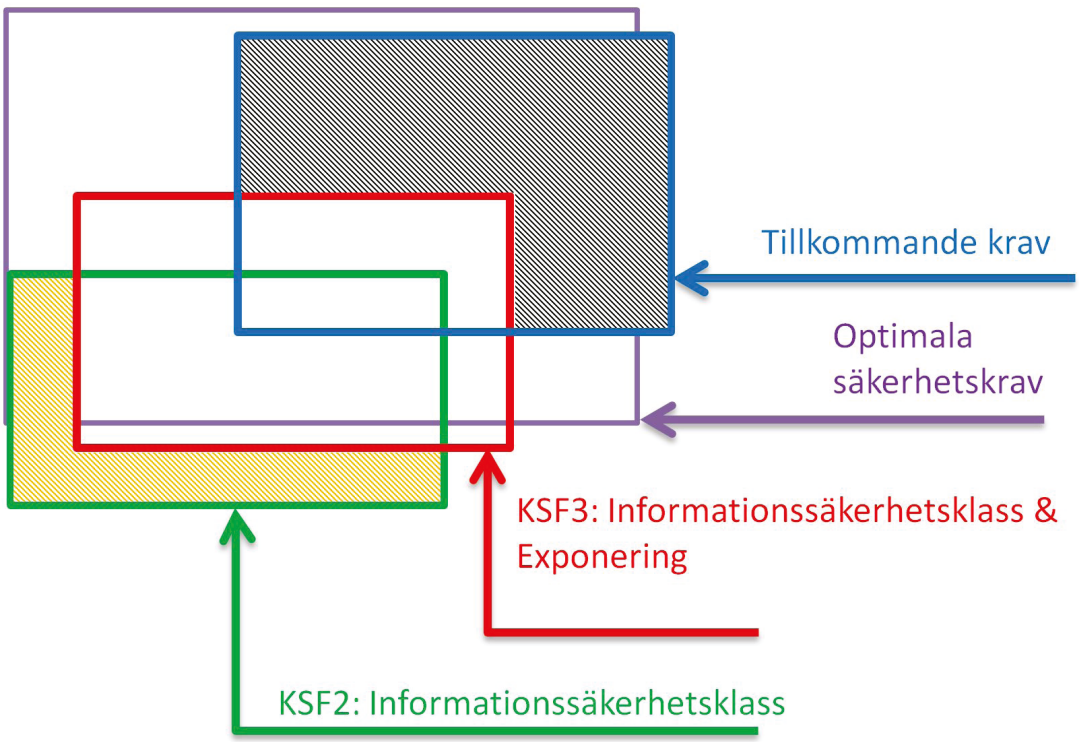
IT-säkerhetskrav i Försvarsmakten

KSF3 och tillkommande säkerhetskrav

JOHAN BENGTSSON, TEODOR SOMMESTAD, HANNES HOLM



FOI-R--4000--SE
ISSN 1650-1942 December 2014

Johan Bengtsson, Teodor Sommestad,
Hannes Holm

IT-säkerhetskrav i Försvarsmakten

KSF3 och tillkommande säkerhetskrav

Bild/Cover: Teodor Sommestad

Titel	IT-säkerhetskrav i Försvarsmakten - KSF3 och tillkommande säkerhetskrav
Title	IT security requirements in the Swedish Armed Forces - KSF3 and additional security requirements
Rapportnr/Report no	FOI-R--4000--SE
Månad/Month	December
Utgivningsår/Year	2014
Antal sidor/Pages	60
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36058
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Denna rapport beskriver två studier kopplade till version 3 av Försvarsmaktens *Krav på Säkerhetsfunktioner* (KSF3) – en riskhanteringsmodell och samling av IT-säkerhetskrav som har skapats av Militära underrättelse- och säkerhetstjänsten (MUST). Utöver dessa två studier har projektet även analyserat hur framgångsrik kravhantering mäts i vetenskaplig forskning.

Den första studien analyserade 13 säkerhetsmålsättningar, dokument som skall visa hur IT-system i upphandlingsfasen uppfyller MUST:s IT-säkerhetskrav. Syfte med studien var att identifiera IT-säkerhetskrav som ofta tillkommer till de krav som KSF3 föreskriver. Totalt 672 unika krav kartlades. Av dessa fanns 288 representerade i KSF3, 308 var tillkommande och 76 var för oklara för att kunna klassificeras. De tillkommande kraven var oftast av icke-fysisk karaktär (60% av kraven), hade en antagonist i åtanke (67% av kraven) och rörde tillgänglighet specifikt (15%). Nio kategorier av tillkommande krav identifierades. De vanligaste kategorierna var krav på konfigurationsmöjligheter (34%) och inbrottsskydd (17%). KSF har nyligen uppdaterats från version 2 (KSF2) till version 3 (KSF3), vilket har inneburit signifikanta förändringar rörande dess innehåll sedan de analyserade säkerhetsmålsättningarna skrevs. Vissa av KSF3-kraven var bättre representerade i de analyserade säkerhetsmålsättningarna. Exempelvis var skydd mot skadlig kod bättre representerat av säkerhetsmålsättningarna än behörighetskontroll.

Den andra studien analyserade hur de funktionella säkerhetskraven i KSF3 enklast kan realiseras med hjälp av typiska säkerhetskomponenter i ett fiktivt system med enkel funktionalitet. Forskarna bedömde att KSF3 på grundläggande nivå enklast realiserades med en Windows-baserad lösning innefattande en terminalserver, antivirus, brandvägg och ett verktyg för samlad logghantering. För KSF3:s krav på utökad nivå bedömdes det tillkomma (i huvudsak) TEID-kort, anomalidetektion, en patchhanteringsserver och stöd för märkning av objekt. TAK-kort, applikationssandlådor och mer avancerade inspektionssystem var de huvudsakliga tillkommande funktionerna för KSF3 på hög nivå. Dessutom tillkommer skydd mot röjande signaler och kabelinspektioner (dessa kan dock även vara relevanta för att uppfylla utökade krav).

Nyckelord: KSF, Säkerhetsanalys, IT-säkerhetskrav, cybersäkerhet

Summary

This report describes two studies related to version 3 of *Krav på säkerhetsfunktioner* (KSF3) – a risk management model and a collection of IT security requirements on security functions developed by the Military Intelligence and Security Directorate (MUST) for the Swedish Armed Forces. In addition to these two studies, the report includes an analysis of how successful requirements engineering is measured in scholarly research.

The first of the two studies analysed 13 documents used in the accreditation process to specify how IT systems fulfil the IT-security requirements of MUST. The purpose was to identify IT security requirements that are frequently added on top of the IT security requirements posed by MUST in the KSF3. Of the 672 unique requirements that were investigated in the study 288 were represented in KSF3, 308 were additional requirements and 76 were too ambiguous to be categorized. The majority of the additional requirements concerned non-physical measures (60%), many of the additional requirements were often motivated by antagonists (67%) and many of the additional requirements specifically addressed system availability (15%). Nine categories of additional requirements were identified. The categories associated with most requirements were configuration functionality (34%) and physical perimeter protection (17%). Furthermore, the current version of MUST's requirements on security functions (KSF3) differs significantly from the previous version (KFS2) which was used when the 13 security requirements specifications were written. Some parts of KSF3 requirements are better represented in the documents than others. For instance, protection against malicious code is better represented in the documents than access control functions.

The second study analysed how the functional security requirements in KSF3 could most easily be realized in a fictive system using typical security components. The researchers found that the basic level of KSF3 could most easily be realized with a Windows-based solution including a terminal server, antivirus software, firewall and a tool for central log management. For the additional security components on the next level of KSF3, the (main) additions were assessed to be smartcard-based authentication, anomaly detection, a patch management server, and support for tagging objects. More advanced smartcards, application sandboxing and more advanced inspection systems for data exchange were the main additional functions for KSF3 on the highest level. Furthermore, in most cases TEMPEST protection and cable inspection are required (these may however also be relevant to fulfil additional requirements).

Keywords: KSF, security analysis, IT-security requirements, cyber security

Förord

När nya IT-system ska tas fram inom Försvarsmakten ska framtagandet göras i enlighet med IT-processen. En viktig del i detta arbete är ta fram den säkerhetsmålsättning som används som underlag när *Militära underrättelse- och säkerhetstjänsten* (MUST) uttalar sig om huruvida det planerade IT-systemet bedöms få en tillräcklig nivå avseende informationssäkerhet eller ej. Bland de stöd som finns att tillgå vid skapandet av en välbalanserad och begriplig säkerhetsmålsättning är förmodligen *Krav på säkerhetsfunktioner* (KSF) det allra mest centrala. I KSF specificeras de miniminivåer av IT-säkerhetskrav som Försvarsmaktens system förväntas uppfylla givet olika förutsättningar.

Under 2014 har en ny version av KSF börjat användas – version tre – och under det första året av projektet *Bedömning och analys av IT-system* (BAIT) har innehållet i KSF3 varit i fokus. Denna rapport beskriver huvudsakligen hur kraven i KSF3 förhåller sig till tidigare godkända säkerhetsmålsättningar och hur kraven i KSF3 kan realiseras i praktiken. Den tilltänkta läsaren är en person som har viss insikt i den auktorisations- och ackrediteringsprocess som KSF skall stödja samt har grundläggande kunskaper inom IT-säkerhet. Med anledning av detta är vissa delar av rapporten tekniska och vissa delar är rika på termer som har en vedertagen innebörd inom Försvarsmakten.

Utöver projektgruppen har tre personer gjort betydelsefulla bidrag till innehållet i denna rapport. Jonas Hermelin har bidragit med extrahering av krav från säkerhetsmålsättningar, Ulrik Franke har bidragit med kunskap om teori inom tillgänglighet i IT-system och Christian Fenger-Krog har bidragit med tolkningar av krav och hjälpt till att inrikta projektet. Projektgruppen vill tacka alla dessa tre, de övriga i projektets referensgrupp på Försvarsmakten och de som hjälpt till att ta fram de säkerhetsmålsättningar som använts som underlag för studien.

