tänkbart att system utan brister kan existera, men den allmänna erfarenheten implicerar tydligt att system alltid är osäkra. Därmed är det rimligt att anta att sårbarheter alltid existerar och likaså hot.

Hot kan vara aktiva eller passiva samt avsiktliga eller oavsiktliga. Aktiva hot påverkar eller förändrar information eller systemdrift [6]. Passiva hot innebär endast läsning eller avlyssning, utan påverkan eller förändring [6]. Avsiktliga hot orsakas av någon aktör med illasinnat syfte, det vill säga med syfte att skada system eller verksamhet [6]. Oavsiktliga hot är slumpmässiga händelser som uppstår utan någon illasinnad aktör [6]. Det kan vara tal om hardvaru- eller mjukvarufel, naturfenomen eller mänskliga misstag.

Skador, i GTRS såväl som i den GTRS-relaterade verksamheten, innebär skadekostnader. För att bedöma möjliga utfall av skadekostnader är det synnerligen viktigt att genomföra en riskanalys. Risk kan definieras på olika sätt. En mycket använd definition är att risk är produkten av sannolikheten för en oönskad

händelse och den associerade skadekostnaden, vilket rör sig inom ramarna av definitionen i [6].

I denna rapport används en risknivåbedömning som en förenklad mätning av risk, då konkreta sannolikheter och skadekostnader har varit svåra att uppskatta. Detta har sin bakgrund i att GTRS fortfarande är ett system under utveckling.

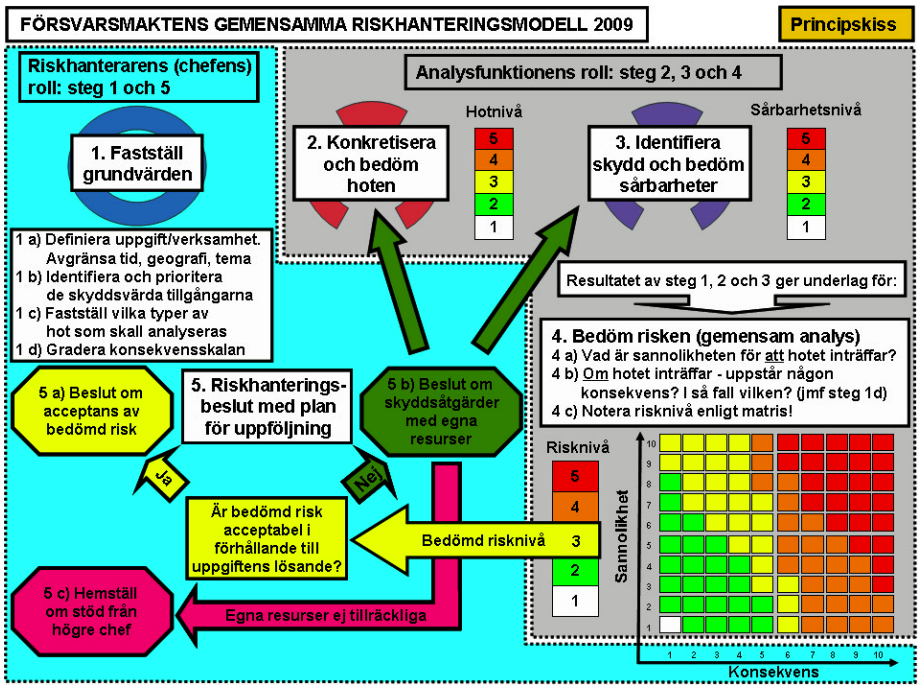
2.2. Försvarsmaktens gemensamma riskhanteringsmodell

Riskhantering kan genomföras på olika sätt. Som ett relevant exempel för GTRS presenteras här kort Försvarsmaktens gemensamma riskhanteringsmodell (FGR) [2]. I [5] jämförs FGR med ett urval riskhanteringsmodeller använda inom svenska civila myndigheter. Modellerna skiljer sig en del avseende mål, utformning och terminologi.

FGR är inte avgränsad till hantering av IT- och informationssäkerhetsrisker. Modellen ska användas för riskhantering vid militära operationer och skapa underlag för underbyggda och spårbara riskhanteringsbeslut. Ansvarsförhållanden rörande vem som har mandat att fatta riskhanteringsbeslut ska klarläggas och kommuniceras. Med detta generella anslag är det intressant att notera att terminologi rörande sårbarhet och hot refererar till en terminologilista för informationssäkerhet.

I FGR ingår fem steg, vilka rollfördelningsmässigt definieras som ingående i en besluts- respektive analysfunktion. Följande fem steg ingår i FGR, se Figur 1:

1. *Fastställ grundvärden (Beslutssteg).* Detta innebär att uppgiften eller verksamheten definieras med avseende på tidsomfattning, respektive var, av vem, varför och hur uppgiften/verksamheten ska genomföras. Likaså ska skyddsvärda tillgångar definieras och prioriteras. Det ska klargöras vilka hot som ska analyseras och konsekvensskalor ska fastställas.
2. *Konkretisera och bedöm hoten (Analyssteg)*
3. *Identifiera skydd och bedöm sårbarheter (Analyssteg)*
4. *Bedöm risken (Analyssteg gemensamt med beslutsfunktionen)*
5. *Riskhanteringsbeslut med plan för uppföljning (Beslutssteg)*



Figur 1: Försvarsmaktens gemensamma riskhanteringsmodell [2]

FGR har inte direkt styrt det här redovisade riskinventeringsarbetet. I stora drag kan dock den här redovisade riskinventeringen ses som ett förenklat genomförande av stegen 2 till 4 för GTRS, utan att ha satt in GTRS i en operativ verksamhetsram. Vidare arbete med framtagande av en IT-säkerhetsarkitektur för GTRS, utgående ifrån riskinventeringen, bör tydligt förhålla sig till FGR med dess olika analys- och beslutssteg.

2.3. Metodik för riskinventering

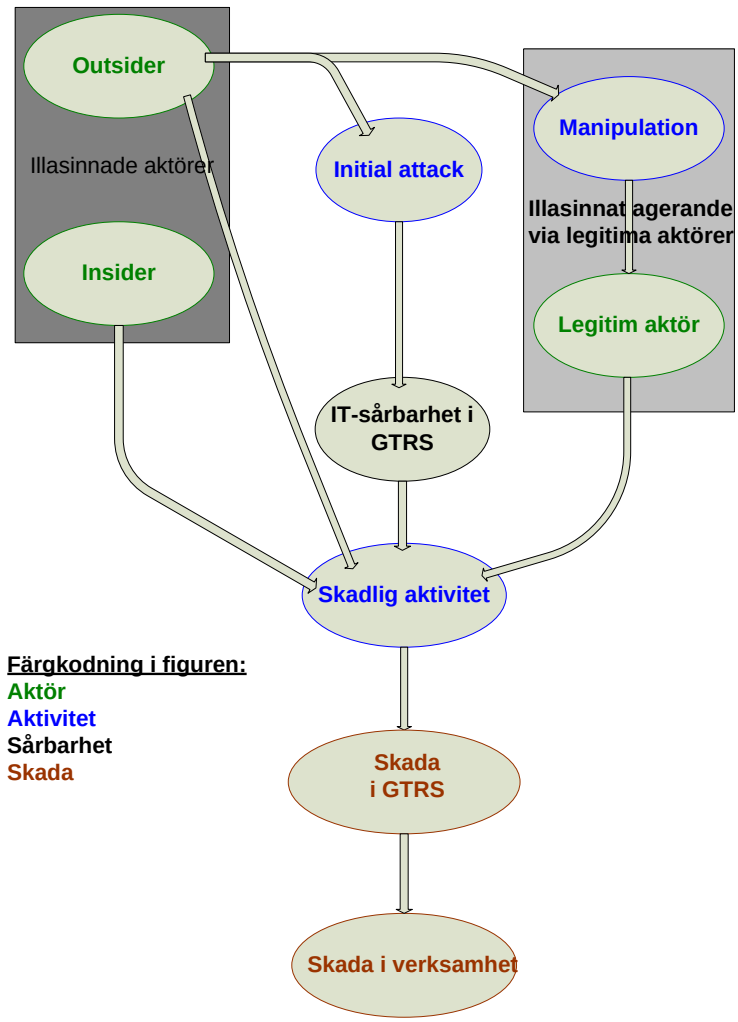
Det i denna rapport redovisade arbetet har till stor grad baserats på det arbetsseminarium som genomfördes 2009-10-06 med FOI-expertis inom IT-säkerhet respektive radio- och telekommunikation. Vid seminariet genomfördes tre separata brainstorming-sessioner, vilket resulterade i en relativt omfattande mängd av identifierade möjliga sårbarheter, hot, skador, risker samt problematiserande säkerhetsreflektioner och -observationer.

Sortering, gruppering och gallring bland dessa resultat från seminariet skedde i efterhand inom projektgruppen. En riskinventeringsmodell för GTRS-relevanta aktörer och aktiviteter togs fram som underlag för vidare analys och diskussion.

Vid riskinventeringen bedömdes enskilda händelser relaterade till riskinventeringsmodellen på en enkel femgradig skala för risknivå.

3. Riskinventeringsmodell

Analys av ett system av GTRS komplexitet med avseende på tänkbara sårbarheter, hot, skador och risker är arbetskrävande. Detta nödvändiggör mer övergripande beskrivningar och utgångspunkter för analys. Med detta som bakgrund valdes att i form av en övergripande riskinventeringsmodell relatera de viktigaste aktörs- och aktivitetskategorierna till varandra, Figur 2.



Figur 2: Riskinventeringsmodell över GTRS-relevanta aktörs- och aktivitetskategorier, sårbarheter och skador

Vidare är tanken att denna riskinventeringsmodell kan användas för analys av händelsekedjor av sårbarheter, hot, skador och risker respektive för analys av utifrån händelsekedjor uppbyggda scenarion.

Modellen är ett resultat och tolkning av det arbetsseminarium där olika sårbarheter, hot och skador identifierades och vid senare strukturering placerades ut som tillhörande de olika aktörs- och aktivitetskategorierna. Varje identifierad enskild aktör, aktivitet etc. beskrivs och ges en risknivåbedömning i kapitel 4. Denna strukturering av det resulterande materialet från arbetsseminariet gjorde det möjligt att prioritera och gallra i materialet. Exempelvis medförde gallringen att sårbarheter och hot med fokus helt på fysisk säkerhet togs bort, då dessa bedömdes som mindre relevanta med avseende på IT-säkerhet.

I och med att riskinventeringsmodellen och de enskilda identifierade aktörerna, aktiviteterna etc. är ett resultat och en tolkning av arbetsseminariet, är det fullt tänkbart att materialet kan struktureras på andra sätt och med andra identifierade enskilda aktörer, aktiviteter etc.

I riskinventeringsmodellen ingår

- *Aktörer:* Outsiders, insiders, legitima aktörer
- *Aktiviteter:* Initiella attacker, manipulation, skadliga aktiviteter
- *Sårbarheter:* IT-sårbarheter i GTRS
- *Skador:* Skador i GTRS, skador i verksamhet
- *Händelsekedjor:* Aktörer, aktiviteter, sårbarheter och skador sammanlänkade med pilar i riskinventeringsmodellfiguren.

Aktörer i modellen är de som initierar eller genomför hot, dvs. hotaktörer. I och med att legitima aktörer kan utsättas för manipulation är dessa i detta avgränsade sammanhang också hotaktörer.

Riskinventeringsmodellfigurens pilar binder ihop aktörer, aktiviteter, sårbarheter och skador till händelsekedjor. Händelsekedjorna åskådliggör hur hot emanerar från hotaktörer – eventuellt via en initial attack eller manipulation av legitima användare – fram till att skada uppstår i GTRS och i verksamheten i vilken GTRS ingår. Med andra ord är det i ett samspel mellan aktörer och aktiviteter som hot uppstår.

I de fall där en outsider – en extern, illasinnad aktör – genomför en initial attack går händelsekedjan vidare via utnyttjandet av en eller flera sårbarheter. Sårbarheter i GTRS är, som tidigare definierats, brister i skyddet av GTRS. De sårbarheter i GTRS som indikeras i riskinventeringsmodellfiguren är de som är relaterade till IT och IT-säkerhet. Som inneboende ej önskvärda egenskaper i GTRS kan dessa utnyttjas för att möjliggöra skadlig aktivitet. Den skadliga aktiviteten medför skada i GTRS, vilket slutligen medför skada i verksamheten i vilken GTRS ingår.

En initial attack är den åtgärd med vilken hotaktören öppnar en första ingång till GTRS. Den initiala attacken räcker i normalfallet inte till för att exploatera en sårbarhet så långt att en skada kan uppstå i GTRS, än mindre i verksamheten som är beroende av GTRS.