Innehållsförteckning

1 Inledning

Projektet *Bedömning och analys av IT-system* (BAIT) syftar till att förbättra Försvarsmaktens metoder for säkerhetsanalys och kravställning inför auktorisation och ackreditering av IT-system. Projektet genomförs av Totalförsvarets forskningsinstitut (FOI) inom ramen för Försvarsmaktens *Forskning och Teknikutveckling* (FoT). BAIT kan ses som en fortsättning på projektet *Effektivare hot-, risk- och sårbarhetsanalyser* som pågick 2011-2013 och hade som mål att undersöka och förbättra Försvarsmaktens hot-, risk- och sårbarhetsanalyser för IT-system. Resultatet av det tidigare projektet pekade på flera områden med förbättringspotential inom processen som leder fram till auktorisation och ackreditering av IT-system. I BAIT fokuseras det på vissa av dessa områden och det görs en till två fördjupande studier per år. Projektet pågår till och med 2016.

Vilka studier som genomförs bestäms årsvis i samråd med en referensgrupp med representanter från CIO-gruppen och MUST SÄKK på Försvarsmakten. Under projektets första år (2014) önskade dessa att BAIT skulle fokusera på att identifiera IT-säkerhetskrav som är frekvent återkommande i Försvarsmakten och därför skulle kunna användas som en utgångspunkt för IT-säkerhetskraven. I Försvarsmakten finns det som kallas *Krav på Säkerhetsfunktioner* (KSF) som syftar till att ge en utgångspunkt för IT-säkerhetskrav – givet en grov beskrivning av systemet föreskriver KSF vilka IT-säkerhetskrav som ställs på det. Inom Försvarsmakten används oftast de fyra kvaliteterna sekretess, tillgänglighet, riktighet och spårbarhet för att fånga begreppet IT-säkerhet. Av dessa använder KSF enbart sekretess som parameter för att bestämma vilka IT-säkerhetskrav som är nödvändiga. Det finns därför anledning att tro att IT-säkerhetskrav för att uppnå tillgänglighet, riktighet och spårbarhet inte helt tillgodoses av KSF. Att komplettera KSF med andra IT-säkerhetskrav än sekretesskrav till en sorts KSF-plus skulle därför vara önskvärt. Utöver detta identifierades lösningar på funktionella KSF-krav och vilka av dessa krav som kan mötas med vanliga komponenter och enkla manuella procedurer.

Studien om tillkommande krav redovisas i Kapitel 3 och lösningar på KSF3-krav redovisas i Kapitel 4. Innan dessa kapitel ger Kapitel 2 en översiktlig beskrivning av KSF tillsammans med teorier om hur tillgänglighetskrav, riktighetskrav och spårbarhetskrav kan klassificeras och härledas. I Kapitel 5 ges slutsatser från studierna samt rekommendationer till Försvarsmakten.

Utöver dessa två studier har även en mer allmän litteraturgenomgång gjorts av experiment inom kravhantering för IT-system. Denna litteraturgenomgång identifierade hur forskning inom kravhantering har mätt hur bra och effektiv kravhantering är. Detta arbete resulterade i ett artikelmanuskript som skickades in till tidsskriften Empirical Software Engineering och nu väntar på att bli vetenskapligt granskat.

2 Grundkrav på säkerhetsfunktioner

I Försvarsmakten är skriften *Krav på säkerhetsfunktioner* (KSF) [1] det huvudsakliga verktyget för att identifiera IT-säkerhetskrav. KSF tas fram av MUST och ska säkerställa att de IT-system och IT-tjänster som används inom Försvarsmakten uppfyller de sekretesskrav som finns på informationen de behandlar. I praktiken är det en enkel metod för att identifiera en grunduppsättning krav som system ska uppfylla på ett eller annat sätt för att kunna ackrediteras. Den första versionen kom i början av 2004; den andra versionen kom i slutet av 2004; version 3 togs i bruk 2012; en uppdatering till version 3.1[1] gjordes 2014. KSF3 skiljer sig betydligt från KSF2:

- I KSF2 användes den informationssäkerhetsklass som informationen i IT-systemet hade som enda parameter för att härleda vilka krav systemet behövde uppfylla. I KSF3 tas även hänsyn till systemets exponering, det vill säga information om vilka användare som har tillgång till systemet och det informationsutbyte som sker med andra system.
- Själva kraven är mer granulärt kategoriserade och mer atomära. Enligt KSF3 leder uppdateringen också till ”bättre anpassning mot dimensionerande hot” [1].

Den intresserade finner såväl förklarande beskrivningar av KSF3 som konkreta krav i [1]. Avsnitt 2.1 till 2.3 ger en översiktlig beskrivning av hur kraven bestäms i KSF3 samt vilka krav KSF3 innehåller. I Avsnitt 2.4 presenteras teorier som eventuellt kan komplettera KSF för att identifiera IT-säkerhetskrav som säkerställer rätt tillgänglighet och riktighet.

2.1 Kravdrivande variabler

KSF3 innehåller 148 funktionella säkerhetskrav och 275 assuranskrav. Vilka av dessa som behöver uppfyllas för ett IT-system bestäms utifrån *konsekvensen* om obehöriga får tillgång till informationen i systemet och systemets *exponering* mot användare och andra IT-system. Konsekvensen bestäms av informationssäkerhetsklassen. Den lägsta konsekvensen (K1) motsvarar att obehöriga får tillgång till öppen information och den högsta konsekvensen (K5) motsvarar att obehöriga får tillgång till information klassificerad som H/TS. Exponeringen bedöms i en skala på fyra steg enligt Tabell 1.

[1] Denna rapport utgår från KSF 3.0 då 3.1 inte fanns tillgänglig när studien påbörjades. Dock är skillnaderna mestadels kosmetiska och slutsatserna skulle därför blivit desamma.

Tabell 1: Exponeringsnivåer med de tillhörande kriterierna *tillgång till systemets fysiska och logiska gränsytor* samt *informationsutbyte*.

Exponeringsnivå	**Tillgång till systemets fysiska och logiska gränsytor**		**Informationsutbyte**
E4	Alla fall som inte uppfyller kriterierna för någon av exponeringsnivå E1-E3 nedan.		Alla fall som inte uppfyller kriterierna för någon av exponeringsnivå E1-E3 nedan.
E3	Alla personer med tillgång till någon av systemets gränsytor är säkerhetsprövade.	**och**	Samtliga system som systemet utbyter information med är ackrediterade till en högre konsekvensnivå **eller** Samtliga system som systemet utbyter information med är ackrediterade till samma konsekvensnivå med högst exponeringsnivå E3.
E2	Alla personer med tillgång till någon av systemets gränsytor är behöriga till någon information inom den högsta konsekvensnivån som behandlas i systemet.	**och**	Samtliga system som systemet utbyter information med är ackrediterade till en högre konsekvensnivå **eller** Samtliga system som systemet utbyter information med är ackrediterade till samma konsekvensnivå med högst exponeringsnivå E2.
E1	Alla personer med tillgång till systemets gränsytor är behöriga till all information som behandlas i systemet.	**och**	Systemet utbyter ingen information med andra system

När konsekvensnivån och exponeringen har bestämts kan kraven enkelt härledas. Tre nivåer finns för krav: grund (G), utökad (U) och hög (H). Tabell 2 beskriver hur kravnivåerna förhåller sig till konsekvensnivåerna och exponeringsnivåerna. Kravmängden är densamma för exponeringsnivå E2 och E3, men det finns skäl

att hålla isär dessa eftersom de skiljer sig i så kallad komponentassuransnivå som beskrivs längre fram i rapporten.

Tabell 2. De tre kravmängderna grund (G), utökad (U) och hög (H) tillsammans med exponering och konsekvensnivå.

		Exponeringsnivå			
		E1	**E2**	**E3**	**E4**
Konsekvensnivå	**K5**	H	H	H	H
	K4	U	H	H	H
	K3	U	U	U	H
	K2	G	U	U	U
	K1	G	G	G	G

Denna förhållandevis enkla modell ligger väl i linje med etablerad säkerhetsteori. Modellen stämmer exempelvis väl överrens med hur allvarligheten på sårbarheter bedöms enligt the *Common Vulnerability Scoring System* (CVSS) [2] – en de facto-standard för att bedöma hur allvarliga enskilda sårbarheter är. CVSS tar bland annat hänsyn till vad en exploaterad sårbarhet kan leda till för konsekvenser, om den är exploaterbar över datornätverk, om det bara är betrodda användare som kan utnyttja den och hur komplex den är att utnyttja (t.ex. om det krävs att användare blir vilseledda). Alla utom komplexiteten passar väl in i KSF:s koncept för konekvens och exponering. På grund av sin enkelhet finns det såklart möjlighet att hitta fall där modellen producerar icke-intuitiva och konstiga resultat. Till exempel gör modellen ingen skillnad på antalet användare av ett system och det är därför samma krav oavsett om det är tre eller 3000 personer som ska använda systemet.

En faktor att ta hänsyn till när systemgränser dras och ett nytt system planeras är hur systemet påverkar exponeringen av andra system. KSF3 är tillåtande om det nya systemet endast ska sammankopplas och utbyta information med betydligt säkrare system. Men förutsättningarna för det betydligt säkrare systemet kan bli annorlunda om det ska kopplas samman med ett mindre säkert system. Nedan följer ett exempel när detta är fallet.

- System EXISTERANDE (E3, K3) behandlar information som är H/C; utbyter information med andra instanser av samma systemtyp; har användare som är säkerhetsprövade, men vissa användare har bara behörighet till H/R eller öppen information.

- System NYTT (E4, K3) behandlar information som är H/C, ska utbyta information med system som bara är ackrediterade till H/R och har användare som är behöriga till all information i systemet.

För system NYTT skulle en sammankoppling med EXISTERANDE inte påverka exponeringen och därmed inte heller IT-säkerhetskraven på systemet. Oavsett om sammankoppling sker eller inte har NYTT högsta exponering (E4) och behöver uppfylla de höga kraven på säkerhetsfunktioner. För EXISTERANDE skulle dock en sammankoppling bli problematisk. Att sammankopplas med ett system med högsta exponering (E4) innebär per automatik att systemet självt får högsta exponering. För ett system som hanterar H/C, vilket EXISTERANDE gör, innebär det strikt tolkat att IT-säkerhetskraven höjs från utökad nivå till hög nivå för såväl EXISTERANDE och alla andra system som EXISTERANDE utbyter information med.

Exakt hur följder av sådana sammankopplingar ska hanteras framgår inte av KSF3. Men det ges exempel som belyser att en viktig del i tillämpningen av KSF3 är att definiera systemet som kraven ska härledas för. Det ges även illustrativa exempel på hur exponeringsnivån i sammansatta system kan reduceras med skydd och hur exponeringen minskas med tunnlad (dvs. krypterad och skyddad) trafik genom högt exponerade miljöer såsom Internet. Det är alltså inte så strikt och enkelt som det först verkar då det finns möjlighet att påverka exponeringen med (extra) säkerhetsskydd som är tillräckligt pålitliga. I exemplet ovan skulle kanske en tillförlitlig datasluss mellan NYTT och EXISTERANDE kunna se till att EXISTERANDE inte påverkas av NYTT:s höga exponering. Alternativt skulle NYTT självt kunna använda en tillförlitlig datasluss för informationsutbyte med H/R-systemen och därmed ha en låg exponering.

Utöver specialfall och undantag av denna typ förklaras i KSF3 även att vissa krav helt enkelt går att uppfylla (och kan bortses från) om systemets miljö är beskaffad på ett visst sätt. Exempelvis kan tänkas att fysiska behörighetskontroller kan ersätta logiska behörighetskontroller om användning av systemet kräver fysisk närvaro och tillträdet är begränsat av vakter och fysiska passersystem.

2.2 Funktionella säkerhetskrav

KSF3 innehåller *funktionella säkerhetskrav* som ställer krav på ”funktion eller beteende hos ett system som syftar till att helt eller delvis ge systemet en viss säkerhetsförmåga” [1]. Kraven är hierarkiskt strukturerade med åtta klasser av funktionella säkerhetskrav. Under dessa klasser finns 23 subklasser (1-5 per klass). Det finns inbördes beroenden för kraven inom dessa klasser och subklasser. Till exempel är vissa av grundkraven för autentisering (t.ex. SFBK_AUT.1, ”Subjekt ska autentiseras vid inloggning och upprättande av session.”) nödvändiga delar av de extra krav som tillkommer på högre nivåer (t.ex. SFBK_AUT.16, ”Sessioner ska omfattas av tidsbegränsning.”) och vissa krav

ersätter andra (t.ex. så blir ”förstärkt inloggning” ”stark inloggning” när nivån ökar från utökad till hög). Totalt innehåller KSF3 148 funktionella säkerhetskrav. På grundnivå ska 83 funktionella säkerhetskrav uppfyllas; på utökad nivå tillkommer 43 krav samtidigt som två krav faller bort; på hög nivå tillkommer ytterligare 22 funktionella säkerhetskrav samtidigt som 6 faller bort. I orienterande syfte ger Tabell 3 en övergripande sammanfattning av hur kraven på de olika nivåerna ökar i form av exempel för valda subklasser. Notera att varje klass innefattar en till fem subklasser och att beskrivningen som ges i tabellen är förenklad.

Från Tabell 3 framgår att kraven inom respektive område i regel är tuffare på den utökade och höga nivån. Ofta innebär detta mer omfattande eller mer frekventa säkerhetskontroller. Utöver detta finns också mer konceptuella skillnader och nya typer av krav som tillkommer. Exempel på detta är krav på att loggar ska anlysseras i ett separat system, att objekt ska säkerhetsmärkas och separation av roller i systemet.

Tabell 3. Exempel på skillnader i funktionella säkerhetskrav på de olika nivåerna (förenklade beskrivningar).

Klass: subklass	**Grund**	**Utökad**	**Hög**
Gemensamma funktioner**:** Säkert tillstånd	Ett ”definierat säkert tillstånd” ska kunna upprätthållas och tiden i systemet ska synkas.	Tillståndet ska kunna upprätthållas även om vissa säkerhetsfunktioner ej fungerar.	Om något är fel måste allt låsas i systemet.
Behörighetskontroll**:** Autentisering av objekt ska ske	Användares unika identitet ska styrkas med åtminstone lösenord.	Förstärkt inloggning krävs.	Stark inloggning krävs.
Säkerhetsloggning**:** Säkerhetsrelaterade händelser ska registreras	Vissa säkerhetshändelser måste loggas tillsammans med relaterad identitet och tid.	Betydligt fler säkerhetshändelser måste loggas.	Även ändringar i systemets konfiguration måste loggas.
Intrångsskydd**:** Systemets komponenter ska härdas mot intrång	Systemet ska följa leverantörens rekommendationer för säker konfiguration.	Säkerhetskänslig funktionalitet som inte används ska tas bort och delar av systemet ska isoleras med existerande behörighetskontroller.	All funktionalitet som inte används ska tas bort och åtkomsträttigheter ska vara restriktiva.

Klass: subklass	Grund	Utökad	Hög
Intrångsdetektering: Intrång och missbruk ska kunna upptäckas och spåras	Kända attackmönster ska upptäckas, signaturer ska kunna anpassas och loggarna ska vara sökbara.	Analyserna ska kunna detektera avvikelser från det normala i exempelvis användningsmönster och dataflöden.	Intrångsdetektering ska ske i ett separat system eller i en separat del av systemet.
Skydd mot skadlig kod: Funktioner för hantering av säkerhetsuppdateringar ska finnas	Det ska gå att kontrollera mjukvaror och säkerställa att uppdateringar är autentiska.	Det ska gå att kontrollera att den senaste versionen av alla mjukvaror används och om systemet är riktigt.	Återkommande automatiska kontrollerer ska göras för att se om den senaste versionen av alla mjukvaror används och om konfigurationen är riktig.
Skydd av röjande signaler: RÖS-krav från gällande regelverk ska uppfyllas	Kraven på RÖS och andra nationers krav gäller.	[Ingen skillnad]	[Ingen skillnad]
Skydd mot obehörig avlyssning: Hemliga uppgifter i elektroniska kommunikationsnät ska skyddas	Kommunikation utan signalskydd får ske inom inhägnat bevakat område eller med obruten fiberkabel som är säkerhetslarmad i ändarna eller med kopparkabel inom sektionerat område.	Kommunikation utan signalskydd får ske genom inspekterbar fiberkabel.	Kommunikation utan signalskydd får endast ske inom sektionerat område.

2.3 Assuranskrav

Assuranskrav är i KSF3 ”krav på förtroende för systemets förmåga att tillhandahålla sin säkerhetsfunktionalitet” [1]. Precis som de funktionella kraven är assuranskraven hierarkiskt ordnade, men med sju klasser och 32 subklasser. Vilken kravnivå som gäller för systemet har dock mindre påverkan på vilka assuranskrav som behöver uppfyllas än vilka funktionella säkerhetskrav som behöver uppfyllas: för 15 av de 32 subklasserna är kraven desamma oavsett nivå och

inom sju subklasser är kraven identiska oavsett om det är ett system på utökad eller hög nivå. I vissa subklasser är skillnaden dock fortfarande stor mellan grundnivån och utökad/hög nivå. Inga krav finns på grundnivån inom de sex subklasserna *Utvecklingssäkerhet*, *Konfigurationsledning*, *Livscykelmodell*, *Gränsytebeskrivning*, *Säkerhetsarkitektur*, *Dataflödesanalys* och *Designdokumentation*. Utöver detta kan skillnaderna mellan de olika nivåerna sammanfattas på följande sätt.

- Inom subklassen *Systemleverans* är den enda skillnaden att det på grundnivå inte krävs att leveransdokumentationen anger hur riktighet ska verifieras vid leverans och därefter.
- Inom subklassen *Utvecklingssäkerhet* är skillnaden mellan utökad och hög nivå att den höga nivån kräver acceptanskriterier och ursprungsidentifikation av alla komponenter, medan utökad nivå enbart behöver göra det för säkerhetsrelaterade komponenter.
- Inom subklassen *Åtkomsträttigheter* är enda skillnaden mellan utökad och hög nivå att det på hög nivå ska finnas rutiner som beskriver hur behörigheter inte får fördelas.
- Resterande skillnader mellan utökad och hög nivå kan sammanfattas med att det på den höga nivån tillkommer krav på att alla säkerhetskomponenter testas, att semiformell sårbarhetsanalys används, att dataflödesanalysen är fullständig, att livscykelmodellen är i linje med ISO 9001, att varje komponents lämplighet verifieras samt att konfigurationsledningssystemet gör ändringar spårbara.

Sammanfattningsvis är det flera typer av assuranskrav som inte krävs för grundnivån men det är liten skillnad mellan utökad och hög nivå.

En betydande del av assuranskraven handlar om ren dokumentation av krav, lösningar och rutiner. De delar som ställer krav på faktiska tester och utvärderingar av säkerheten finns i subklasserna *Testtäckning*, *Funktionstester*, *Angripartester*, *Evaluerarens testning*, *Avvikelseanalys*, *Sårbarhetsanalys* och *Restriskanalys*. Det vill säga, endast sex av 32 subklasser ställer krav på utvärdering av säkerhet eller bevis på säkerhet. I texterna för KSF3 på säkerhetsfunktioner finns dock även begreppet *komponentassurans*, vilket är betydligt närmare den typ av krav som ger direkt assurans än alla de krav på dokumentation som finns i bilagan assuranskrav [3].

Komponentassuransen finns i fyra nivåer och beskrivs kort i KSF3. En kortfattad beskrivning av nivåerna ges nedan.

- N1 tillåter generella produkter som är commercial-off-the-shelf (COTS) om utvecklaren visar prov på gott säkerhetsmedvetande.

- N2 tillåter också generella COTS-produkter, men det krävs att säkerhet hanteras i en dokumenterad säkerhetsprocess.
- N3 kräver att utvecklaren bistår med tillgång till utvecklarens dokumentation och personal. Dessutom ska allt arbete med produkten ske enligt en dokumenterad säkerhetsprocess.
- N4 kräver att MUST evaluerar och godkänner dokumentation samt att utvecklingen sker enligt en formell metod med tydliga avstämningspunkter.