En outsider kan istället för att gå via en initial attack välja att manipulera en legitim aktör. Manipulation kan ske i form av social ingenjörskonst, hot eller mutor. Därmed kan outsidern, som inte har åtkomst till GTRS, på ett illegitimt sätt skaffa sig åtkomst till GTRS via den legitima aktören. Via manipulation kan skadlig aktivitet initieras och medföra skada. Vad som här kan noteras är att ingen sårbarhet i GTRS utnyttjas. Däremot utgör i sådana fall den legitima aktören en sårbarhet som en outsider som hotaktör kan utnyttja.

Skadlig aktivitet kan också initieras direkt av outsidern, utan utnyttjande av IT-sårbarheter i GTRS. Vad som åsyftas här är skadliga aktiviteter som på ej IT-relaterade sätt åstadkommer skada i GTRS och berörd verksamhet. Exempelvis kan det vara tal om strålning eller sprängning av GTRS. Även i dessa fall är det i någon mening sårbarheter som utnyttjas, men inte IT-sårbarheter vilka här är i fokus.

En ytterligare hotaktör återstår att beskriva: Insidern – en intern, illasinnad aktör. En insider är, som illustreras i riskinventeringsmodellfiguren, en legitim aktör som utan direkt föregående manipulation, väljer att utnyttja sin legitima åtkomst till GTRS för att direkt utföra en skadlig aktivitet med påföljande skada i GTRS och verksamheten. Inte heller här utnyttjas någon sårbarhet i GTRS, men insidern utgör i sig en sårbarhet.

Skador i den av en IT-incident direkt berörda verksamheten kan ofta anses vara allvarligare än den direkta konsekvensen i GTRS. Exempelvis kan sekretessbelagt innehåll i en fil tänkas bli läst av en illegitim användare. Detta behöver inte medföra någon egentlig konsekvens för GTRS, annat än att någon har forcerat skyddsmekanismer. Däremot kan skadorna inom en berörd verksamhet vara betydligt mer omfattande. Det kan till exempel vara tal om att taktisk information röjs av en motståndare, vilket i en stridssituation kan vara direkt förödande.

Den skadliga aktivitetens omfattning och komplexitet kan variera. Detsamma gäller för skador som kan uppstå i GTRS, såväl som i verksamheten. Detta implicerar behov av riskanalys och riskhantering. Riskinventeringsmodellen innehåller inte dessa begrepp explicit, men utgör en god utgångspunkt för ett sådant vidare arbete. Försvarsmaktens gemensamma riskhanteringsmodell, [2], är för en sådan fortsättning ett adekvat och relevant ramverk att använda som redskap.

4. Riskinventering

I detta kapitel, som bygger på riskinventeringsmodellen från det förra kapitlet, beskrivs enskilda riskfaktorer. Riskfaktorer är i enlighet med riskinventeringsmodellen aktörer, aktiviteter, sårbarheter, och de hot som bygger på dessa liksom de möjliga skadorna.

För varje enskild riskfaktor redovisas, förutom en problemdiskussion, en risknivåbedömning. Risknivåbedömningen är en sammanvägning av sannolikheten för att ett hot realiseras samt allvarlighetsgraden av skadan som kan uppstå. Faktorer som påverkar sannolikheten är hur svårt det är för en hotaktör att realisera hotet på ett visst sätt, hur stor och kraftfull organisation som krävs samt hur lång tid som hotaktören måste lägga ner. Dessutom vägs det in hur lätt det är att skydda sig. Komplexiteten i GTRS samt det faktum att det inte går att styra över vissa av de ingående komponenterna, såsom standardprotokoll, gör att det inte alltid är uppenbart hur sannolikheten och den skadeverkan som kan uppstå ska minskas och till vilken grad det överhuvudtaget är möjligt. Eftersom GTRS fortfarande är ett system under utveckling, är det inte möjligt att göra exakt bedömningar av sannolikheter och skadekostnader. Därför har exakta risknivåvärden bytts ut mot heltal i intervallet 1 till 5, där 1 är minst allvarlig och 5 är mest allvarlig. Risknivåvärden bör därför främst användas för att avgöra inom vilka enskilda riskfaktorer och problemområden som ytterligare insatser och resurser ska satsas.

Risknivåbedömningen är inte resultatet av någon metodisk analys utan istället en gemensam bedömning av författarna. Denna subjektiva metod för värdering har valts eftersom det är svårt att hitta en objektiv metod att applicera på översiktligt beskrivna problem. Vi menar dock att det, denna kritik till trots, finns information att hämta ur bedömningarna eftersom de är gjorda mot bakgrund av stor allmän kunskap om IT-säkerhet och en god förståelse för designen av GTRS som den ser ut idag.

I avsnitten 4.8, Skador i GTRS och 4.9, Verksamhetsskador görs inga risknivåbedömningar. Skadorna kan uppnås på många olika sätt, vilket gör sannolikhetsbedömning i det närmaste omöjlig. Dessutom är i princip alla skadorna mycket allvarliga och svåra att skilja mellan vad gäller allvarlighetsgrad.

4.1. Outsiders

Med outsiders avses illasinnade aktörer som inte har någon särskild, betrodd position i systemet, dvs. de finns på utsidan av systemet. I denna grupp återfinns både hotaktörer som är ute efter just GTRS och hotaktörer som genomför oriktade attacker utan att kanske ens känna till GTRS existens. Nedan presenteras

några olika grupper av outsiders tillsammans med en diskussion av deras egenskaper.

4.1.1. Internet-aktörer

Bedömd risknivå: 2

GTRS är i huvudsak IP-baserat, både på röd och svart sida. Det innebär att något av de anslutna näten kan ha konnektivitet med Internet; om inte direkt så via andra nät längs vägen. Om sådan konnektivitet finns blir GTRS per automatik utsatt för alla de hot som kan finnas på Internet. Dessa är i allmänhet oriktade och dessutom anpassade för andra plattformar än GTRS, men ett visst ”grundbrus” måste varje enhet som är ansluten till Internet tåla. Om det är känt att GTRS har internetkonnektivitet är det också möjligt att riktade attacker genomförs den vägen, av mer eller mindre resursstarka hotaktörer.

Det kommer antagligen att finnas många fall där internetkonnektivitet aktivt undviks. Det är dock också möjligt att tänka sig fall där det är önskvärt att avlasta en kapacitetssvag radiokanal genom att koppla in det svarta ethernetgränssnittet till någon typ av IP-nät som är mindre kontrollerat, men har större kapacitet än radionäten. Om GTRS kan designas på ett sätt så att detta kan göras med upprätthållande av en tillräcklig säkerhetsnivå skulle det kunna vara en värdefull möjlighet.

Även om internetkonnektivitet skulle innebära lägre säkerhet så kommer systemet troligen att vara på en helt annan nivå säkerhetsmässigt än de allra flesta system på Internet. Det bakgrundsbrus som finns med exempelvis diverse skadlig kod och automatiserade intrångsförsök bör knappast utgöra något större hot i sig, men på grund av den stora mängden och möjligheten för mer riktade angrepp kan man inte helt negligera hotet. Den bedömda risknivån blir därför 2.

4.1.2. Samarbetspartners

Bedömd risknivå: 2

Samarbetspartners i koalitioner kan vara av olika slag. Variationsrikedomen medför tänkbara hot i och med att intentioner, ageranden och beteendemönster kan variera betydligt mellan olika grupper inom samma koalition. Inte minst är det svårt att utöva kontroll över varierande partners.

Varje form av samarbete kräver kommunikation. Om denna kommunikation till exempel görs med någon sorts koalitionsvågform som körs i GTRS, blir det med nödvändighet så att de man samarbetar med får en specialstatus gentemot GTRS. Om inte annat är de en godkänd avsändare för meddelanden som man vill ta emot. Om dessa meddelanden är IP-baserade, vilket synes rimligt, har någon sorts sammankoppling mellan näten skett, vilket skulle kunna innebära att IP-

baserade attacker eller liknande läcker mellan näten. GTRS blir alltså till viss del påverkat av säkerheten i övriga sammankopplade nät, men har ingen reell möjlighet att påverka den.

Koalitionspartners har en särställning med eventuellt både mer behörighet i och kunskap om GTRS varför de skulle kunna utgöra ett farligt hot. Dock är troligtvis fallet att sådana aktörer sällan är illvilliga och på sin höjd kan man förvänta sig mindre skärmytslingar vid exempelvis mindre diplomatiska incidenter eller genom spionage trots att de normalt är potenta aktörer. Att andra hotaktörer tar vägen via koalitionspartners är fullt möjligt, men är troligtvis inte något större hot då hotaktören först måste infiltrera en kraftfull organisation innan den kan inrikta sig på GTRS. Därför blir den bedömda risknivån 2. Det är viktigt att poängtera att före detta koalitionspartners liksom före detta anställda har extra möjligheter att angripa systemet.

4.1.3. Icke-statliga organisationer

Bedömd risknivå: 1

Icke-statliga organisationer (non-governmental organisations, NGO) är exempel på samarbetspartners där intentioner, ageranden och beteendemönster kan vara betydligt annorlunda jämfört med militära partners och civila myndigheter. Det kan vara tal om kommersiella företag, ideella organisationer och samarbetsorganisationer. De utgör alltså ett specialfall av samarbetspartners där säkerhetsavvägningar och prioriteringar kan vara gjorda på ett sätt som inte uppfyller de krav man förväntar sig, och där man riskerar att interagera och kommunicera med aktörer med okänd säkerhetsnivå. Samtidigt kan dessa vara synnerligen värdefulla och viktiga partners.

Dessa organisationer har visserligen en lägre och mer obestämbar säkerhetsnivå men som illasinnade aktörer, så kallade hotaktörer, är de troligen förhållandevis resurssvaga och mindre intresserade av att angripa GTRS. Vidare är det sannolikt att de inte får tillgång till lika mycket information som koalitionspartners och inte heller får lika stora rättigheter i systemet. I och med detta bedömer vi det som mindre troligt att andra hotaktörer tar vägen genom icke-statliga organisationer eftersom det trots allt innebär ett extra moment. Därför bedöms risknivån till 1.

4.2. Insiders

Insiders arbetar för en motståndare eller sig själva men har någon sorts betrodd roll i GTRS, det vill säga de finns på insidan av systemet i någon bemärkelse. För att ta hänsyn till detta hot måste systemet antagligen ha någon sorts skydd även mot en motståndare med viss giltig behörighet. En lägsta rimlig nivå borde vara att systemet är motståndskraftigt mot motståndare med operatörs- och lägsta service/administrationsbehörighet. Naturligtvis går det inte att helt undvika att en

administratör med sådan behörighet laddar felaktiga kommunikationsparametrar. Däremot ska det inte vara möjligt för en sådan individ att påverka GTRS på sätt som medför inkorrekt, men ej observerbart felaktigt, systembeteende. För åtminstone de lägre behörighetsnivåerna är det önskvärt att fel som förs in är relativt lätta att upptäcka för angränsande roller.

Nedan presenteras några olika grupper av insiders tillsammans med en diskussion av deras egenskaper.

4.2.1. Anställda med oväntade sympatier

Bedömd risknivå: 2–5

Eftersom GTRS kommer att vara ett stort och välanvänt system i Försvarsmakten, kommer många individer att komma i kontakt med det. Detta innebär att åtminstone några av dem som interagerar med GTRS kan ha åsikter som till del överensstämmer med motståndarsidan. Det kan handla om ett slumpmässigt sammanträffande att någon med särskilda sympatier plötsligt befinner sig i en situation där lojaliteten är delad, eller att någon målmedvetet har sökt sig in i Försvarsmakten i syfte att hamna i en position där den kan agera utifrån sina sympatier.

Risknivån kan variera med kategori av anställd, den anställdes befogenheter och kompetens respektive vilken information denne har tillgång till. Om det är tal om en användare med begränsade befogenheter och utan större tillgång till sekretessbelagd information, är problemet mindre allvarligt. Däremot är problemet inte negligerbart, varför nivå 1 trots allt inte är aktuell. Om det däremot är tal om kryptologen som designade kryptolösningen, är risknivån betydligt högre.

4.2.2. Manipulerade anställda

Bedömd risknivå: 2–5

Även om en person inte har avvikande sympatier kan den, mot betalning, under hot eller genom att bli lurad, ha blivit en insider. De olika manipulerande aktiviteterna beskrivs närmare i avsnitt 4.4, Manipulation. Att manipulera någon att agera på ett sätt den normalt inte skulle göra, är inte enkelt. Illojalt agerande är sannolikt lättare att förmå någon till att göra i de fall där konsekvenserna av agerandet inte är tydligt. Till exempel kan detta gälla att lämna ifrån sig sekretessbelagd information i en fredlig situation i Sverige, kontra under en insats i Afghanistan. Om skadan dessutom är abstrakt till sin natur och svår att knyta till att någon tydligt drabbas, minskas troligen också motståndet mot manipulation.

Utöver detta underlättas manipulation också av om det är svårt att spåra det illojala agerandet åter till en viss aktör. Den illojala är i behov av att inte avslöjas. Vilken risk man är villig att ta för sitt illojala agerande beror därmed

också på vilka fördelar man själv får av agerandet, till exempel i form av betalning.

Risknivån kan liksom i avsnitt 4.2.1, Anställda med oväntade sympatier, variera beroende på den anställdes befogenheter.

4.3. Legitima aktörer

I [1] listas ett antal aktörer och deras funktion i GTRS, vilket upprepas här översatt till svenska. De flesta rollerna är sådana att de ger rättigheter som möjliggör ett agerande som skadar systemet eller dess funktioner.

De olika användarrollerna beskrivs nedan i termer av uppgifter och rättigheter. En intressant frågeställning att beakta är huruvida GTRS övervakar och upprätthåller användarrollernas definierade uppgifter och rättigheter. Om inte, är det tänkbart att en användare med lätthet kan agera utanför sin definierade roll.

I detta avsnitt finns inga bedömda risknivåer. Skälet är att en legitim användare som utgör ett problem per definition blir en insider, varför läsaren hänvisas till avsnitt 4.2, Insiders, för diskussion kring sådan riskbedömning.

4.3.1. Slutanvändare (user)

Rollen som slutanvändare är sannolikt den enda som inte kan skada systemet. Rollen syftar på individer eller system som använder de tjänster GTRS erbjuder. Med nuvarande design av GTRS har slutanvändarrollen inte rättigheter nog att kunna påverka systemet annat än på triviala sätt.

4.3.2. Radiooperatör (radio operator)

Rollen som radiooperatör är aktiv i fält och har som uppgift att konfigurera GTRS-noder så att de kan kommunicera. Det handlar om att ladda nycklar, konfigurationsfiler för kommunikation (så kallade commplaner), välja kanaler med mera.

Eftersom radiooperatörer har befogenhet att konfigurera GTRS-noder har de också möjlighet att konfigurera dem så att de inte fungerar eller så att de fungerar suboptimalt. Operatören har därmed tillgång till information som kan vara av värde för en motståndare som vill angripa GTRS.

4.3.3. Kommunikationsbefäl (communication officer)

Rollen som kommunikationsbefäl är aktiv i fält och har som uppgift att administrera konfigurationsfiler för kommunikation (så kallade commplaner).

Kommunikationsbefälet har alla rättigheter som radiooperatören, samt några ytterligare, till exempel att ändra i commplaner, modifiera användarroller och läsa driftsloggar. Kommunikationsbefälet har alltså ytterligare möjligheter att utföra skadliga aktiviteter jämfört med radiooperatören.

4.3.4. Systemadministratör (system manager)

Rollen som systemadministratör är aktiv i fält och har som uppgift att övervaka, konfigurera och underhålla GTRS, samt att utföra vissa reparationer.

Systemadministratören har ungefär samma rättigheter som kommunikationsbefälet, med de viktiga tilläggen att systemadministratören får uppgradera mjukvara i GTRS och får välja COMSEC/TRANSEC-nycklar.

Rätten att uppgradera mjukvara gör systemadministratören till en möjlig väg för den som vill föra inte skadlig kod i GTRS. Det skulle också kunna handla om att välja att föra in auktoriserade, men äldre mjukvaruversioner med kända sårbarheter för att på så sätt skapa en lättare situation för ett senare angrepp.

4.3.5. Serviceverkstad (service facility)

Funktionen som serviceverkstad är aktiv i fält, men inte alltid tillgänglig. Uppgiften är underhåll, mjukvaruuppgraderingar och att ladda den svarta delen av vågformsapplikationerna (WFA).

Serviceverkstaden har ungefär samma rättigheter som kommunikationsbefälet, med tillägg av rätten att importera vågformsapplikationer, och är därför känslig på ungefär samma sätt.

4.3.6. Kryptoverkstad (crypto facility)

Funktionen som kryptoverkstad är inte aktiv i fält. Uppgiften är att ladda algoritmer, ladda den röda sidan av vågformsapplikationer (WFA), ladda certifikat och att hantera manipuleringsskydd.

Kryptoverkstaden har mycket stora befogenheter inom säkerhetsområdet och kan skapa stora problem om verksamheten inte sköts korrekt.

4.3.7. Säkerhetsansvarig (security administrator)

Rollen som säkerhetsansvarig är aktiv i fält och har som uppgift att hantera loggar och verifiera manipuleringsskydd.

Den ur säkerhetssynvinkel väsentliga rättigheten som den säkerhetsansvarige har är rätten att exportera säkerhetsloggar. I den mån dessa innehåller information som är till nytta för en hotaktör så har den säkerhetsansvarige möjlighet att

hantera denna information på ett sätt som är skadligt. Det kan också finnas skäl för en hotaktör att vilja dölja delar i säkerhetsloggarna, vilket skulle kunna vara möjligt för den säkerhetsansvarige att göra.

Logghantering diskuteras närmare i avsnitt 6.2, Logghantering.

4.3.8. Superanvändare (superuser)

Rollen som superanvändare är endast aktiv under test- och utvecklingsfaser, och då bara i en kontrollerad miljö. Rollen tillåter alla aktiviteter i systemet, utom export av säkerhetsloggar.

Som framgår av namnet så är superanvändare en roll som har närmast full kontroll över alla delar i systemet och kan därför göra stor skada på många sätt. Det är därför mycket viktigt att ha extra kontroller för den roll som kan definiera rättigheter och därmed ändra rättigheter för existerande konton och till exempel lyfta ett konto till superanvändar-nivå.

4.4. Manipulation

En hotaktör kan på olika sätt påverka en legitim användare för att få denne att agera på ett sätt som gynnar hotaktören och därmed bli en insider som det beskrivs i avsnitt 4.2, Insiders. Det finns flera möjliga sätt att göra detta på och i detta avsnitt beskrivs några av dem.

4.4.1. Social engineering

Bedömd risknivå: 2

Med social engineering menas att lura människor så att de utför handlingar som hotaktören vill och som de annars inte skulle ha gjort. Ofta handlar det om att hotaktören på olika sätt inger tillräckligt mycket förtroende för att offret ska lita på hotaktören även när objektiva skäl för detta saknas. I GTRS-sammanhang skulle det kunna handla om att övertyga en vakt om att ge tillträde till en GTRS-nod utan att hotaktören behöver uppvisa dokumentation som styrker dennes rätt till, och behov av, att få tillträde.

Social engineering-attacker har visat sig vara mycket effektiva, [4]. En pålitlig uppsyn tillsammans med en bra historia och god kunskap om relevanta detaljer i sammanhanget räcker långt för att förmå människor att bortse från reglementen och sunt förnuft. Hur långt sådant räcker i en militär organisation är svårt att veta, men det torde inte gå att helt bortse från möjligheten att genomföra en sådan attack.

Social engineering är ett allvarligt problem, som ofta negligeras eller ges för liten prioritet. I GTRS-sammanhang är bedömningen ändå att risknivån kan sättas till

2, ty GTRS är ett säkerhetsmässigt specialdesignad system som används i hårt regelstyrda sammanhang och organisationer. Dessutom kan man utgå ifrån att användarna också är väl orienterade och utbildade i gällande reglementen och rutiner.

Det torde därmed kräva en stor insats för att lyckas med social engineering i en så hårt reglerad situation, vilket talar för 2 som nivåbedömning. Lägre nivåbedömning känns dock inte rimligt, ty en sådan attack skapar en insider vilket ger stora problemskapande möjligheter.

4.4.2. Utpressning

Bedömd risknivå: 2–4

Med hjälp av utpressning går det att påverka de flesta människor så att de agerar på ett sätt som de annars aldrig skulle göra. Det är inte enkelt att skydda sig mot den här typen av hot. Det finns många individer som någon gång under systemets livstid är i position att påverka det på ett skadligt sätt. Om man ska skydda sig mot det här problemet fullt ut leder det till stora komplikationer eftersom man inte längre kan ha förtroende för sina medarbetare.

Risknivån har satts utifrån en bedömning att vem som utpressas påverkar allvarligheten mycket. Inom sammanhang och organisationer där GTRS används är rimligen individer som innehar roller värda att utpressa skyddade av att deras roller inte på något sätt blir öppet tillgängliga. Därmed bedöms även att risknivå 5 inte är aktuellt, då individer som kan vara aktuella för en sådan bedömning torde vara de allra mest skyddade och svåra att hitta för en manipulerande aktör.

4.4.3. Betalning

Bedömd risknivå:2–3

På samma sätt som människor går att hota går många människor att köpa, och resonemanget blir motsvarande som i avsnitt 4.4.2, Utpressning. Det går dessutom utmärkt att kombinera utpressning och betalning för att förstärka effekten. Oavsett vilket så blir effekten densamma som vid utpressning; det är bara en fråga om hur hotaktören övertygar offret om att samarbeta. Risknivån bedöms utifrån att det rimligen är svårare att köpa än utpressa.

4.5. Initiala attacker

Attacker, primärt medvetna och planerade attacker, utgör tydliga hot. Dessa kan ske med såväl automatiska som manuella verktyg och åtgärder. Utvecklingen av verktyg går mot verktyg som kan utnyttjas av amatörer, men som även kan användas med utökad verkan av specialister. Intrång är kanske det mest uppenbara

och rättframma IT-relaterade hotet mot IT-system. Det är dock ännu mer relevant nu än tidigare eftersom man med den allmänt spridda IP-tekniken byggt ett system av system som har konnektivitet över mycket stora avstånd, kanske till och med globalt. Om en hotaktör lyckas göra ett intrång med fullständigt övertagande av en GTRS-nod kan det ge mycket stora möjligheter att agera i det bakomliggande IP-nätet, i kraft av identiteten som giltig GTRS-nod.

Nedan presenteras och diskuteras några klasser av möjliga attacker mot GTRS.

4.5.1. Utnyttjande av bakdörrar

Bedömd risknivå: 2

Komplexiteten hos GTRS möjliggör fientligt agerande eller spaning via dolda eller för legitima aktörer okända ingångar (bakdörrar). En existens av sådana ingångar till systemet skapar svårdetekterade sårbarheter. Kommunikationsbeteenden som kan vara svåröverskådliga, exempelvis i stora koalitioner, kan implicera hot. Illegitim kommunikation kan dölja sig i volymen av legitim trafik.

I riskbedömningen ingår en uppskattning av sannolikheten för att bakdörrar existerar, huruvida de kommer att utnyttjas och med vilken konsekvens. Som bakdörr räknas här inte in renodlade programmeringsmissar, vilka kan fungera som en bakdörr. Bakdörr är här avgränsat till ingångar skapade av illasinnade aktörer, en typ som även berörs i avsnitt 4.6.9, Utvecklingsprocess, och ingångar för tester och underhåll för systemets programmerare.

Vid bedömningen har det förutsatts att mjukvaruleverantören har genomfört bland annat noggrann kodgranskning innan leverans. Likaså förutsätts att svenska instanser har genomfört motsvarande aktiviteter. Därmed torde de högre risknivåerna kunna undvikas. Samtidigt bedöms den lägsta nivån inte vara aktuell, ty om attacken lyckas blir konsekvenserna relativt allvarliga.

4.5.2. Virus, maskar och trojaner

Bedömd risknivå: 2

Olika typer av illasinnad mjukvara, såsom virus, maskar och trojaner, kan medföra störningar i kommunikationsflödet. I det fall attacken är framgångsrik kan också olika sorters påverkan på informationen i noderna genomföras. Även om inte GTRS är sårbart i sig självt, kan illasinnad mjukvara spridas i kringliggande system och fylla radionätet med attackförsök så till den grad att det blir svårt att kommunicera verkliga data på ett tillräckligt snabbt och effektivt sätt.

Riktade attacker mot GTRS kräver förmodligen en resursstark hotaktör med ingående kunskap om systemet och dessutom möjlighet att nå fram med attacken. Detta är alltså en mer osannolik attack, men desto allvarligare om den faktiskt genomförs.

Oriktade attacker via illasinnad mjukvara bedöms inte vara något större problem. GTRS är i förhållande till andra system specialutvecklat, även med avseende på säkerhet. Allmänt spridd illasinnad mjukvara torde därför rimligen inte utgöra ett problem. En högre nivå än den bedömda faller huvudsakligen bort baserat på att det antagligen är enklare att genomföra andra typer av attacker än via illasinnad mjukvara. Att nivån ändå inte fallit till den lägsta beror på att en riktad attack från en kvalificerad motståndare i princip kan vara mycket kraftfull och resultatet vid en lyckad attack är mycket allvarligt.

4.5.3. Protokollattacker

Bedömd risknivå: 3

Med protokollattacker menas attacker som inte är riktade mot implementationsdefekter i olika slags mjukvara, utan som istället nyttjar sårbarheter i specifikationerna i ingående protokoll. Om protokollen innehåller sårbarheter kan attacker genomföras trots att implementationen av protokollen är helt korrekt. Detta är en obehaglig typ av säkerhetsproblem eftersom den är svår att lösa med uppdateringar om det inte är möjligt att samtidigt uppdatera alla kringliggande system som använder samma protokoll. Typiskt ger protokollattacker inte hotaktören möjlighet att överta noder eller exekvera godtycklig kod, men exempelvis är kommunikationsbortfall och bruten sekretess möjliga konsekvenser.