Även dessa nivåer härleds från exponering och konsekvens enligt Tabell 4. Tabellen visar också hur dessa fyra nivåer förhåller sig till de tre kravnivåerna i KSF3. Även om konsekvensnivå och exponeringsnivå är ingångsvärden till komponentassuransnivå bestäms den inte på samma sätt som systemets nivå. Kraven på komponentassurans bestäms nämligen utifrån komponentens individuella exponering och konsekvensnivån på den information som den ska skydda. Om det exempelvis finns systeminterna funktioner för att säkerställa att en komponent i ett K5-system inte kommer att skydda mer än K2-information räcker assurans på K2-nivån. På samma sätt kan exponeringsnivån justeras ner om det är så att komponenten i sig inte är exponerad. Till exempel om den bara skyddar en nätverksdel där samtliga användare är behöriga till all information. Dessutom finns möjligheten att använda komponenter med lägre komponentassuransnivå än vad som anges i Tabell 4 om det kan påvisas att det inte påverkar säkerheten negativt.

Tabell 4. Exponerings- och konsekvensnivå och de tre kravmängderna (Grund, Utökad, Hög) samt komponentassuransnivå (N1-N4).

		Exponeringsnivå			
		E1	**E2**	**E3**	**E4**
Konsekvensnivå	**K5**	H/N2	H/N3	H/N4	H/N4
	K4	U/N2	H/N2	H/N4	H/N4
	K3	U/N2	U/N2	U/N3	H/N4
	K2	G/N1	U/N2	U/N2	U/N3
	K1	G/N1	G/N1	G/N1	G/N1

2.4 Teorier om tillkommande säkerhetskrav

KSF3 är framtaget för att definiera de krav på säkerhetsförmågor som IT-system i Försvarsmakten behöver ha för att tillräckliga skyddsåtgärder ska föreligga.

KSF3 innehåller krav som syftar till att hantera risken kopplat till att en händelse påverkar sekretessen för den information som systemet hanterar. KSF3 fokuserar alltså inte på verksamhetens krav på tillgänglighet, riktighet och spårbarhet när de nödvändiga IT-säkerhetskraven bestäms. Det är därför rimligt att tro att KSF3 missar sådana krav. Det är också rimligt att förvänta sig att ytterligare sekretessrelaterade krav kan behövas för IT-system, till exempel för att en annan nations utrustning ska kunna användas eller för att personuppgiftslagen kräver det. I KSF3 kallas alla ytterligare krav för *tillkommande säkerhetskrav*. De tillkommande säkerhetskraven identifieras genom verksamhets- och säkerhetsanalyserna.

Att KSF3 fokuserar på sekretess betyder inte att alla krav på riktighet, tillgänglighet och spårbarhet är förbisedda. Många populära säkerhetslösningar bidrar till mer än en av dessa egenskaper. Skydd mot skadlig kod skyddar till exempel mot såväl kod som vill extrahera information, kod som vill manipulera information och kod som låser ute användare. Dessutom inkluderar KSF3 krav som är direkt relaterade till riktighet och spårbarhet. Krav på riktighetskontroll finns bland annat för konfigurationer, mjukvaror och meddelanden; krav på spårbarhet finns både i form av krav på loggar och krav på oavvislighet. Inget av dessa krav leder till ökad sekretess i första hand även om det är bra för sekretessen om eventuella antagonister kan avskräckas av att deras handlingar är spårbara och att systemet är som det är tänkt att vara.

Trots att KSF3 redan täcker in vissa krav utöver sekretesskraven finns det skäl att tro att en stor del av de tillkommande kraven syftar till att möta hot mot riktighet, tillgänglighet, och spårbarhet. Nedan presenteras teorier kopplade till dessa tre egenskaper. Teorierna har valts för att de är på ungefär samma abstraktionsnivå som KSF3 när det kommer till variabler som bestämmer kraven. Dessa teorier ska jämföras med modellen i KSF, där exponering och konsekvensnivå är det som bestämmer kravmängden. Tillsammans med detta ges också en bild av populära sätt att klassificera och gruppera kraven. Dessa klassificerings- och grupperingsmetoder ska jämföras med klasserna och subklasserna i KSF3.

2.4.1 Tillgänglighetskrav

Inom tillförlitlighetsforskning och tillgänglighetsforskning finns ett stort antal modeller. Tyvärr har de allra flesta av dessa en helt annan abstraktionsnivå än vad som passar för Försvarsmaktens behov. Typiskt föreslås att krav och bedömningar bör utgå från hur komponenterna strukturerats tillsammans med tillståndsdiagram som har sannolikheter för att komponenter fallerar i olika tillstånd och sannolikheter för att hopp sker mellan olika tillstånd (se t.ex. [4]). Dessa modeller ges information om mer eller mindre konkreta fel- och orsakstyper, såsom vilka faktorer som påverkar livslängden för magnetiska diskar [5] och

SSD-minnen [6]. Det är inte prediktioner på denna detaljerade nivå som KSF3 syftar till, och informationen som behövs (t.ex. hårddiskars egenskaper) finns sällan att tillgå för IT-system under de tidiga faser där säkerhetsrelaterade krav på Försvarsmaktens IT-system ska identifieras.

Litteraturen innehåller få lovande alternativ till detta sätt att identifiera tillgänglighetskrav. Ett undantag är den teori som presenteras av Franke [7]. Franke anser att det förutom den eftersträvade andelen tillgänglighet (t.ex. 99% av året) bör identifieras om det är antalet korta avbrott eller antalet långa avbrott som ska undvikas[2]. Ibland kan korta IT-avbrott vara oproblematiska medan långa avbrott är en katastrof. Ett exempel är kortbetalningssystem där en misslyckad uppkoppling då och då sällan innebär stor skada men ett avbrott på flera dagar skulle vara djupt problematiskt. Ibland kan också korta IT-avbrott vara lika problematiska som långa. Om till exempel styrsystemet för maskinerna i en pappersmassafabrik slutar fungera kortvarigt innebär det typiskt timlånga stopp innan produktionen kan komma igång igen. Skälet till att använda längden på avbrott som parameter är att vissa skydd framförallt skyddar mot korta avbrott (t.ex. en UPS på batteri) medan andra skydd framförallt skyddar mot långa avbrott (t.ex. en dieselgenerator). Naturligtvis finns det saker som påverkar såväl antalet korta som långa avbrott (t.ex. god kvalité på komponenter), men det förtar inte värdet av att kunna identifiera de krav som motverkar korta respektive långa avbrott.

Litteraturen har mer att erbjuda när det kommer till klassificering och gruppering av tillgänglighetskrav och tillgänglighetslösningar. Till exempel kan innehållsförteckningar i böcker om tillgänglighet användas som utgångspunkt för en sådan klassificering. När Franke [8] sammanfattar de kausala faktorer som nämns i en bok skriven av Marcus och Stern [9] så är resultatet 16 kategorier. Några exempel på dessa är fysisk miljö, drift, ändringshantering, teknisk backuplösning, redundans i infrastruktur och undvikande av externa tjänster som fallerar (vår översättning). Det är också förhållandevis rättframt att identifiera mer granulära och mer abstrakta kategoriseringar än denna. Underkategorier till de 16 kausala faktorerna (t.ex. *luftfuktighet i fysisk miljö*) ger mer granularitet medan generaliseringar (t.ex. sammanslagning av allt som handlar om *redundans*) ger mer abstraktion. Litteraturen innehåller även andra förslag på mer abstrakta och mer granulära kategoriseringar. De tre feltyper som listas av Morgan m.fl. [10] är ett exempel på något mer abstrakt. Morgan m.fl. anser att fel antingen är (1) design- eller implementationsfel, (2) komponentfel eller (3) fel skapade av operatör eller användare.

Ett problem med den tillgängliga litteraturen är att den så gott som uteslutande avser tillgänglighetsproblem som uppstår utan att någon har illvilliga avsikter.

[2] En annat sätt att tänka kring detta är om syftet är att minska tiden mellan avbrott (mean-time-between-failure, MTBF) eller reparationstiden (mean-time-to-repair, MTTR). Tillgänglighet (upptid) definieras ofta med hjälp av dessa två variabler: Tillgänglighet = MTBF/(MTBF+MTTR).

Teorierna är alltså, till skillnad från KSF, inte fokuserade på aktörsdrivna eller antagonistiska hot. Teoretiska modeller och skydd skapta för stokastiska fel som antas vara oberoende har en tveksam validitet om hotet istället består av en antagonist som kan introducera fel på ett strategiskt och ondsint sätt. Till exempel kan skadlig kod slå ut såväl ordinarie system som backupsystem samtidigt, men för ett hårdvarufel drabbas förmodligen inte både körande instans och backup vid samma tidpunkt. Avsaknaden av antagonistiskt perspektiv talar emot att basera en KSF-utökning på kategoriseringar som är tillgängliga i litteraturen.

2.4.2 Riktighetskrav

När det gäller *riktighet* finns en uppsjö av modeller att tillgå. Många av dessa har en tydlig koppling till de krav som finns i KSF3. Det finns till exempel modeller och lösningar för att verifiera riktigheten för kod som exekveras i olika maskinarkitekturer [11], riktighetskontroller i databaser [12], förhindrande av illvillig manipulation genom separation av roller [13] och bevismodeller för att filer överförts utan att deras riktighet påverkats [14]. Men även om det finns många modeller som matchar kraven i KSF3 konceptuellt sett, är de i regel på en helt annan abstraktionsnivå. Modellen för att verifiera riktigheten för kod som presenteras i [11] handlar till exempel om sätt att markera upp och kontrollera enskilda kodstycken medan KSF3:s krav på riktighet formuleras på nivån att *”objekt ska kontrolleras innan de accepteras för användning*” (SFSK_EXE.2); lösningen för förhindrande av illvillig manipulation genom separation av roller i [13] är en notation för att hålla koll på alla tidigare roller som individer haft i systemet medan KSF3 kräver att rollerna för säkerhetslogg, daglig drift och tilldelning av åtkomsträttigheter kan separeras. Modeller som dessa matchar alltså inte KSF3:s abstraktionsnivå och är snarare möjliga lösningar på KSF3:s krav under särskilda omständigheter. De passar därför dåligt som utgångspunkt för ett eventuellt komplement. Två etablerade modeller som har fokus på att bevara riktighet under antagonistiska hot och som har lämplig abstraktionsnivå är Bibas modell [15] och Clark-Wilsons modell [16].

Bibas modell är förhållandevis enkel och innehåller två regler: (1) informationens riktighetsnivå ska anges med en nivå (som konsekvensnivåerna i KSF3) och (2) information ska inte skrivas till högre nivåer eller läsas från lägre nivåer. System konstruerade på detta sätt skulle förmodligen ge liten nytta för Försvarsmakten eftersom det skulle innebära stora begräsningar i vilket datautbyte som får göras.