Protokollattacker har bedömts ligga på risknivå 3, då de bygger på sårbarheter i protokoll vars design GTRS-utvecklingskollektivet inte har någon egen kontroll över. Protokollen ser ut som de gör, och de är inte alltid utvecklade med säkerhet i fokus. Att risknivån trots detta inte bedömts som högre har sin grund i att det är välkända protokoll som använts och granskats under lång tid i en mängd olika sammanhang, så de flesta problem som kan finnas borde vara kända vid det här läget.

4.5.4. Manuella nätbaserade attacker

Bedömd risknivå: 3

Om mjukvara någonstans i systemet är behäftad med fel så skulle en noggrant designad signalsekvens kunna innebära att hotaktören påverkar det interna tillståndet i maskinen på ett sätt som ger säkerhetsproblem. Exempel är att delar av maskinen skulle kunna krascha, kanaler kopplas samman eller säkerhetsfunktioner stängas av. Även införande av körbar kod skulle kunna göras på detta sätt. Vissa typer av maskar på Internet har använt den här typen av sårbarhet för att infektera nya maskiner. Utan kryptoskydd under länklagret går det inte att fullt ut skydda sig mot denna typ av attack, eftersom det på alla ingränssnitt finns mjukvara som på lägsta protokollnivå tar emot de data som kommer innan de autentiserats eller verifierats.

Den här typen av attack är den man normalt förknippar med hackning i vid bemärkelse. En kompetent individ, eller en grupp av individer, som manuellt spanar, kartlägger, undersöker och slutligen genomför attacker är ett allvarligt hot, speciellt då försvarsmekanismerna inte kan vara fullständiga, varför en lägre risknivå än 3 inte kan komma på fråga. Att nivån inte bedömts vara högre beror på att det är en svår attack att genomföra eftersom GTRS rimligen skyddas av brandväggar och andra begränsande system. Därmed kommer GTRS vara svårt att få kontakt med för hotaktören. I allmänhet är GTRS, som en produkt avsedd för militärt användande, präglad av ett systematiskt säkerhetstänkande.

4.5.5. Radio-baserade attacker

Bedömd risknivå: 1

På samma sätt som andra gränssnitt kan attackeras, är de delar som tar emot och sänder, de så kallade UT:arna efter engelskans Universal Transceivers, möjliga att attackera. En attack mot en UT från radiogränssnittet är speciellt så till vida att radiogränssnittet är skyddat både av frekvenshoppning och av ett kommersiellt krypto (AES). Frekvenshoppningen gör det svårt för en hotaktör att sända information till GTRS när inte hoppsekvensen är känd. Möjligen går det att sända hela informationssekvensen på alla delkanaler parallellt, så att GTRS tolkar det som att sändarens hoppsekvens är korrekt. Detta kan radiomässigt vara svårt med krav på stora uteffekter och bredbandiga slutsteg och antenner, men borde vara i princip möjligt. Lyckas hotaktören komma förbi problemet med frekvenshoppningen är det möjligt för denne att angripa UT:n på lägsta protokollnivå, på det sätt som beskriv i avsnitt 4.5.4, Manuella nätbaserade attacker.

Vi har bedömt risknivån till 1, baserat på att radiogränssnittet skyddas av frekvenshopp och AES-kryptering, vilket gör det svårt för en hotaktör att överhuvudtaget uppnå konnektivitet med GTRS. Skulle detta trots allt lyckas finns fortfarande alla andra IT-säkerhetsmekanismer att forcera innan någon skadlig aktivitet kan initieras.

4.6. IT-sårbarheter i GTRS

I det här avsnittet presenteras ett antal sårbarheter, det vill säga brister i skyddet av GTRS. Dessa kan i enlighet med riskinventeringsmodellen användas för att initiera en skadlig aktivitet som kan medföra skada i GTRS eller i berörd verksamhet. Vissa av dessa är inte av den karaktären att de är direkta ingångar för attacker. Snarare är det mer allmänna egenskaper som kan vara besvärliga ur ett säkerhetsperspektiv eller vara grogrund för mer explicita problem.

4.6.1. Komplexa protokoll

Bedömd risknivå: 3

GTRS bygger i all väsentlighet på standardiserade protokoll från IP-världen. Standardiseringen kan utöver många uppenbara fördelar även medföra vissa sårbarheter. Exempelvis kan felkopplingar medföra att kommunikationsförmåga i enlighet med standard möjliggörs, men på ett sätt som inte är planerat, lämpligt eller önskvärt i GTRS. Vidare kan komplexiteteten hos standardiserade protokoll möjliggöra existensen av svårdetekterade sårbarheter. Ytterligare diskussion om problematiken kring standardiserade protokoll och standardlösningar i allmänhet återfinns i avsnitten 4.5.3, Protokollattacker och 6.4.1, Standardlösningar.

Denna sårbarhet har bedömts som risknivå 3 då den relaterar till protokoll vars design GTRS-utvecklingskollektivet inte har någon egen kontroll över. Protokollen ser ut som de gör, och de är inte alltid utvecklade med säkerhet i fokus. Att risknivån trots detta inte bedömts som högre har sin grund i att implementationen går att granska och att det är välkända protokoll som använts under lång tid.

4.6.2. Öppen svart ethernetport

Bedömd risknivå: 4

Den svarta ethernetporten har stora fördelar. Den kan fungera som ingång till UT:arna i en konfiguration där GTRS-noden har som enda funktion att ge svart IP-konnektivitet över radio. Den kan också fungera som utgång till ett trådat nät för en GTRS-nod som sitter t.ex. på en stabsplats. En annan möjlig användning är att koppla samman flera GTRS-noder via en extern switch/router och t.ex. tillåta routing mellan ett stort antal parallella radionät.

Det går också att se principiella svårigheter med denna ethernetport. Genom routern i GTRS-noden transporteras även nodintern information som möjligen skulle kunna spridas på ett felaktigt sätt genom denna port. Även påverkan utifrån på den nodinterna informationen är en möjlig form av angrepp via porten. Möjligheten till falsksignalering från utsidan diskuteras i avsnitt 4.7.9, Falsk kommunikation till kryptokanalen. Även rena överbelastningsattacker kan tänkas, något som diskuteras i avsnitt 4.8.4, Överbelastning.

Ethernetporten har bedömts som en svår sårbarhet, risknivå 4. Detta baseras på att den är en ingång för ett stort antal attacker. Att den inte når upp till den högsta nivån beror på att den trots allt tillhör den svarta sidan och därför i princip inte ska vara mottaglig för attacker, åtminstone inte mot konfidentialiteten hos känslig information.

4.6.3. Gränssnitt till andra protokoll

Bedömd risknivå: 3

Vid kommunikation inom en koalition kan varianter av besläktade kommunikationssystem såväl som helt olika system användas med protokollgränssnitten som sårbara punkter. Även existensen av äldre kommunikationssystem (arvssystem), i koalitioner liksom i egna led, utgör sårbarheter. Omfattande åtgärder kan krävas för att införliva dessa system i GTRS och GTRS-arkitekturen blir lätt omfattande. Risken är dessutom att de gamla systemens sårbarheter öppnar upp GTRS. Om inte annat är det uppenbart att komplexiteten ökar ytterligare, vilket gör det svårare att analysera och förstå systemet ut ett säkerhetsperspektiv.

Denna sårbarhet bedöms ligga på risknivå 3 då gränssnitt mellan system som använder olika protokoll kan göra GTRS komplext och svåröverskådligt.

4.6.4. Autentisering och auktorisering på röd kommunikationssida

Bedömd risknivå: 1

När en GTRS-nod används som gateway in i ett GTRS-baserat radionät skulle den i vissa fall kunna ha ett helt nät inkopplat på den röda sidan. Detta nät skulle kunna bestå av ett relativt stort antal enheter som ska kunna kommunicera dels med varandra dels med enheter på andra sidan radionätet. Behöver externa enheter autentisera sig mot GTRS för att få rätt att använda de tjänster som finns? Hur hanteras i så fall detta? Hur hanteras auktorisering? Beroende på hur detta görs skulle dessa funktioner, eller bristen på funktioner, kunna utgöra sårbarheter som kan användas av en hotaktör.

Eftersom den som designar GTRS helt och hållet kan styra hur denna autentisering och auktorisering ska se ut, bedöms sannolikheten som låg för att den är behäftad med allvarliga fel. Risknivån har därför bedömts vara 1.

4.6.5. Administrativt gränssnitt

Bedömd risknivå: 2

Det administrativa gränssnittet är potentiellt sårbart i och med att det medger betydande påverkansmöjligheter på GTRS. Det administrativa gränssnittet utgör därmed en känslig punkt som kan utnyttjas av illasinnade aktörer och ge betydande möjligheter att styra hela GTRS vid ett lyckat intrång. Vid ett sådant intrång är det inte en bakdörr in i systemet som används utan ett otillbörligt nyttjande av normala konfigurations- och administrationsmöjligheter. Beroende på exakt vilken typ av tillträde hotaktören skaffat sig så kan olika resultat uppnås.

Genom det administrativa gränssnittet kan relativt mycket i GTRS påverkas. Då gränssnittet inte är helt likt något som tidigare skapats kan det, trots att det noggrant testats, innehålla sårbarheter. Av dessa skäl bedöms risknivån vara 2.

4.6.6. Mjukvaruuppdateringsmekanism

Bedömd risknivå: 3

GTRS är designat för att det ska vara svårt att föra in mjukvara som inte är korrekt och godkänd, se även avsnitt 6.3, Mjukvaruförändringar. Samtidigt finns ett behov hos dem som har rätten och uppgiften att uppdatera systemet av att någorlunda enkelt kunna göra det när behov uppstår. Det är rimligt att tänka sig att en hotaktör som vill föra in illasinnad mjukvara försöker att använda sig av existerande uppdateringsfunktioner i GTRS eftersom detta kan vara enklare än att ge sig på andra delar av systemet som helt och hållet är gjorda för att hindra förändringar. Lyckas hotaktören bara lura uppdateringsfunktionen så får denne kanske hjälp med delar av installationsprocessen.

Möjligheten till mjukvaruuppdateringar innebär i sig en öppning även för en hotaktör varför risknivån bedömts vara 3. Att den inte är högre beror på att uppdateringsprocessen troligen är någorlunda välkontrollerad med exempelvis olika tester samt signering av mjukvaran som ska föras in i systemet.

4.6.7. Exekvering av körbar kod

Bedömd risknivå: 3

GTRS måste i sin helhet, med undantag av uppdateringsfunktionaliteten, vara designat för att hindra alla aktörer från att föra in körbar kod och få den exekverad. Körbar kod kan vara ren maskinkod men också olika former av makron eller liknande om någon sorts interpretering används i noderna. Även konfigurationsdata skulle kunna fungera som rudimentära program i vissa fall, beroende på funktionaliteten hos de system som styrs av dessa data.

Om denna utestängning brister finns möjligheten för en hotaktör att i någon utsträckning styra vad som händer inuti GTRS, med risken att information läcker eller förvrängs eller att funktionalitet tappas.

Att utestänga körbar kod är ett svårt problem att lösa. Trots att produkten troligen kommer att vara välgranskad är det inte säkert att den är fri från sårbarheter, varför risknivån uppskattas till 3.

4.6.8. Fysisk säkerhet

Även ett mjukvarubaserat kommunikationssystem som GTRS körs på en hårdvaruplattform. Ett sätt att angripa systemet är att fysiskt angripa denna hårdvara, i

syfte att förändra systemets beteende genom att till exempel begränsa kommunikationsförmågan. Denna rapport inriktar sig på IT-attacker av olika slag, men det fysiska skyddet är en nödvändig förutsättning för systemets totala säkerhet.

Då angrepp av denna natur ligger utanför ramen för IT-säkerhet har vi valt att inte bedöma denna sårbarhets risknivå.

4.6.9. Utvecklingsprocess

Bedömd risknivå: 5

GTRS är ett system med flera hierarkiska nivåer och många delsystem och komponenter i både hårdvara och mjukvara. Någon eller några av dessa skulle exempelvis kunna vara behäftade med en dold ingång som införts vid design- eller produktionsfasen som ett led i ett angrepp. En sådan ingång skulle kunna fungera som bakdörr för en hotaktör och därigenom göra systemet lättillgängligt. Den stora komplexiteten i systemet som helhet gör det till en svår uppgift att verifiera att sådana möjligheter inte finns.

Om man inte kan lita på design- och produktionsteam, kan man inte heller lita på produkten. Därför värderas risknivån till 5. Visserligen kan tester och kontroller utföras av många olika, någorlunda oberoende, grupper men ett välorganiserat angrepp skulle trots allt vara möjligt med extremt allvarliga konsekvenser.

4.7. Skadliga aktiviteter

I detta avsnitt berörs ett antal skadliga aktiviteter som skulle kunna inträffa. I de flesta fall är det aktiviteter som rimligen endast skulle utföras av en hotaktör, men i vissa fall är det aktiviteter som lika gärna skulle kunna utföras av misstag eller av oförstånd av en legitim användare. En poäng med den modell som använts är att det framgår att aktiviteter kan vara skadliga i sig, oavsett vem det är som utför dem.

Om man bortser från insiders och misstag från legitima aktörer är en initial attack det första steget för en hotaktör. Därnäst följer, enligt riskinventeringsmodellen, en eller flera skadliga aktiviteter vilka kan följa direkt på den initiala attacken eller vara mer frikopplade, varför olika attacker kan leda till samma skadliga aktiviteter. Medan den initiala attacken normalt inte kräver någon särskild tillgång eller särskilda befogenheter kan de flesta skadliga aktiviteter, överbelastning är ett undantag, endast utföras om sådan tillgång eller befogenhet redan innehas. En skadlig aktivitet kan ha som mål att ta hotaktören djupare in i systemet, och kan då ses som en behörighetseskalering. En sådan aktivitet kan lika gärna beskrivas som en attack, även om detta inte kan beskrivas inom riskinventeringsmodellen..

4.7.1. Utnyttjande av övertagen fungerande apparat

Bedömd risknivå: 5

Om en hotaktör lyckas få fysisk tillgång till en fungerande och aktiv apparat så är förutsättningarna väsentligt annorlunda än efter andra typer av lyckade attacker. Möjligheten öppnas för hotaktören att försöka läsa ut kryptonycklar, att undersöka mjukvara och att studera kryptoalgoritmer och övriga funktioner i systemet.

Om någon säkerhetsegenskap är avhängig av att någon information eller mjukvara i apparaten är okänd för motståndaren, behövs rutiner för hur sådant kan ersättas i kvarvarande apparater för att åter nå ett säkert tillstånd i systemet som helhet. Om en övertagen eller försvunnen apparat återfinns behövs antagligen rutiner för hur den ska återföras till ett känt tillstånd, alternativt hur det kan verifieras att den inte påverkats på ett skadligt sätt. Antagligen är det önskvärt att förhindra att motståndaren kan använda övertagna apparater för eget bruk, även i de fall det inte direkt påverkar den egna säkerheten eller funktionen.

Vad är egentligen det största hotet om motståndaren får tag i en fungerande och aktiv nod? Förslagsvis kan det vara tal om:

- Korrekt konfigurerad falsksignalering
- Störning av nätets konnektivitet genom att noden skickar ut felaktig routinginformation
- Avtankning av hemliga kryptonycklar eller hemlig konfigurationsdata
- Avtankning av systemmjukvaran
- Avlyssning av kommunikationen, till exempel positionsinformation

Att denna grupp aktiviteter hamnar på risknivå 5 är ingen överraskning, då de innebär de allra värsta typerna av konsekvenser, samtidigt som de är mycket svåra att skydda sig mot. Motståndare med lägre nivå av kompetens eller mindre tid kanske väljer en av de enklare av de möjliga aktiviteterna under rubriken medan andra kan välja de mer sofistikerade och problemet är därför mångfacetterat.

4.7.2. UT-påverkan via radio

Bedömd risknivå: 1

Beroende på design och implementation skulle det kunna vara möjligt att påverka UT:arna via radiogränssnittet utan att kommunikationen kommer hela vägen fram till CSS:en och resten av apparaten. Eftersom textskyddet sitter i CSS:en så är detta inte ett hot mot konfidentialiteten i kommunikationen. Däremot skulle det kunna påverka möjligheten att kommunicera både för den enskilda noden och, eftersom det är ett multihoppnät, för nätet som helhet. En tillräckligt

sofistikerad hotaktör skulle till och med kunna utnyttja GTRS för att bära egen information eller för att attackera mer avlägsna nätnoder.

Eftersom den initiala attacken mot radiogränssnittet försvåras av frekvenshopp, blir det svårt för en hotaktör att ens kommunicera med GTRS. Den efter initial attack följande skadliga aktiviteten som leder till överbelastning är därmed inte enkel att genomföra. Risknivån bedöms därför vara 1.

4.7.3. Vågformspåverkan

Bedömd risknivå: 2

En möjlighet för en hotaktör vore att påverka själva vågformsimplementationen. Det är CSS:en som är den säkra punkten i en GTRS-nod och när UT:arna laddas med mjukvara måste denna skickas över den interna, svarta, routern. Möjligen kan det här finnas ett sätt för en hotaktör att påverka vågformskoden. En vågform som påverkats av en hotaktör skulle kunna förlora viktiga egenskaper eller tillföras oönskade egenskaper.

Då denna effekt kan uppnås på flera sätt bedöms risknivån vara 3. Att risknivån inte bedöms vara högre beror på att CSS:en inte påverkas.

4.7.4. Påverkan på konfigurationsfiler

Bedömd risknivå: 3

Uppförandet hos GTRS definieras i hög utsträckning av ett antal konfigurationsfiler. Ser man till GTRS i sin helhet blir det viktigt att upprätthålla integriteten hos dessa filer. Kan de påverkas i apparaten eller vid andra tillfällen i hanteringen? Ett antal oönskade uppträdanden hos apparaten eller radionätet skulle kunna framtvingas av en hotaktör om väl valda ändringar infördes i konfigurationsfilerna.

Konfigurationsfiler är troligtvis förhållandevis enkla att förstå sig på och att ändra med tanke på att detta är deras funktion. Risknivån bedöms därför vara 3, men inte högre, eftersom effekten trots allt är begränsad.

4.7.5. Nollställning styrd av användare

Bedömd risknivå: 2

Det kommer att byggas in möjligheter för operatören att nollställa systemet. Exakt vad en sådan nollställning innebär beror på vilken sorts nollställning som görs. Ur ett tillgänglighetsperspektiv kommer det att innebära att den enskilda noden förlorar kontakten med nätet. Det kan också innebära att noden slutar att delta i nätet och därmed inte längre stödjer nätverksbyggandet vilket skulle

kunna innebära att även övriga noder i nätet får sämre konnektivitet. Som hotaktör skulle det vara intressant att kunna provocera fram en nollställning för att därigenom störa kommunikationen i nätet. En sådan provokation skulle kunna föranledas av någon form av IT-attack men också genom en fysisk attack eller någon sorts social engineering. Det är alltså inte nödvändigtvis ett IT-problem utan snarare ett problem i systemet som helhet.

Den potentiella effekten av att tappa kommunikationsförmågan, om än för bara en kortare tid, samt det faktum att funktionen är lättillgänglig för auktoriserade användare gör att denna skadliga aktivitet inte kan bedömas ligga på risknivå 1. Eftersom det dock varken är svårt eller tidsödande att få igång systemet igen och att själva effekten är direkt märkbar samt troligtvis begränsad till en enskild nod, bedöms risknivån vara 2. Om nollställningen är sådan att noden måste sändas till verkstad eller motsvarande för att återstartas, blir risknivån högre.

4.7.6. Byte till dåligt krypto

Bedömd risknivå: 3

Säker kommunikation av sekretessbelagd information är beroende av starka kryptosystem som är korrekt implementerade och korrekt använda. I ett system som är så generellt som GTRS, där man tänker sig att olika krypton ska kunna väljas beroende på vad som ska kommuniceras och med vem kommunikationen ska ske, finns en risk att kommunikationsströmmen kopplas fel och krypteras med fel krypto. Om detta krypto inte är anpassat för uppgiften, eller rent av är ett ”nollkrypto” som lämnar klartexten oförändrad, kan säkerheten som kryptot ska ge helt eller delvis gå förlorad. Den felaktiga kopplingen kan bero på en attack av en hotaktör, handhavandefel hos operatören, fel i konfigurationsfiler eller en oväntad teknisk defekt i mjukvaran eller hårdvaran.

GTRS designas troligen med mycket god kontroll av CSS:en. Den eventuella, mycket allvarliga, effekten av ett byte till ett dåligt krypto gör dock att risknivån värderas till 3.

4.7.7. Påverkan av router/protokoll

Bedömd risknivå: 2

Routern sitter på svart sida, vilket i vissa anslutningskonfigurationer skulle kunna göra den lättåtkomlig för en hotaktör. Samtidigt sänds viss skyddsvärd information över routern, till exempel hoppsekvensdata från CSS:en till UT:arna. Routern kan också vara inblandad i förflyttningen av IP-paket i GTRS eller i ett större IP-nät. Den här typen av skadlig aktivitet skulle kunna tappa av viss känslig information eller störa routingfunktionen antingen lokalt i maskinen eller i IP-nätet. Relevanta frågor är var mjukvaran till routern är lagrad, vem som kan komma åt den och när.

Routrar och protokoll är centrala i GTRS varför det vore relativt allvarligt om de komprometterades även om endast svart data är tillgänglig. Risknivån blir därför 2.

4.7.8. Nyttjande av GTRS för falsksignalering

Bedömd risknivå: 4

En fungerade och aktiv GTRS-nod i händerna på en hotaktör kan användas för att kommunicera på ett giltigt och korrekt sätt med övriga noder i radionätet. Eftersom kommunikationen förväntas vara databaserad, finns små möjligheter för övriga noder i nätet att upptäcka att apparaten övertagits av en hotaktör. Detta ger hotaktören möjlighet att sprida falsk information till övriga noder och, om det är en apparat hos någon i chefsställning, kanske möjlighet att ge falska order.

Även om konsekvenserna under tiden kan vara mycket skadliga, bör problemet med nyttjande av GTRS för falsksignalering vara övergående varför risknivån bedöms vara 4.

4.7.9. Falsk kommunikation till kryptokanalen

Bedömd risknivå: 2

En hotaktör skulle kunna rikta ytligt sett korrekta IP-paket till de olika kryptokanalerna i CSS:en, antingen i syfte att mätta mottagaren eller för att göra den förvirrad när det kommer paket till den som inte hör hemma i paketströmmen. Att IP-paketen inte innehåller korrekt krypterad information är inget hinder för den här typen av skadlig aktivitet eftersom målet inte primärt är att få information att passera kryptosystemet och nå en verklig mottagare på andra sidan. Istället är hotaktören nöjd om den överhuvudtaget lyckas nå kryptokanalen med sina falska IP-paket.

Denna aktivitet kan helt klart bli besvärlig för den försvarande sidan, även om det troligen till viss del går att undvika åtminstone de allvarligare effekterna. Risknivån bedöms vara 2.

4.7.10. Falsk kommunikation till UT:ar

Bedömd risknivå: 2

Samma typ av falsk kommunikation som beskrivs i avsnitt 4.7.9, Falsk kommunikation till kryptokanalen, skulle kunna riktas till UT:arna istället. De förses av CSS:en med data för TRANSEC. Det skulle kunna vara möjligt att störa deras funktion genom att skicka korrekt adresserade IP-paket till dem, även om innehållet i dessa paket inte är korrekt. Beroende på vilken typ av skydd som finns för denna sorts falsksignalering så skulle det kunna vara möjligt att göra

UT:arna förvirrade på olika sätt genom att förse dem med rimliga, men falska, data.

Även om aktiviteten kan leda till vissa skadliga konsekvenser, så finns troligen tillräckligt med skydd och prestanda för att inte innebära några mer allvarliga effekter. Risknivån uppskattas därmed vara 2.

4.7.11. Påverkan av uppstartssekvens

Bedömd risknivå: 2

En hotaktör som har möjlighet att påverka en GTRS-nod som är under uppstart har andra möjligheter än om endast driftsatta noder är tillgängliga. En startande nod skulle kunna påverkas vid ett känsligt tillfälle under uppstartssekvensen när det interna tillståndet medger speciella typer av påverkansmöjligheter. Om detta är möjligt eller inte beror förstås helt på om noderna är säkerhetsmässigt svagare under uppstarten. Säkert är dock att det delvis är andra programavsnitt som körs och att andra egenskaper gäller i systemet vid dessa tillfällen.

Under uppstart är systemet troligen mer påverkbart i vissa avseenden. För att kunna påverka uppstartssekvensen måste en hotaktör troligen ha haft ganska ingående tillgång till systemet tidigare och har därmed kunnat genomföra vissa andra skadliga aktiviteter. Därför är aktiviteten förhållandevis omständlig, vilket resulterar i att den bedömda risknivån är 2.

4.7.12. Felkopplade sladdar

Bedömd risknivå: 2

Varje GTRS-nod har åtminstone fyra röda kommunikationsanslutningar, en svart och ett gränssnitt för administration. Alla dessa använder standardprotokollen Ethernet och IP för att kommunicera. Komplexiteten hos GTRS gör att nät som inte borde ha kontakt med varandra skulle kunna få konnektivitet av misstag. Detta skulle kunna ske genom en oplanerad fysisk sammankoppling, men också genom en oönskad logisk sammankoppling. Utnyttjandet av standardprotokoll och standardgränssnitt i GTRS gör vidare att nät som får kontakt med varandra också har goda möjligheter att kommunicera. Det finns inte, som i många äldre system, skillnader som förhindrar överföring av information mellan nät som inte är tänkta att kommunicera.