Clark och Wilsons [16] modell är lite mer pragmatisk då den fokuserar på hur riktighet ska kunna tillgodoses i mer komplexa miljöer som inte kan uppfylla de strikta kraven i Bibas modell. Modellen använder två procedurer, två typer av dataobjekt och två typer av regler. Procedurer är antingen procedurer för verifikation av riktighet eller transformationsprocedurer; dataobjekt är antingen interna (constrained) eller externa (unconstrained); regler är antingen certifieringsregler

eller tillämpningsregler. Utifrån detta beskrivs fem certifieringsregler och fyra tillämpningsregler för hur de interna dataobjektens riktighet ska bibehållas. Den första certifieringsregeln säger till exempel att riktighetsverifikationsprocedurer ska säkerställa att systemet är i ett godkänt tillstånd, medan den tredje tillämpningsregeln säger att användare ska autentiseras innan de tillåts exekvera en transformationsprocedur. Omtolkat till kravklasser kan Clark och Wilsons nio regler bli: (1) krav på riktighetsverifikationer, (2) krav på pålitlig programkod, (3) krav på indatakontroll till program, (4) krav på indatakontroll betingad på användare, (5) krav på separation av roller, (6) krav på användarautentisering, (7) krav på loggning, (8) krav på kontroll av extern data och (9) krav på separation av certifierare och användare.

Det finns också alternativ som klassificerar tekniker som syftar till att säkerställa riktighet. I [17] föreslås till exempel en indelning av lösningar baserat på (1) om de ska förebygga riktighetsproblem eller detektera och åtgärda dem, (2) nivån som angrepp sker på och vilken nivå kontrollen behövs på och (3) om riktighet behöver säkerställas kontinuerligt eller om det räcker att göra det på begäran.

Den samlade bedömningen är dock att ytterligare nedbrytningar av riktighetskrav och faktorer som påverkar vilka riktighetskrav som behövs är överflödigt att presentera i denna rapport. KSF3 innehåller redan idag krav som passar in på alla av Clarks och Wilsons regler. KSF3 innehåller alltså redan samtliga typer av riktighetskrav som behövs enligt en av de etablerade teorierna.

2.4.3 Spårbarhet

Spårbarhet i IT-system kan motiveras av flera skäl. Ett motiv till att ha god spårbarhet är det som på engelska kallas *deterrence theory* – teorin att hårda, sannolika och snabba bestraffningar minskar avsikterna att begå brott. Empirisk forskning på efterlevnad av informationssäkerhetsbestämmelser pekar på en komplex relation mellan avskräckningsmekanismer och viljan att följa bestämmelser, med spretiga och ibland motstridiga resultat [18]. Inom vissa domäner är spårbarhet ändå centralt som säkerhetsmekanism. Inom vård och polisiär verksamhet är det till exempel praxis att behörigheter i system är generösa och tekniskt tillåter att användare slår fritt i databaser under vetskap att missbruk sannolikt beivras i efterhand.

En stor andel av spårbarhetsforskningen rör forensiska analyser, vilket i IT-sammanhang innebär studier av digitala system för att spåra olika typer av aktivitet. Forensiska analyser är inte enbart värdefulla för att spåra inkräktare och bedöma informationsförluster (t.ex. kopierade dokument), utan de är också värdefulla för att på ett effektivt och precist sätt städa upp efter incidenter. Exempelvis visar [19] på att riktade IT-attacker i genomsnitt inte detekteras förrän efter 312 kalenderdagar, vilket innebär att en mängd illvilliga aktiviteter hinner utföras innan detektion. Om det finns goda stöd i form av loggar och verktyg för att

utföra forensiskt arbete när skadlig kod upptäcks så blir arbetet med att spåra all illvillig aktivitet som utförts snabbare och bättre utfört.

Garfinkel m.fl. [20] summerar forskningen kring IT-forensiska analyser och beskriver att det finns otaliga metoder och verktyg för ändamålet – exempelvis hur krypterade filer bäst identifieras [21] och hur bildfiler analyseras på bästa sätt [22] – men att det saknas goda standarder. Med andra ord, det finns en stor spridning av tekniska metoder för IT-forensiska analyser som skulle kunna användas för att realisera kraven i KSF3, men det saknas etablerade teorier som behandlar KSF3:s abstraktionsnivå.

3 Analys av säkerhetsmålsättningar

I detta kapitel presenteras en analys av säkerhetsmålsättningar för IT-system som redan har godkänts av Försvarsmakten. Avsnitt 3.1 presenterar metoden som använts och de säkerhetsmålsättningar som legat till grund för analysen. Avsnitt 3.2 beskriver de tillkommande kraven genom att klassificera dem och ge exempel på sådana krav. Projektet gavs inte tillgång till tillräckligt många säkerhetsmålsättningar för att med god empirisk grund kunna undersöka vilka faktorer som driver tillkommande krav. Avsnittet försöker ändå ge ett svar på frågan om faktorer som driver tillkommande krav utifrån den empiri som varit tillgänglig och de argument som har använts i säkerhetsmålsättningarna. Avsnitt 3.3 presenterar skillnader mellan KSF3 och KSF2 (som gällde då säkerhetsmålsättningarna skapades). I Avsnitt 3.4 diskuteras resultatet.

3.1 Metod för att jämföra krav

Totalt 13 olika säkerhetsmålsättningar ligger till grund för den analys som beskrivs i detta kapitel. En översikt av den information som dessa säkerhetsmålsättningar behandlar, samt de krav som de innefattar ges i Tabell 5. Då de skapades mellan 2005 och 2014 utfördes kravhanteringsprocesserna för dessa säkerhetsmålsättningar innan införandet av KSF3. Detta bör tas i åtanke när resultaten tolkas.

Tabell 5. Översikt av innehållet i de säkerhetsmålsättningar som studerats.

ID	År	Verksamhetsbeskrivning	Styrande säkerhetsmål	Systembeskrivning	Regelverksanalys	Informationsklassning	Hot-, risk och sårbarshetsanalys	Hotbildsanalys	Säkerhetsanalys	Säkerhetsmål	Bedömda krav
1	2014								•		0
2	2014								•		0
3	2014								•		0
4	2011	•	•	•	•	•	•		•	•	250
5	2011	•			•	•	•	•	•	•	72
6	2012	•	•	•	•	•		•			241
7	2005	•			•	•		•	•	•	3
8	2006					•			•		1
9	2004	•		•	•	•		•			1
10	2010				•						0
11	2009	•			•	•	•	•		•	90
12	2005	•			•			•	•	•	0
13	2006	•		•	•	•	•	•		•	125

Alla krav nedtecknades från dessa 13 säkerhetsmålsättningar av två forskare med hjälp av ett extraheringsformulär. För varje krav nedtecknades ett unikt identifikationsnummer, den relevanta säkerhetsmålsättningen (1-13), identifikationsnumret i säkerhetsmålsättningen (t.ex. ”HSIS-5-6” och ”Sec 10”), kravområdet (t.ex. ”Verksamhetskrav” eller ”Säkerhetsmål[3]”), kravets kategori (t.ex. ”Behörighetskontroll”, ”Intrångsdetektion” och ”Tillgänglighet”), kravets källa (t.ex. ”KSF ej hemliga uppgifter” och ”KSF H/S”), kravets motivering (t.ex. referens till specifikt hot eller Taktisk Teknisk Ekonomisk Målsättning), kravets lösning

[3] Säkerhetsmål är oftast formulerade som krav (t.ex. ”Antalet möjliga misslyckade inloggningsförsök skall vara begränsat”) men ibland även som mål (t.ex. ”Förhindra att sekretessklassat materiel kommer obehörig tillhanda”).

(t.ex. ”Tas om hand av delsystem X” eller ”att endast av FM tillhandahållna krypton nyttjas”), den faktiska kravtexten, samt förklarande kommenterar från den ansvarige forskaren. Extraheringsformuläret togs fram via studier av säkerhetmålsättningarna och formaliserades genom en intern workshop inom projektgruppen.

Vissa krav är pekare mot andra dokument som innehåller faktiska krav. Exempelvis kan en sådan pekare vara att alla KSF2-krav för H/S ska vara uppfyllda, eller att fysisk säkerhet ska uppfylla bestämmelserna i extern samarbetspartners regelverk. Om dokumentet som pekades på fanns tillgängligt extraherades alla relevanta krav från det enligt tidigare beskriven process. Om det inte fanns tillgängligt behölls det som ett enda unikt krav.

En översikt av resultatet av detta arbete beskrivs i Tabell 5. Av de 13 säkerhetsmålsättningarna innehöll åtta antingen mycket få (i tre fall) eller inga (i fem fall) krav. Säkerhetsmålsättning fyra och sex innefattade majoriteten av kraven, men överlappar också till stor del då båda dokumenten kräver att KSF2 H/S (109 krav) uppfylls.

Efter att samtliga krav (totalt 672 unika) hade extraherats kartlades de mot KSF3. Fyra forskare var delaktiga i kartläggningsarbetet där varje krav granskades av minst två forskare. Denna metod valdes då kravbedömning inte är en rättfram process med ett enkelt svar – samma krav kan bedömas olika av olika människor (och vid olika tillfällen). För varje krav angavs alla KSF3-krav (både funktionella säkerhetskrav och assuranskrav) som det motsvarade. Om det inte gick att kartlägga mot enskilda krav, men mot kravklasser i KSF3 så användes denna kategori (t.ex. kravet ”[…] ska vara försett med av MUST godkänd funktion för behörighetskontroll” kartlades mot kravklassen behörighetskontroll [SFBK] i KSF3). Om kravet inte hade någon motsvarighet i KSF3 så bedömdes det som *Tillkommande*; om kravet var för oklart för att bedömas alls så bedömdes det som *Oklart*.