I den mån även de mekaniska anslutningarna är kompatibla finns en risk att anslutningarna helt enkelt blandas samman och fel system ansluts på fel ingångar. Om sladdar inte når dit de ska kan en praktisk lösning vara att skarva med en switch. Kanske tycker man att vissa saker fungerar smidigare om vissa sladdar kopplas samman i samma switch. Sådana felaktiga inkopplingar och sammankopplingar kan bryta separationen mellan system eller i värsta fall mellan röd och

svart sida. Kontaktdon som är fysiskt inkompatibla mellan olika system skulle minska denna risk.

Även om problemet är lätt att åtgärda och hantera är det mycket troligt att det någon gång inträffar vilket föranleder den uppskattade risknivån 2.

4.7.13. Utnyttjande av dolda kanaler och sidokanaler

Bedömd risknivå: 2

Varje GTRS-nod har en röd-svart separering vilket innebär att hemlig data på den röda sidan inte ska kunna läcka över till den svarta sidan. Detta säkerställs av en mycket liten, mycket noggrant kontrollerad, delkomponent i mitten av CSS:en. Dock är GTRS-noderna mycket komplexa runt denna säkra kärna. Det skulle kunna hända, medvetet eller av misstag, att hanteringen av den känsliga informationen på den röda sidan läcker information till den svarta sidan. Det skulle kunna röra sig om fördröjningar som är beroende av den hemliga informationen, prioritetsinformation som inte ”tvättas bort” korrekt, variationer i paketstorlek eller läckage via bypassfunktionaliteten.

På grund av sin komplexitet kan även ett så vältestat system som GTRS innehålla sidokanaler. Däremot är aktiviteten svår att genomföra och komplex varför risknivån bedöms vara 2.

4.8. Skador i GTRS

I det här avsnittet tas det som definierats som skador i GTRS, det vill säga direkta konsekvenser i systemet, upp. Med detta menas den omedelbara följd som kommer av en skadlig aktivitet. Det syftas därmed på att effekten inte är beskriven i termer av verksamheten, utan snarare på en teknisk nivå. Effekten beskrivs ur systemets perspektiv, inte ur nyttjarens perspektiv.

I detta och det följande avsnittet görs inga riskbedömningar av de skäl som angavs i kapitlets inledning, nämligen att mängden scenarier är mycket stor och samtliga konsekvenser anses vara allvarliga.

4.8.1. Brist på separation

Hantering av känslig information kräver åtkomstkontroll med olika säkerhetsnivåer definierade. Röd-svartsepareringen är den kanske tydligaste separationskomponenten, men även separation mellan olika röda delar måste upprätthållas för att systemet ska vara säkert. Utöver detta finns behovet av att se till att olika typer av administrativa inställningar och funktioner bara kan nås av behörig personal, vilket också är en sorts separation. I allmänhet kan brist på separation

beröra information, tjänster, systemets funktioner, personalkategorier och så vidare.

4.8.2. Störning genom styrd GTRS-nod

En GTRS-nod skulle kunna användas för att effektivt störa det nät den borde ingå i. Detta eftersom den har tillgång till samma frekvenshoppsekvens som nätet i övrigt, och därför kan emittera radioenergi helt synkront med övriga stationers frekvenshopp, vilket tar bort effekten av frekvenshoppandet på störtåligheten. Detta blir i så fall ett angrepp mot tillgängligheten, det vill säga möjligheten att kommunicera i nätet.

4.8.3. Skadlig omkonfiguration av GTRS

En hotaktör som lyckas få kontroll över de administrativa funktionerna har potential att göra stor skada. I bästa fall kan hotaktören bara göra inkorrekta, men rimliga konfigurationsval, men även i detta fall bör följden åtminstone bli att den omkonfigurerade apparaten förlorar sin konnektivitet med nätet och i värsta fall att hela nätets funktion påverkas. Om hotaktören får tillgång till mer fundamentala konfigurations- och administrationsmöjligheter kan i värsta fall central mjukvara och data bytas ut vilket kan leda till hot mot konfidentialiteten hos skyddsvärd kommunikation och information.

4.8.4. Överbelastning

En möjlig effekt hos GTRS, antingen på systemnivå eller på nodnivå, är att något delsystem eller delkomponent överlastas genom att ta emot mer data än delsystemet/-komponenten kan ta hand om. Detta kan ske medvetet av en hotaktör eller omedvetet av en användare. Till exempel skulle det relativt kapacitetssvaga radionätet kunna fyllas med oväsentlig eller oprioriterad data. Med tanke på systemets komplexitet är det inte otänkbart att det skulle kunna finnas flera delsystem eller delkomponenter som skulle kunna drabbas av denna typ av problem.

4.9. Verksamhetsskador

I det här avsnittet beskrivs några verksamhetsskador. Med verksamhetsskador menas negativa effekter på den funktion GTRS har som uppgift att stödja. Det är förstås svårt att dra en skarp gräns mellan skador i GTRS och verksamhetsskador eftersom konsekvenser ger nya konsekvenser i långa kedjor.

4.9.1. Oförmåga att kommunicera

GTRS uppgift är att erbjuda möjligheten att kommunicera mellan GTRS-bärande plattformar. Om kommunikation omöjliggörs har systemet misslyckats med det som är dess uppgift, vilket får betraktas som en mycket påtaglig skada. Denna skada kan i sin tur leda till olika typer av nya följder, beroende på vilken uppgift plattformen råkar ha. Några exempel på följder är bortfall av positioneringstjänster, oförmåga att begära hjälp, oförmåga att samordna en insats och oförmåga att rapportera spaningsinformation.

4.9.2. Motståndare kan dra nytta av känslig information

Det ligger i själva definitionen av försvarshemlig information att Sverige i något avseende lider skada om sekretessen brister. Det kan röra sig om att positioneringsinformation blir känd eller att orderinformation röjs. Exempel på vidare följder som detta skulle kunna få är att motståndarens insatser kan riktas direkt mot Sveriges enheter eller att en insats avslöjas i förväg.

4.9.3. Införande av falsk information i system

Förändringar i systemen kan skapa förvirring och svårt skada förtroendet för riktigheten i den information som systemen presenterar. Detta kan i sin tur leda till att effektiviteten minskar på grund av att information ibland måste dubbelkollas, eller till och med att systemet helt måste tas ur drift om tilliten blir för låg. I ett sådant fall är man tillbaka i det som diskuteras i avsnitt 4.9.1, Oförmåga att kommunicera.

5. Scenarier

I detta kapitel presenteras tre scenarier där IT-angrepp mot GTRS används för att främja verksamhetsrelevanta syften för hotaktören. Varje scenario inleds med en kort vinjett där metoden för angreppet beskrivs som en berättelse. Vinjetten följs av en diskussion där angreppet beskrivs i termer av riskinventeringsmodellen i kapitel 3. Angreppet diskuteras med fokus på vad som krävs för att attacken ska vara möjlig bland annat vad gäller tid, pengar, kompetens, personal samt planering för hotaktören. Dessutom nämns olika motiv hotaktören kan ha och vilken risk som denne därför kan acceptera. Vidare utreds hur lätt det är att skydda sig, hur vanlig attacken är samt huruvida den är specifik för just GTRS i sin utformning. Slutligen ges en förteckning över relevanta säkerhetsåtgärder som skulle öka säkerheten vid det beskrivna angreppet.

Då GTRS ännu inte är färdigdesignat på detaljnivå följer med naturlighet att scenarierna är vaga och ibland avviker från vad som kommer att vara möjligt i det färdiga systemet. De har dock fortfarande ett värde som en tankeväckande analys och vår förhoppning är att det färdiga GTRS kommer att vara mer motståndskraftigt mot de beskrivna attackerna än systemet nedan.

5.1. Ineffektiv commplan

Detta scenario involverar ett mutat kommunikationsbefäl och resulterar i stora kommunikationsproblem.

5.1.1. Vinjett

Ett kommunikationsbefäl, som har rätt att designa de konfigurationsfiler som kallas commplaner, får pengar mot att i gengäld konfigurera den nuvarande commplanen så att den innehåller alldeles för många GTRS-noder. Systemet fungerar vid uppstartstest på morgonen innan fordonen beger sig på uppdrag. När fordonen är ute och kör provoceras de av motståndare vilket resulterar i ett kraftigt ökat meddelandeflöde i nätet. På grund av sin ineffektiva konfiguration orkar nätet inte med trafiken, vilket får till följd att all trafik blockeras eller fördröjs kraftigt. Detta får i sin tur som resultat att fordonsgruppen inte kan fortsätta med sitt uppdrag då deras samband inte fungerar tillfredställande.

5.1.2. Diskussion

Beskrivet i termer av riskinventeringsmodellen i kapitel 3 har vi följande händelseförlopp: Ett kommunikationsbefäl (legitim aktör) mottar betalning (manipulation) av en hotaktör (outsider) för att påverka commplanerna (skadlig aktivitet). Den ineffektiva konfigurationen i kombination med provokationen

från motståndarna leder till överbelastning av systemet (skada i GTRS) vilket i sin tur resulterar i oförmåga att kommunicera (verksamhetsskada) och i förlängningen ett avbrutet uppdrag.

Eftersom den slutliga provokationen måste resultera i tillräckligt mycket trafik består troligen den angripande sidan av en grupp med även fysisk stridsförmåga. Hotaktören måste dessutom utreda vilka individer som är befäl och vilka av dessa som är lämpliga att muta. Eftersom ett misslyckande där troligen leder till direkt misslyckande med hela operationen och gör att den angripna parten i fortsättningen kommer att vara mer på sin vakt, förstår man att hotaktören måste väga in denna risk. Vidare måste motståndaren ha tillräckliga ekonomiska resurser för att kunna övertyga det korrupta befälet. Ingen större teknisk kompetens, utöver en grundläggande uppfattning om vad som är möjligt, krävs dock, speciellt då hotaktören efter en tid har en person på insidan. Förutom att det kan ta viss tid att hitta rätt person att muta bör angreppet gå förhållandevis snabbt och inte kräva mer än en moderat mängd planering. Om hotaktören dessutom har kontakter som snabbt kan peka ut en lämplig individ att muta går angreppet än fortare och smidigare.

Då angreppet är jämförelsevis lätt att genomföra och endast kräver begränsade resurser, är det troligt att attacken är vanlig hos olika typer av hotaktörer. Eftersom man på sätt och vis slipper att angripa systemet som helhet, särskilt då tekniskt, och istället kan inrikta sig på enskilda individer som lätt kan sättas under stor press bör attackmetoden helt klart tas på allvar, speciellt då liknande metoder kan ha använts av hotaktören mot andra system och organisationer tidigare.

5.1.3. Relevanta säkerhetsåtgärder

En rad olika säkerhetsåtgärder kan vidtas för att minska risken för och/eller effekten av en sådan här attack. Vissa åtgärder är specifika för just det här angreppet, andra mer generella.

- För att undvika att anställda manipuleras och mutas bör anställningsprocessen innehålla någon sorts individgranskning. Målbilder och värdegrund bör tydliggöras. Adekvat utbildning krävs. Löneutrymme och förmåner bör vara adekvata.
- Medarbetare bör övervakas på olika sätt, i möjligaste mån utan att göra intrång på den personliga integriteten.
- Mjukvara och data bör kontrolleras noggrant och av fler individer. Dessa får gärna vara förlagda på olika ställen.
- Olika typer av rimlighetsanalyser för datavärden bör genomföras direkt före användning för att vara säker på att uppstartstestet motsvarar verkligheten.

- Systemet bör hantera överbelastningar på ett rimligt och för användarna förutsägbart sätt med bra och säkra reservsystem att tillgå.

5.2. Bugg i IP-stack

I detta scenario är hotaktören mycket tekniskt kompetent och är attacken lyckad kommer GTRS räckvidd att begränsas.

5.2.1. Vinjett

En bugg i en IP-stack, det vill säga en implementation av ett nätverksprotokoll, i GTRS gör att det är möjligt att skriva över minnet genom en så kallad ”buffer overrun” och därmed injicera egen kod som exekveras på svart sida. En hotaktör har lyckats skaffa tillgång till ett trådat IP-nät som är i förbindelse med de svarta ethernetportarna på flera av GTRS-noderna i ett GTRS-nät. Hotaktören utnyttjar buggen i IP-stacken och injicerar ett program som lyssnar på laddningstrafiken genom den svarta routern under uppstartssekvensen. Programmet lyckas fånga upp och vidarebefordra mjukvaran som implementerar vågformen i UT:arna. Pseduoslumptalsalgoritmen som används för frekvenshoppsekvensen analyseras och hotaktören kan efter några månader bygga en störsändare som är korrelerad till frekvenshoppsekvensen i långt högre grad än vad hade varit möjligt utan algoritmanalysen. Detta leder till att räckvidden för GTRS under den pågående missionen minskar drastiskt, vilket försvårar och fördyrar insatsen.

5.2.2. Diskussion

Beskrivet i termer av riskinventeringsmodellen har vi följande händelseförlopp: En hotaktör (outsider) genomför en nätattack (initial attack) i form av en buffer overrun (IT-sårbarhet i GTRS) via den öppna svarta ethernetporten (IT-sårbarhet i GTRS) och utnyttjar den bristande utestängningen av körbar kod genom att injicera egen kod (IT-sårbarhet i GTRS). Denna kod avlyssnar laddningen av mjukvara till UT:arna under uppstartssekvensen (skadlig aktivitet) och bryter separationen genom att skicka den till hotaktören på utsidan (skada i GTRS). Utifrån detta bygger hotaktören en störsändare som resulterar i försämrad förmåga att kommunicera (verksamhetsskada) och i förlängningen en dyrare insats.

Attacken kräver inte någon stor organisation eller mycket personal men å andra sidan en hög teknisk kompetens, motsvarande akademiska examina inom relevanta tekniska ämnen. Eftersom hotaktören behöver viss kunskap om systemet (inte nödvändigtvis hemlig sådan) kommer denne att behöva lägga ner viss tid på planering, men det föreligger inte några omfattande finansiella behov eller behov av avancerad teknisk planering. På så vis kan hotaktören vara allt från en

främmande makt till en nyfiken eller politiskt driven hacker och med olika motiv följer olika riskbenägenhet.

Att utnyttja buffer overruns är en mycket vanlig angreppsmetod mot mjukvarusystem och ser i mångt och mycket ut på samma sätt oavsett specifikt angreppsmål, varför eventuella hotaktörer mycket väl kan öva på andra system före angreppet. Även att bygga avlyssningsprogram samt störsändare bygger på ganska generella tillvägagångssätt.

5.2.3. Relevanta säkerhetsåtgärder

Relevanta säkerhetsåtgärder omfattar att producera buffer overrun-fri kod och kräver därför ett omfattande säkerhetstänkande vid utveckling genom exempelvis successiva kontroller, kodgranskning säkrare programspråk och utvecklingsmiljöer samt penetrationstester. För att försvåra för och fördröja hotaktören kan fjärradministration döljas, programkod fördunklas och pesudoslumptalsalgoritmer väljas med omsorg. Vidare bör systemet ha starka mekanismer för att hindra körbar kod från att injiceras.

5.3. Informationsläckage från röd till svart sida

I detta scenario leder en lång operation av en välorganiserad hotaktör till allvarligt informationsläckage.

5.3.1. Vinjett

Genom en kombination av hot och mutor av ett flertal personer lyckas hotaktören få till en subtil ändring i säkerhetsmjukvaran i GTRS som gör att det i vissa fall är möjligt att få information på röd sida att återutsändas oskyddad på svart sida. Hotaktören gör en liknande insats mot stridsledningssystemet på bataljonsnivå (SLB) och lyckas förändra koden så att positionsinformation för alla ledningsvagnar kontinuerligt läcks oskyddat och på ett sätt så att det även passerar GTRS. Flera ledningsvagnar råkar ut för överraskande beskjutning på långt avstånd innan det framkommer att positionsinformationen läckts till motståndarsidan ända sedan insatsens början.

5.3.2. Diskussion

Med hot och mutor (manipulation) får hotaktören (outsider) in fel i GTRS mjukvara redan vid leveransen (IT-sårbarhet i GTRS). Mjukvarufelet skapar en brist på separation mellan röd och svart sida (skada i GTRS) vilket gör att känslig

information läcker till motståndarsidan som kan dra nytta av den (verksamhetsskada) genom att på avstånd rikta attacker specifikt mot ledningsvagnar.

Då angreppet börjar redan före leverans måste hotaktören vara beredda att investera mycket tid i sin operation. En hel del pengar och manskap för mutor respektive hot krävs dessutom. Då inte alltför mycket i systemet behöver ändras och man skaffar sig många insiders behöver hotaktören dock troligtvis ingen betydande grad av teknisk kompetens. Den stora utmaningen är snarare att undgå upptäckt vid kontroller och tester. En betydande organisation krävs, liksom vissa stridsmedel för att dra nytta av informationen som inhämtats även om man kan tänka sig att den inhämtande organisationen istället säljer informationen vidare till någon med stridskapacitet.

Attacken kan knappast karaktäriseras som vanlig. Både dess omfattning, mångfacetterade natur samt tidiga start gör att den bör ses som en mycket svårgenomförbar attack av en kvalificerad hotaktör med goda resurser, där minsta misstag kan röja och därmed förstöra hela operationen. En såhär komplicerad attack kommer troligen bara de mest motiverade och riskbenägna hotaktörerna att välja och även då finns troligen ofta lättare angreppsmetoder att tillgå.

5.3.3. Relevanta säkerhetsåtgärder

Även om sannolikheten för en lyckad attack av den här typen är låg bör man se över säkerheten och implementera vissa säkerhetsåtgärder i förebyggande syfte. För att minimera risken för angreppsmetoden bör man kontrollera systemkoden genom att exempelvis simulera olika stridsscenarier och sedan särskilt kontrollera kod som aldrig körs i simuleringarna. Denna kan rymma så kallade bakdörrar till och från systemet. Ytterligare tester kan genomföras med olika automatiska verktyg och genom att anlita utomstående experter för att undvika insiders, även om man då till viss del måste lita på nya individer. För att undvika att hot och mutor fungerar på de anställda bör anställningsprocesser, moral, utbildningar och löner ses över samtidigt som att man förbättrar övervaknings- samt kontraspionageverksamhet främst när det gäller de anställda. Vidare bör man säkra SLB och andra perifera system samt se till att olika anställda endast har de rättigheter de behöver för sina nuvarande arbetsuppgifter. Slutligen bör den röd/svarta separationen verifieras så långt det är möjligt.

6. Problemområden

I det här kapitlet beskrivs några problemområden som inte passar in i riskinventeringsmodellen som beskrivs och används i kapitel 3–5. Även dessa problemområden har sitt ursprung i det tidigare nämnda arbetsseminariet, men de är av en lite mer övergripande eller diskuterande karaktär än de som beskrivits i de tidigare kapitlen.

6.1. Koppling mellan säkerhet och användbarhet

I en verklig situation kommer slutanvändarna av de tjänster som GTRS erbjuder prioritera förmågan att kommunicera framför informationssäkerhet. Om de kommunikationssystem som erbjuds är svåra, långsamma eller besvärliga att använda finns en risk att andra, osäkrare kommunikationssystem används istället trots att man då går emot regelverket. Om det system som då väljs är ett civilt konsumentsystem, till exempel någon sorts mobiltelefoni, förlorar man mycket av den säkerhet som GTRS erbjuder. Det finns alltså säkerhetsmässiga anledningar att beakta användbarhetsaspekter hos GTRS och de system det förser med konnektivitet. GTRS behöver vara så lättanvänt, stabilt och användbart att det inte finns anledning att gå över till alternativa kommunikationstekniker. Ett sätt att underlätta för användarna är att designa användargränssnitt snarlika de som finns på andra system. Då är det dock viktigt att gränssnittet verkligen fungerar på liknande sätt och inte är olika på ett sätt som förbryllar.

Av säkerhetsskäl kan det dessutom finnas anledning för omdesign av GTRS, exempelvis för att förstärka skyddsmekanismerna eller för att det gamla systemet innehöll direkta brister. Säkerhetsfunktionalitet kan således utgöra en viss störande effekt även för en legitim användare. Idealet vore därför att ha anpassningsbar säkerhet där vissa säkerhetsfunktioner automatiskt eller manuellt slås av då dessa inte behövs. I praktiken är dock en sådan lösning svår att implementera då det krävs goda mekanismer för att avgöra om och när sådan avstängning får och ska ske. Om metoden innehåller sårbarheter kan hotaktörer manipulera den såsom en bakdörr för att ge systemet nedsatt säkerhet. Dessutom måste man se till att säkerhetsfunktionaliteten slås på igen när ett skarpare läge inleds.

6.2. Logghantering

För att underlätta bland annat felsökning och spårbarhet är det av vikt att logga vad som sker i GTRS och därmed bevaka informations- och trafikflöden. För att uppnå en god säkerhetsnivå bör alla system och applikationer loggas med särskilt fokus på händelser som kräver högre rättigheter. Exempel på sådana händelser är

att starta och stoppa aktiviteter och program samt loggning av ändringar av tidsservrar för att säkerställa en gemensam tid och därmed ordningen hos händelseförlopp. Det är av särskild vikt att logga informationsflöden över gränsytor inklusive utskrifter och överföring till flyttbara media. Även själva loggförfarandet samt logghanteringen[2] bör, för att hantera insiderhot, i någon mån loggas även om ett sådant resonemang inte kan fortsätta ad infinitum. Viktiga aspekter att ta med för varje händelse som loggas är:

- Vem eller vad utförde handlingen?
- Vad bestod handlingen av?
- Hur utfördes den?
- Var, i vilken nod och applikation, utfördes den?
- När inträffade händelsen?

Loggverktyget som används ska hämta in loggarna från de olika loggkällorna. Detta kan ske antingen genom att installera en så kallad loggningsagent på varje loggkälla eller låta de senare själva sända loggarna till en central lagringsplats. Vidare bör man avgöra om en säkerhetskopia av loggarna ska ligga kvar på varje loggkälla efter export. Verktyget bör dessutom kunna normalisera för att uppnå ett enhetligt format samt ha funktionalitet för logganalys och lagring. Beroende på hur avancerad logghantering som krävs kan man även behöva inkludera funktionalitet för att slå samman logghändelser till händelsekedjor, för att underlätta analysen, samt olika former av reaktiv förmåga. Exempel på reaktiv förmåga är larm, rapporter samt automatisk nedstängning av applikationer eller utloggning av användare. De senare förmågorna innebär dock att loggsystemet får mer kontroll över systemet vilket i sig kan utgöra en säkerhetsrisk. Beroende på mängden logghändelser som genereras kan viss filtrering för att minska resursförbrukning användas om säkerhetsföreskrifterna tillåter detta.

För att säkerställa att loggarna endast kan läsas av auktoriserade och autentiserade användare bör loggarna krypteras. Eftersom en del loggar kan komma att innehålla information som bör hållas hemlig även för loggansvariga samt logganalytiker, kan det vara en god idé att kräva olika rättigheter för att komma åt olika delar av loggarna. Sekretessen kan på så viss bevaras genom hela loggprocessen: generering, inhämtning, analys samt lagring.

Om en hotaktör lyckas ta sig in i logglagringssystemet kan denne försöka ta bort loggar som exempelvis beskriver intrånget. För att hindra borttagning kan hårdvara som inte tillåter detta, utan att förstöras, användas.

[2] Med loggförfarande avses processen att skriva loggar, medan logghantering är den därpå följande processen med att agera och besluta i verksamheten utgående ifrån vad som har loggförts av händelser.

Det finns en rad övriga aspekter som avgör hur man bör handskas med loggarna. Exempelvis kan regelverk kräva lagring en viss tid och internationell samverkan kan innebära att flera regelverk måste samexistera. Loggarna kan dessutom behöva användas till att utkräva ansvar samtidigt som delar av innehållet måste förbli hemligt. Loggarna i sig kan indirekt innehålla information om systemets uppbyggnad, till exempel kan en auktoriserad användare utröna vilka loggkällor som finns och när olika loggkällor genererar logghändelser. Förutom att specificera vem som får tillgång till olika loggrader bör även tillvägagångssätt samt tidpunkt för sådan tillgång bestämmas. Ytterligare måste man avgöra om systemet får fortsätta att köras även om loggfunktionen inte fungerar och hur loggsystemet ska hantera en nollställning av kryptosystemet i GTRS.

6.3. Mjukvaruförändringar

I princip all mjukvara innehåller vid en första lansering olika typer av fel, såsom säkerhetsproblem, prestandanedsättande misstag och sådant som påverkar systemets användbarhet. I takt med att säkerhetshål och andra så kallade buggar påträffas bör också det skarpa systemet uppdateras. I ett så stort och komplext mjukvarusystem som GTRS så kommer det att krävas en noggrann logistik för att distribuera och installera korrekt version av alla mjukvaror i alla apparater. Inkonsistens inom ett nät vad gäller mjukvaruversioner skulle kunna leda till oförutsägbara resultat. En del uppdateringar, främst kritiska säkerhetshål, måste implementeras mycket skyndsamt vilket ställer tuffa krav på uppdateringsprocessen. Andra uppdateringar är av mindre vikt och kan därför vänta. Dessa kan vara lämpliga att samla ihop för att sedan installera genom ett större paket. Eftersom GTRS är ett system som troligtvis ofta kommer att användas kontinuerligt i skarpa situationer bör man utreda hur olika typer av uppgraderingar får göras, hur dessa ska distribueras och vem som får uppdatera. Exempelvis kan man tänkas undersöka om vissa uppdateringar kan genomföras utan att behöva stänga ner systemet eller den enskilda noden.