Ett skript användes sedan för att automatiskt bedöma hur samstämmiga bedömningarna av varje krav var enligt en egenutvecklad heuristik. Skriptet jämförde samtliga kombinationer av bedömningar gjorda av forskarna. Om bedömningarna av ett krav matchade helt gavs maxvärdet 1 i samstämmighet. Om de inte matchade helt användes en straffunktion för att räkna ut avståndet mellan bedömningarna[4]. Mindre lika bedömningar gav lägre samstämmighetsvärde. Per-

[4] Om forskare angav olika KSF3-krav, men dessa rörde samma huvudklass och subklass (t.ex. SFBK_AUT.1 och SFBK_AUT.2) så gavs ett straff på -0.1.
Om forskare angav KSF3-krav med olika subklasser, men med samma huvudklass (t.ex. SFBK_AUT.1 och SFBK_ÅTK.1) så gavs ett straff på -0.2.
Om forskare angav KSF3-krav med olika subklasser och huvudklasser (t.ex. SFBK_AUT.1 och SFSL_ANA.1) så gavs ett straff på -0.5.
Om forskare angav bedömningar som inte alls överensstämde (t.ex. Tillkommande och SFBK_AUT.1) så gavs ett straff på -1.

fekt samstämmighet mellan bedömarnas klassificering fanns för cirka hälften av alla krav (348 krav) och den högsta negativa samstämmighetsvärde ett krav fick var -8. Fördelningen över de olika kravtyperna ges i Tabell 6. Differensen i samstämmighet mellan typerna är statistiskt signifikant: test med envägs-ANOVA visar att det är mindre än en tusendels promilles sannolikhet att skillnaderna i samstämmighet beror på slumpen. Samstämmigheten var störst för tillkommande krav och lägst för krav av oklar typ. Samstämmigheten var också högre för funktionella säkerhetskrav än för assuranskrav.

Tabell 6. Samstämmighet för kravbedömningar. Ett högre värde indikerar större samstämmighet.

Mätvärde	Assurans	Funktionellt	Tillkommande	Oklart
Antal krav	65	223	308	76
Samstämmighet (medel)	0,45	0,60	0,77	0,18
Samstämmighet (varians)	0,22	0,24	0,22	1,15

Som nästa steg i processen diskuterade forskarna alla krav som det inte förelåg fullständig konsensus kring (324 krav, eller 48% av kravmassan) i grupp. Målet med denna diskussion var att uppnå en klassificering som alla forskare kunde enas om. Under detta arbete blev det tydligt att åsikterna kring assuranskraven skilde sig mer åt än för de funktionella och tillkommande kraven. Dessutom tog det mycket mer tid att nå en samstämmighet kring assuranskraven än för de övriga kraven. Orsaken till detta var assuranskravens mer abstrakta natur. Med grund i detta avgränsades de 65 identifierade assuranskraven från fortsatt analys i studien.

Det avslutande steget i processen bestod av att kategorisera de tillkommande kraven.

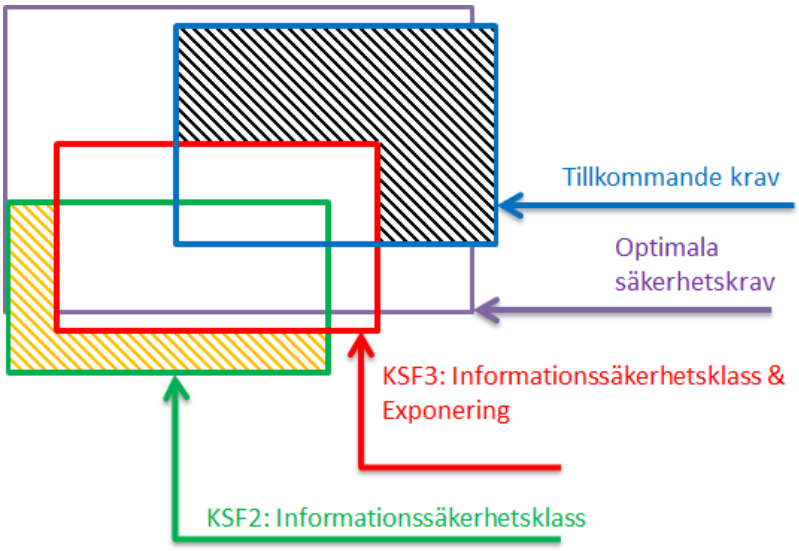
3.2 Tillkommande krav

Kraven i KSF3 ger endast stöd vid identifierandet av nödvändiga krav för att minska risker som påverkar sekretessen för den information som bearbetas, lagras eller på annat sätt hanteras av systemet [1]. Resterande krav på ett IT-system identifieras genom verksamhetsanalysen, säkerhetsanalysen och författningsanalysen. De krav som identifieras i dessa analyser kallas inom Försvarsmakten för *tillkommande krav*.

Den studie som genomförts av tillkommande krav utgick från de godkända säkerhetsmålsättningar som presenterades i Tabell 5. Fokus låg på de tillkommande krav som identifierats i verksamhetsanalysen och säkerhetsanalysen. Krav som

härrör från författningsanalysen har inte analyserats i denna studie. Säkerhetsmålsättningarna innehöll totalt 672 krav. Av dessa bedömdes 288 täckas in av redan befintliga krav från KSF3. Ungefär hälften av kraven som täcktes in av KSF3 var från KSF2 och den andra hälften var tillkommande krav som identifierats i verksamhetsanalysen eller säkerhetsanalysen. Det verkar således som att delar (ungefär en femtedel) av det som tidigare var tillkommande krav nu omfattas av KSF3.

För att få en rättvisande bild av vilka krav som skulle anses vara tillkommande krav i dagsläget, baserat på KSF3, utgick denna studie av tillkommande krav från de krav som inte bedömdes vara KSF3-krav. Detta motsvarar i Figur 1 den svartstreckade och den orangestreckade ytan och innefattar totalt 308 krav. Den orangestreckade ytan består av de KSF2-krav som inte omfattas av KSF3. Då dessa krav var obligatoriska när säkerhetsmålsättningarna gjordes är det svårt att veta om det är krav som annars skulle ha identifierats som tillkommande krav. I denna studie är utgångspunkten att alla krav som inte omfattas av KSF3 är möjliga tillkommande krav. Den svartstreckade och den orangestreckade ytan kommer fortsättningsvis refereras till som de tillkommande kraven.



Figur 1: Visualisering av olika kravmängder. Den svartstreckade ytan motsvarar de tillkommande krav från säkerhetsmålsättningarna som inte bedöms ha någon motsvarighet i KSF2 eller KSF3. Den orangestreckade ytan motsvarar de KSF2-krav som inte har sin motsvarighet i KSF3. Rektanglarnas storlek motsvarar inte förhållandet mellan kravmängderna.

För att få en uppfattning om vilka risker som minskas genom de tillkommande kraven gjordes en bedömning av vilka kvaliteter kraven påverkar. Minst två fors-

kare bedömde varje krav. De kvaliteter som användes i bedömningen var *tillgänglighet*, *sekretess*, *riktighet*, *spårbarhet* och *annat*. Kvaliteten *annat* användes då kravet bedömdes påverka något annat än de andra fyra kvaliteterna. Detta kunde vara krav såsom ”Risken för personskada p.g.a. fientligt angrepp, överfall eller inbrott skall minimeras”. För de krav där det inte var konsensus mellan forskarnas bedömningar gjordes en gemensam genomgång för att nå konsensus. Resultatet av bedömningen återges i Tabell 7. Övriga kombinationer av kvalitetsuppfyllnad än de som återges i tabellen hade inga eller få krav och togs därför inte med i tabellen. Dessa övriga kombinationer innefattade totalt 26 krav (8%).

Tabell 7: Resultat från bedömning av vilka av kvaliteterna *sekretess*, *riktighet*, *tillgänglighet*, *spårbarhet* och *annat* som varje krav påverkar.

Sekretess	Riktighet	Tillgänglighet	Spårbarhet	Annat	Antal	Andel
•					17	6%
	•				8	3%
		•			47	15%
			•		11	4%
				•	64	21%
•	•				22	7%
•	•	•	•		80	26%
•	•	•	•	•	33	11%

De tillkommande kraven analyserades för att identifiera vilka olika kategorier av krav som förekommer i säkerhetsmålsättningarna. Kraven bedömdes först utifrån om de avsåg något fysiskt och om de syftade till att motverka antagonistiska händelser. Kraven fördelade sig enligt Tabell 8.

Tabell 8: Fördelningen av fysiska och antagonistiska krav.

		Antagonistiskt		
		Ja	**Nej**	**Oklart**
Fysiskt	**Ja**	87	36	1
	Nej	118	63	0
	Oklart	2	1	0

I många fall kan kraven tolkas som att de syftar till att motverka både antagonistiska och icke-antagonistiska händelser. Exempelvis kan kravet ”Avbrottsfri kraft

av typ B bör medge operativ drift om 7 dygn” hjälpa till att hålla tillgängligheten på en acceptabel nivå om det blir strömavbrott på grund av blixtnedslag, men det skulle även kunna vara motiverat av att antagonister medvetet slår ut kraftförsörjningen. I fall som detta, då både antagonistiska och icke-antagonistiska händelser kan vara aktuella, bedömdes vad det primära syftet med kravet var givet andra krav i säkerhetsmålsättningarna samt hur det presenterades i säkerhetsmålsättningen. Drygt 67% av kraven bedömdes syfta till att primärt motverka antagonistiska händelser, medan 32% bedömdes motverka icke-antagonistiska händelser. För ett krav var det inte möjligt att avgöra huruvida det syftade till att motverka antagonistiska händelser eller ej.

Noterbart är att mer än en fjärdedel av kraven bedömdes ha en påverkan på alla de fyra kvaliteterna sekretess, riktighet, tillgänglighet och spårbarhet. Alla dessa 80 krav syftar dessutom till att motverka händelser av antagonistisk art. Det huvudsakliga skälet är att dessa krav handlar om skydd mot antagonistiska händelser där den eventuella skadan till stor del beror på antagonistens syfte. Ett exempel på detta är kravet ”Klienter skall förvaras inom av Försvarsmakten tillträdesskyddat område”. Detta krav bedöms motverka stöld av klienter alternativt att obehöriga kan skaffa sig tillgång till klienter för att manipulera eller extrahera information. Vad som är möjligt för en antagonist om den får tillgång till en klient beror också på omständigheter som kravet inte tar upp – exempelvis om en användare är inloggad på klienten eller ej.