Sårbarheter i rutiner för uppdatering av GTRS-mjukvaran måste klarläggas så att all ny kod testas lika noggrant som den ursprungliga, för att undvika att systemet får nya fel. Dessutom måste det verifieras att uppgraderingarna är korrekta och att de implementeras på ett korrekt sätt. Ytterligare frågeställningar av vikt är: Är det bra att tillåta successiva uppgraderingar eller är det bättre att helt nollställa hela apparaten först och sedan läsa in den mjukvaruversion som ska användas? Hur hanterar man om en viss version visar sig oanvändbar av någon anledning? Går det att stega tillbaka bland versionerna? Vem kan göra det?

En apparat kan ha hamnat under bristande kontroll under en period på flera sätt, till exempel om den återfunnits efter att ha varit borta, inte bevakats på ett korrekt sätt eller om plomberingen skadats. I alla dessa fall kan det misstänkas att modifieringar gjorts i hård- eller mjukvara. Frågan är hur man kan verifiera att

mjuk- och hårdvara är oförändrad eller åtminstone hur man kan verifiera hårdvaran och därefter ladda den med korrekt mjukvara på ett kontrollerat sätt. Går det överhuvudtaget? I så fall, kan det göras i fält, i svensk kryptoverkstad eller endast hos tillverkaren?

6.4. Utmaningar och långsiktighet

GTRS skiljer sig från äldre radiokommunikationslösningar på flera sätt. Skillnaderna som här diskuteras är i huvudsak tekniska, men får effekter och konsekvenser även inom andra områden.

6.4.1. Standardlösningar

GTRS bygger i stor utsträckning på standardlösningar. Det finns fördelar med att använda standardlösningar, såväl i valet av mjukvara som i valet av protokoll. Det möjliggör att komma åt väl kända och stabila lösningar på olika problem och att kunna konsultera många olika aktörers kunnande och erfarenheter. Det är också ett kostnadseffektivt och snabbt sätt att bygga ett komplext system. Samtidigt finns även risken att dessa standardlösningar leder till problem. Militära uppgifter är inte alltid representativa för de verksamheter som standardlösningarna är tänkta att lösa, vilket kan ge problem med avseende på robusthet, kommunikationseffektivitet och säkerhet.

6.4.2. Generationsklyfta

Det finns ett grundläggande problem i GTRS relation till omvärlden. Problemet hänger ihop med att det tänkta systemet är minst en generation modernare än regler, föreskrifter och mentala bilder av vad ett kommunikationssystem är. En jämförelse som kan göras är med skillnaden mellan en väggtelefon med pulsval och en 3G-mobiltelefon. Ett reglemente som förutsätter att telefoni görs med en väggmonterad telefon kommer att fungera dåligt om de verkliga telefonerna är 3G-mobiler.

GTRS är svårt att kravställa, utveckla, upphandla, analysera, certifiera och så vidare, eftersom systemet inte ser ut som något har sett förut. Det finns också en risk att man, så att säga, bygger en väggtelefon inuti mobiltelefonen. Detta kan ske nära på bokstavligt i fallet med implementering av äldre system i GTRS. Det kan också ske indirekt om man bygger kommunikationslösningar som är konceptuellt lika de som använts tidigare, även om det nu finns andra sätt att lösa samma problem.

6.4.3. Förändring över tid

GTRS och den kontext det befinner sig i kommer med stor sannolikhet att förändras under systemets livstid. Detta är förstås sant även om äldre system, men vi tror att det faktum att GTRS i så hög utsträckning är en IT-produkt gör att denna förändring kommer att vara mycket mer påtaglig, och av betydelse även i relativt korta tidsskalor. Här nämns några ytterligare faktorer som bedöms bidra till detta:

- Ackrediteringsprocessen är huvudsakligen anpassad till att hantera statiska system som inte enkelt kan uppdateras. GTRS, med sin stora mängd mjukvara, kan behöva uppdateras med ny mjukvara många gånger under sin livstid. Det kan röra sig om säkerhetsuppdateringar, nya vågformer eller nya kryptolösningar, eller kanske bara nya kombinationer av existerande delar. Hur påverkar detta ackrediteringsprocessen?
- Hela vägen från de tidiga faserna av ett systems livscykel, som till exempel kravställnings- och designfaserna, fram till avveckling, är det viktigt med ett adekvat säkerhetsarbete. Allt för ofta blir satsningar på säkerhet koncentrerade till en eller få faser. Typiskt är att säkerhetssatsningar görs sent i utvecklingsfasen när det mesta övriga är klart och svårligen låter sig påverkas och ändras. När systemet väl är driftsatt finns vidare risken att säkerhetsarbetet anses avslutat, något som det i själva verket knappast är för ett IT-system som GTRS. Det är sällan lätt att börja säkerhetsarbetet från projektets start eftersom man först behöver viss tid att utveckla sin idé. Däremot bör säkerhet redan på ett förhållandevis tidigt stadium belysas även om det då av nödvändighet sker på en ganska abstrakt nivå. När man sedan funderar på implementering bör man inte leva med förhoppningen att det går att baka in all säkerhet i en säkerhetsmodul. Istället måste man acceptera att varje detalj i systemet kan innebära en sårbarhet. Även om det ofta verkar enklare att i en sen säkerhetsanalys leta sårbarheter, är det nödvändigt att redan från början stå på en stabil grund.
- Hotbilden utvecklas över tiden. Även om ett system inte ändras och sårbarheterna kvarstår kommer högst sannolikt hotbilden att ändras genom att sårbarheter upptäcks som därmed kan utnyttjas av hotaktörer. Uppdatering av system kan introducera nya sårbarheter med associerade hot, något som diskuteras i avsnitt 6.3, Mjukvaruförändringar.
- I framtiden kanske man vill introducera nya GTRS-noder, t.ex. mindre och mer portabla sådana vilket ställer nya krav på säkerheten. Det kan vara viktigt att redan från början till viss del planera för sådana förändringar för att senare inte behöva bygga om hela GTRS.
- GTRS innehåller och kommunicerar med många andra system och sårbarheter i dessa kan i vissa fall påverka säkerheten i GTRS. Exempelvis kan

autentiseringsmetoder brista eller hårdvara gå sönder. Vidare kan systemtiden påverkas genom att GPS störs vilket kan leda till problem med bland annat synkronisering och loggning.

6.5. Stödfunktioner och utbildning

Kunskap om GTRS inom den egna organisationen och hos koalitionspartners är central för att uppnå adekvat IT-säkerhet. Vet användarna inte exakt hur GTRS ska användas finns möjligheten att de orsakar eller utlöser säkerhetsincidenter. Bra stödfunktioner som är samordnade med utbildningsinsatser är av stor vikt för funktionaliteten och särskilt säkerhetsfunktionaliteten hos GTRS, speciellt på grund av systemets komplexitet. Även för att minimera genomslag av hot baserade på manipulering, är utbildning av mycket hög vikt. Exempelvis måste varje individ som är inblandad i systemet veta hur den ska hantera förfrågningar och uppmaningar även från sådana som normalt inte behöver dennes assistans. Som tidigare nämnts i rapporten är den mänskliga faktorn viktig att studera ur ett säkerhetsperspektiv och eftersom det är naturligt för individer att vara hjälpsamma måste man ge dem kunskap om att det i vissa fall kan vara lämpligt att, istället för att ge direkt stöd, hänvisa till exempelvis dennes chef som är mer kunnig om diverse procedurer och reglementen. Exempelvis behöver inte en person vara behörig bara för att denne har viss sekretessbelagd kunskap om systemet eftersom denna kunskap kan ha fåtts på olaglig väg. Vidare är utbildning om hot, mutor och liknande icke-tekniska angrepp nödvändig.

I ett system som GTRS används många olika autentiseringsmetoder och användare kan behöva skapa och komma ihåg många lösenord. Genom utbildning kan man se till att lösenorden väljs så att de är förhållandevis lätta att komma ihåg utan att de minskar betydligt i styrka. Detta kan vidare förebygga att användare skriver ner lösenord för att använda som minnesanteckningar och göra det möjligt för användare att minnas rätt även i stridens hetta. Om även metoder som bygger på användarens kroppsliga egenskaper, biometri, används behövs eventuellt en annan typ av utbildning för att lära användarna att hantera situationer där egenskaperna ändrats eller där en hotaktör utnyttjar mer riktade hot mot individen som person.

6.6. Rättighetshantering och fjärradministration

Det är lätt att beakta frågan om autentisering, det vill säga att klargöra vem man har med att göra, och glömma av eller inte tillräckligt beakta frågan om vad denne får göra inom GTRS, det vill säga auktorisationsfrågor. Speciellt viktigt blir det att ha tydliga rutiner i samband med koalitioner, där olika aktörer från en uppsättning organisationer och länder är i behov av att ha tydliga besked om

typen av auktorisation och att berörda system, som här GTRS, tekniskt implementerar detta. Likaså skall dessa rutiner klargöra vad respektive aktör inte tillåts göra. För komplexa system som GTRS behöver olika användarklasser och roller därför tydligt definieras.

Ett speciellt problem i samband med auktorisation är hur systemet ska hantera fallet att en rättighet tas bort, det vill säga återkallande eller revokering av rättigheter. Revokering är nödvändigt i de fall en person eller apparat inte längre anses betrodd, till exempel för att de försvunnit eller blivit tillfångatagna. Hur ska sådan revokeringsinformation spridas på ett säkert sätt? Om revokering inte hanteras bra, riskeras att en hotaktör kan revokera giltiga användare, eller att en enhet som inte borde vara betrodd längre ändå tolkas som trovärdig av någon som inte fått information om revokeringen.

För att snabbt sprida uppdaterad information till GTRS i drift måste systemet medge administration på distans, över radiogränssnittet. Fjärradministration är en mycket önskvärd förmåga ur ett funktionellt perspektiv, men kan utgöra ett problem ur ett säkerhetsperspektiv. I vilken mån ska och bör GTRS kunna fjärradministreras? Vilka möjligheter och risker medför detta? Vilka ställningstaganden är rimliga för att uppnå bästa möjliga funktion respektive säkerhet hos systemet? Hur kan man jämföra risken med att möjliggöra fjärradministration med att apparaterna måste konfigureras individuellt?

7. Diskussion

Det huvudsakliga bidraget i denna rapport är riskinventeringen i kapitel 4 med sin tillhörande bedömning av risknivån för varje riskfaktor. Denna inventering har vidareutvecklats genom att struktureras med utgångspunkt i den riskinventeringsmodell som beskrivs i kapitel 3 och genom att kompletteras med scenarierna i kapitel 5 och problemdiskussionerna i kapitel 6. Ser man till dessa delar tillsammans framträder en bild av GTRS som en mycket IT-intensiv produkt. Det finns IT-säkerhetsrelevanta frågor och problem att beakta inom snart sagt varje delkomponent och aspekt av systemet.

En vidare observation av samma typ är att kryptodelen i GTRS är lika generell som radiodelen. Det rör sig alltså lika mycket om ett ”software defined crypto” som en ”software defined radio”, mjukvarudefinierad radio. Visserligen ingår kryptofunktionalitet i begreppet mjukvarudefinierad radio enligt SCA-standarden, men vår känsla är ändå att det inte alltid framgår helt tydligt att kryptofunktionaliteten har samma frihetsgrad som radiofunktionaliteten.

Det vi vill komma till med denna utläggning är inte att systemet är inneboende dåligt på något sätt. Vår poäng är att GTRS består av ett mjukvarudefinierat krypto och en mjukvarudefinierad radio, och att dessa binds samman i en apparat som är lika mycket en dator (eller egentligen ett nät av datorer) som det är något annat. FOI:s uppdrag har varit att studera GTRS ur en IT-säkerhetssynvinkel, varför vi lämnar våra icke IT-relaterade observationer utan åtgärd.

Riskinventeringen i denna rapport är omfångsrik och det finns ett behov av att sortera ut en mindre mängd områden att studera mer ingående. En naturlig fortsättning är därför att genomföra en mer systematisk prioritering av områdena för att därmed få underlag för att välja ut de mest intressanta och gå vidare med dessa.

De risknivåer som redan finns ansatta är en början på ett sådant arbete, men det behövs en djupare analys och gärna återkoppling från personer som har en djupare insikt i hur GTRS ska användas än den som vi som IT-säkerhetsexperter besitter. En sådan prioritering är också en god början på arbetet att ta fram den IT-säkerhetsarkitektur som kommer att vara huvudinnehållet i FOI:s nästa rapport i projektet.

Referenser

1. Combitech, *Actors*, arbetsmaterial med tabell över legitima användare av GTRS .
2. Försvarsmaktens gemensamma riskhanteringsmodell – Metodanvisning, Försvarsmakten M7739-350012, 2009.
3. Hunstad, A. och Löfvenberg, J., *Avrapportering arbetsseminarium IT-säkerhet i GTRS, oktober 2009*, FOI Memo 3075, 2009.
4. Mitnick, K.D., Simon, W.L., *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, Inc., 2003 .
5. Palm, T., Försvarsmaktens gemensamma riskhanteringsmodell – En beskrivning av modellen samt jämförelse med riskhanteringsmodeller hos civila myndigheter, FOI-R--259--SE, 2008.
6. SIS. (2007). SIS HB 550: Terminologi för informationssäkerhet, utgåva 3. SIS Förlag.