Cirka 40% av kraven handlade om skydd av fysiska artefakter. Inom dessa identifierades fyra tydliga kategorier: *elförsörjning* (15%), *nätverk* (21%), *plats/miljö* (25%) och *inbrottsskydd/skalskydd* (48%). De krav som inte passade in i någon av dessa kategorier placerades i kategorin *övrigt fysiskt* (16%). Vissa krav passade in i flera kategorier, oftast på grund av att de var sammansatta krav som innehöll flera krav, men också för att kategorierna inte är ortogonala – skalskydd kan exempelvis motiveras för att systemet är i en viss miljö. I de fallen markerades att kravet tillhörde alla de kategorier som var relevanta. För tre krav kunde det inte avgöras vad som skyddades. Resterande krav handlade alltså om skydd för något icke-fysiskt, som information i IT-system eller en användarsession. Bland kraven på icke-fysiska artefakter kunde fyra kategorier identifieras: *konfigurationsmöjligheter* (68%), *användarfunktionalitet* (28%), *dokumentation/utbildning* (14%) och *organisation* (4%).

Tabell 9 ger en överblick av hur de olika kraven fördelar sig inom de kategorier och kvaliteter de påverkar. Tabellen visar hur många krav som placerats i varje kategori fördelat på vilka kvaliteter kraven uppfyller. Resultatet diskuteras för varje kategori i avsnitten som följer.

Tabell 9: Antalet krav per kategori för varje befintlig kombination av kvaliteterna *sekretess*, *riktighet*, *tillgänglighet*, *spårbarhet* och *annat*.

Sekretess	Riktighet	Tillgänglighet	Spårbarhet	Annat	Elförsörjning	Nätverk	Plats/miljö	Inbrottsskydd/skalskydd	Övrigt fysiskt	Konfigurationsmöjligheter	Användarfunktionalitet	Dokumentation/utbildning	Organisation
•					1	3	4	1	4	5	3	1	0
	•				0	0	1	0	2	4	2	0	0
		•			14	10	7	9	3	8	11	4	1
			•		0	0	0	1	1	8	0	1	0
				•	1	3	5	4	4	13	20	15	5
•	•				0	3	2	2	3	13	1	0	0
•			•		0	0	0	0	0	2	2	0	0
•				•	0	0	2	1	0	0	0	0	0
		•	•		0	0	0	0	0	0	0	1	0
		•		•	2	1	0	1	0	2	4	0	0
			•	•	0	0	0	0	0	3	1	0	0
•	•	•			0	1	1	0	0	3	1	0	0
•	•		•		0	0	0	1	0	1	0	0	0
•	•			•	0	0	0	0	1	0	1	0	0
	•	•	•		0	0	0	1	0	1	0	0	0
•	•	•	•		1	3	6	16	2	53	4	2	1
•	•	•	•	•	0	2	3	23	0	7	0	1	0

3.2.1 Krav på skydd av fysiska artefakter

I detta avsnitt beskrivs innehållet i kategorierna för krav på skydd av fysiska artefakter.

Elförsörjning

Kraven på IT-systemets elförsörjning syftar primärt till att tillhandahålla en adekvat tillgänglighet. Av de 19 krav som bedömdes tillhöra kategorin elförsörjning var det endast två krav som inte påverkade tillgängligheten. Enligt bedömningen handlar de flesta kraven i denna kategori (79%) om skydd mot strömavbrott som inte orsakas av antagonister.

Nätverk

Totalt kategoriserades 26 krav som tillhörandes denna kategori. Påverkan på kvaliteter ser något annorlunda ut jämfört med elförsörjning då det är fler krav som inte bedöms påverka tillgängligheten. Av de 26 kraven bedöms endast 17 (65%) påverka IT-systemets tillgänglighet och 12 (46%) bedömdes handla om krav på sekretess. Fördelningen mellan antagonistiska (54%) och icke-antagonistiska (46%) händelser är också annorlunda än i elförsörjningskategorin. Båda dessa skillnader är rimliga eftersom nätverk kan innehålla information som är sekretessbelagd.

Plats/miljö

Kraven på plats och miljö var 31 till antalet och de handlar till stor del om var olika typer av utrustning ska placeras. Kraven har en ganska spretig påverkan på de olika kvaliteterna. De två vanligaste kvaliteterna som påverkas är sekretess (58%) och tillgänglighet (55%). Närmare 68% av kraven syftar till att motverka antagonistiska händelser. Det finns en tydlig korrelation mellan att sekretessen påverkas och att kravet syftar till att motverka antagonistiska händelser – hela 94% av kraven som påverkar sekretessen har även bedömts motverka primärt antagonistiska händelser.

Inbrottsskydd/skalskydd

Kraven i kategorin *inbrottsskydd/skalskydd* var 60 till antalet och har till stor del påverkan på många olika kvaliteter. Anledningen till detta är svårigheten att på förhand bedöma vad som är syftet med ett inbrott eller angrepp. Drygt 87% av kraven bedöms motverka händelser av antagonistisk art. Om ett inbrott sker i syfte att få tillgång till känslig information eller om det sker i syfte att få tag i icke-känslig hårdvara att sälja har naturligtvis stor påverkan på vilka kvaliteter som påverkas av inbrottet. Totalt 16 krav (27%) bedöms påverka alla de fyra kvaliteterna *sekretess*, *riktighet*, *tillgänglighet* och *spårbarhet* medan ytterligare 23 krav (38%) även bedöms ha en påverkan på något mer (*annat*) utöver de fyra säkerhetskvaliteterna.

Övrigt fysiskt

Kategorin *övrigt fysiskt* innefattar 20 krav som bedömdes handla om fysiska faktorer, men samtidigt inte direkt passade in i någon av kategorierna *elförsörjning*, *nätverk*, *plats/miljö* eller *inbrottsskydd/skalskydd*. Dessa omfattar exempelvis krav på att det inte ska krävas stora manuella insatser vid avhjälpande underhåll, och krav på hur märkning av fysisk lagringsmedia ska göras. De kvaliteter som påverkas till störst grad är sekretess (50%) och riktighet (40%). Även för denna kategori finns en tydlig samstämmighet (90%) i att det är krav som påverkar sekretessen och som syftar till att motverka antagonistiska händelser.

3.2.2 Krav på skydd av icke-fysiska artefakter

I detta avsnitt beskrivs innehållet i kategorierna för krav på skydd av icke-fysiska artefakter.

Konfigurationsmöjligheter

Kategorin *konfigurationsmöjligheter* omfattar icke-fysiska krav som primärt specificerar funktionalitet som möjliggör konfiguration av systemets säkerhetsfunktioner. Totalt bedömdes 123 krav tillhöra denna kategori. Vanligast (43%) är att kraven påverkar alla fyra kvaliteterna *sekretess*, *riktighet*, *tillgänglighet* och *spårbarhet*. Att en så stor andel bedöms påverka fyra kvaliteter beror på att införandet av funktionalitet för att ändra konfigurationen av säkerhetsfunktionerna (t.ex. att förändra när kontroller av IT-systemet sker) skulle få olika påverkan beroende på val av konfiguration. Denna kategori innefattar primärt krav som motverkar antagonistiska händelser (87%).

Användarfunktionalitet

Användarfunktionalitet är kategorin för icke-fysiska krav som kravställer funktionalitet som fokuserar på att IT-systemet ska vara användbart och ha den funktionalitet som användarna behöver. Fokus ligger alltså inte på systemets säkerhet. Kategorin innefattar totalt 50 krav varav hälften bedöms påverka kvaliteten *annat* (dvs. inte informationssäkerhet). Anledningen till att hälften av kraven bedöms påverka någon av de mer säkerhetsrelaterade kvaliteterna beror på att användarfunktionalitet och konfigurationsmöjligheter ibland sammanfaller. Exempelvis kan krav på att en funktion för *klippa och klistra* ska vara avstängd både anses vara ett krav som handlar om konfigurationsmöjligheter samtidigt som det begränsar användarfunktionaliteten. Kraven i kategorin som helhet är mestadels fokuserade på icke-antagonistiska händelser (64%).

Dokumentation/utbildning

Kategorin *dokumentation/utbildning* omfattar krav som fokuserar på vad som ska dokumenteras eller på vilka utbildningar som ska genomföras. I kategorin återfinns 25 krav där den vanligaste kvalitetspåverkan inte är på någon av de mer

säkerhetsinriktade kvaliteterna utan istället på kvaliteten *annat* (64%). Den näst vanligaste kvaliteten som påverkas är tillgänglighet (32%), vilket kan förklaras med att det finns kravställning på exempelvis dokumentation i form av avbrottsplaner eller utbildning av personal i att hantera driftstopp. Kraven i denna kategori fokuserar primärt (76%) på att motverka händelser som är av icke-antagonistisk art.

Organisation

Endast 7 krav ingår i kategorin *organisation* som innefattar krav på struktur och roller i organisationen. Det kan innebära krav på att vara organiserad så att nyckelpersonberoende undviks. Den vanligaste kvalitetspåverkan i denna kategori är *annat* (71%). Andelen krav som syftar till att motverka icke-antagonistiska händelser uppgår även den till 71%, dock är det inte samma delmängd av kravmassan som påverkar *annat*.

3.2.3 Faktorer som motiverar tillkommande krav

Det huvudsakliga målet med den första studien beskriven i denna rapport var att identifiera enkla metoder för att kunna prediktera de tillkommande krav som är passande för ett system. Att reda ut detta med den begränsade empiri som funnits tillgänglig för projektet (de fem säkerhetsmålsättningarna beskrivna ovan) med någon större säkerhet har inte varit möjligt. Det finns också egenskaper associerade till säkerhetsmålsättningarna som gör det svårt att dra slutsaster. Några av dessa återges i följande punktlista.

- Även om stora ansträngningar gjorts för att ge oss tillgång till säkerhetsmålsättningarna är urvalet ett bekvämlighetsurval som förmodligen inte är representativt. Det finns till exempel skäl att tro att det är vissa skapare av säkerhetsmålsättningar som är överrepresenterade i urvalet.
- Många krav är oprecisa eller på hög abstraktionsnivå. Majoriteten (57%) av de tillkommande kraven täcker till exempel in minst tre av de fyra säkerhetskvaliteterna sekretess, riktighet, tillgänglighet och spårbarhet.
- Två säkerhetsmålsättningar (ID 4 och 6 i Tabell 5) står för över hälften (60%) av de tillkommande antagonistiska kraven. Dessa två är också relaterade till varandra.
- Bara två tredjedelar av de tillkomande kraven handlar om skydd mot antagonistiska hot och drygt en tiondel av dessa handlar inte alls om IT-säkerhet utan om personskydd eller liknande.

Trots dessa problem finns det tydliga tendenser som är värda att rapportera när det kommer till krav motiverade av antagonistiska hot. En tydlig tendens är att antalet tillkommande krav hänger ihop med sekretessnivån som systemet ackrediteras för. De två säkerhetsmålsättningarna med högst informationssäkerhets-

klass står för 79 respektive 53 av de tillkommande kraven, den med tredje högst står för 40 av de tillkommande och de resterande systemen står tillsammans för 35 av de tillkommande kraven. Att hög informationssäkerhetsklass innebär fler krav var väntat. En annan tydlig tendens är att användning av andra aktörers system kan innebära att avtalskrav behöver följas. I den säkerhetsmålsättning som innehåller flest tillkommande krav härrör en tredjedel från krav kopplade till användning av andra aktörers kryptografiska utrustning.

Drygt sex av tio krav påverkar systemets tillgänglighet. Också detta var väntat eftersom tillgänglighet inte är någon parameter när kravnivå ska bestämmas och eftersom ordet tillgänglighet inte ens nämns i de funktionella säkerhetskraven förutom när det handlar om information som ska vara tillgänglig för säkerhetsanalys, uppdateringars tillgänglighet eller när det handlar om funktioner som inte ska vara tillgängliga. Av Frankes sexton kausala faktorer för att öka tillgänglighet [8] dominerar fysisk miljö och fysisk plats bland de tillkommande kraven med antagonistisk motivering och det finns exempelvis inga krav som handlar om att undvika fel i komponenter eller att undvika externa beroenden. Många av dessa tillgänglighetskrav har alltså en koppling till fysiskt skydd.

De två säkerhetsmålsättningar som står för merparten av de tillkommande säkerhetskraven är system som kräver en fysisk installation i utmarken och syftar till att ge stöd i form av taktisk kommunikation. Jämfört med de andra systemen har dessa två säkerhetsmålsättningar en relativt hög andel tillkommande krav som berör fysiska skydd. Dessa har 59% respektive 49% av kraven medan övriga säkerhetsmålsättningar i snitt har 28% krav som berör fysiska skydd. De flesta av dessa tillkommande krav rör skydd av byggnad eller kraftförsörjning. En möjlig orsak är att sådana fysiska IT-säkerhetskrav följer av utlokalisering av IT-system utanför bevakade områden. Det bör dock noteras att dessa två system också är de med högst informationssäkerhetsklass och att det därför är svårt att dra en sådan slutsats.

3.3 Skillnader mellan KSF2 och KSF3

Vid kartläggningen av krav noterades att en av de studerade säkerhetsmålsättningarna innefattade KSF2:s krav för öppna system och två innefattade KSF2:s krav för H/S[5]. Som en tilläggsanalys tolkades dessa krav mot KSF3 för att identifiera hur KSF3:s funktionella säkerhetskrav förhåller sig till kraven i KSF2. En *vid tolkning* och en *snäv tolkning* gjordes. Den vida tolkningen innebar att en kravmatchning på rubriknivå medförde att samtliga KSF3-krav inom rubriken ifråga uppfylldes. Ett exempel på en vid tolkning är KSF2-kravet HRSL-4-3 (”Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att spårning av missbruk, och försök till missbruk av IT-systemet kan genomföras”) som mat-

[5] Det är oklart varför övriga säkerhetsmålsättningar saknar referens till KSF-krav.

chades mot kravkategorin SFSL_ANA i KSF3. Den snäva tolkningen innebar att en kravmatchning på rubriknivå inte var tillfredsställande (och därmed förkastades).

Dessa två tolkningar genomfördes för både KSF2 H/S (109 krav) och KSF2 Öppen[6] (50 krav). Totalt 50 (46%) KSF2-krav H/S hade ett eller flera matchande krav i KSF3 med en snäv tolkning och 58 (53%) krav med en vid tolkning. För KSF2 Öppen var samma siffror 28 (56%) givet en snäv tolkning och 32 (64%) givet en vid tolkning. Att cirka hälften av KSF2-kraven för Öppen och H/S hade någon motsvarighet i KSF3 förmedlar att KSF genomgått signifikanta förändringar från version 2 till version 3.

En översikt av resultatet för de olika uppfyllda kraven för KSF2 H/S med en snäv eller vid tolkning ges av Tabell 10.

Med en snäv tolkning matchas 52% av KSF3:s krav på kravnivå Grund, 41% av alla krav på kravnivå Utökad och 37% av alla krav på kravnivå Hög. Detta mönster är intressant då KSF2 på H/S rimligen borde passa in åtminstone lika väl för krav på nivå Utökad och krav på nivå Hög (vilket det trots allt är skapat för) som för krav på nivå Grund. En förklaring är att detaljnivån för krav i KSF3 ökar i samband med kravnivån samtidigt som KSF2 innefattar mer övergripande kravformuleringar som därmed passar bäst in på KSF3-krav på nivå Grund.

Med en vid tolkning matchas 75% av alla krav på nivå Grund, 73% av alla krav på nivå Utökad och 72% av alla krav på nivå Hög. Högst matchning för medelvärdet av kravnivåerna Grund, Utökad och Hög ges för krav rörande säkerhetsloggning (SFSL) som täcks in till 48% (snäv tolkning) och 100% (vid tolkning). Skydd mot obehörig avlyssning (SFOA) och skydd mot röjande signaler (SFRS) täcks inte in alls. Skydd mot skadlig kod (SFSK) matchar näst bäst givet en snäv tolkning (47%), men i jämförelse med de andra kategorierna sällan för vid tolkning (48%). Det finns även stora skillnader på subklassnivå, framförallt då KSF3-kategorierna härdning (SFIS_HRD), skydd av kommunikation (SFIS_INT), krav på unik identitet (SFBK_UID) samt oavvislighet[7] (SFSL_OAV[8]) inte fanns med i KSF2.

[6] Krav på säkerhetsfunktion för IT-system som inte är avsedda för behandling av hemliga uppgifter.
[7] Krav på spårbarhet snarare än sekretess.
[8] Denna subkategori har dock komplett matchning givet en vid tolkning då ett krav i KSF2 H/S ansågs passa in på SFSL_OAV som helhet.

Tabell 10. Matchning av KSF2 H/S mot KSF3. Siffrorna i tabellen förmedlar hur många krav som matchade i relation till antalet krav i varje kategori.

	KSF2 H/S					
	Snäv tolkning			Vid tolkning		
KSF3-kategori	**Grund**	**Utökad**	**Hög**	**Grund**	**Utökad**	**Hög**
SFBK	*11/20*	*12/28*	*13/33*	*13/20*	*18/28*	*20/33*
SFBK_ADM	1/1	2/3	2/5	1/1	2/3	2/5
SFBK_AUT	7/13	7/17	8/19	9/13	13/17	15/19
SFBK_UID	0/2	0/2	0/2	0/2	0/2	0/2
SFBK_ÅTK	3/4	3/6	3/7	3/4	3/6	3/7
SFGK	*2/4*	*2/6*	*2/7*	*3/4*	*4/6*	*5/7*
SFGK_FEL	1/2	1/3	1/4	2/2	3/3	4/4
SFGK_TID	1/2	1/3	1/3	1/2	1/3	1/3
SFID	*7/16*	*7/22*	*7/23*	*16/16*	*22/22*	*23/23*
SFID_ANA	5/8	5/13	5/14	8/8	13/13	14/14
SFID_DAT	2/8	2/9	2/9	8/8	9/9	9/9
SFIS	*4/9*	*8/20*	*7/24*	*6/9*	*13/20*	*14/24*
SFIS_HRD	0/2	0/4	0/7	0/2	0/4	0/7
SFIS_INT	0/1	0/3	0/3	0/1	0/3	0/3
SFIS_KIN	3/4	4/6	3/7	4/4	6/6	7/7
SFIS_KUT	1/2	4/7	4/7	2/2	7/7	7/7
SFOA	*0/2*	*0/3*	*0/3*	*0/2*	*0/3*	*0/3*
SFOA_KBL	0/2	0/3	0/3	0/2	0/3	0/3
SFRS	0/2	0/2	0/2	0/2	0/2	0/2
SFRS_REG	0/2	0/2	0/2	0/2	0/2	0/2
SFSK	*9/15*	*10/19*	*11/21*	*9/15*	*10/19*	*12/21*
SFSK_EXE	6/6	6/6	6/7	6/6	6/6	7/7
SFSK_KIN	1/2	1/4	1/4	1/2	1/4	1/4
SFSK_KUT	1/2	1/2	1/2	1/2	1/2	1/2
SFSK_RIK	0/2	1/3	2/4	0/2	1/3	2/4
SFSK_UPD	1/3	1/4	1/4	1/3	1/4	1/4
SFSL	*10/15*	*12/24*	*12/27*	*15/15*	*24/24*	*27/27*
SFSL_ANA	5/8	5/11	5/11	8/8	11/11	11/11
SFSL_OAV	0/0	0/1	0/3	0/0	1/1	3/3
SFSL_REG	4/4	5/5	5/6	4/4	5/5	6/6
SFSL_SKY	1/3	2/7	2/7	3/3	7/7	7/7
Totalt	**43/83**	**51/124**	**52/140**	**62/83**	**91/124**	**101/140**

En översikt av resultatet för KSF2 Öppen beskrivs i Tabell 11. Då det finns färre krav i KSF2 Öppen än för KSF2 H/S är matchningen mot KSF3 föga förvånande sämre än för KSF2 H/S i allmänhet och mot KSF3-krav på nivåerna Utökad och

Hög i synnerhet oavsett vilken typ av kravtolkning som görs. Det finns dock undantag: exekveringsskydd (SFSK_EXE), systemgemensam tid (SFGK_TID) och oavvislighet (SFSL_OAV) har samma matchning som för KSF2 H/S; kontroll av indata (SFIS_KIN), kontroll av utdata (SFIS_KUT) och analys av säkerhetsloggar (SFSL_ANA) har samma matchning givet en vid tolkning; preservering av säkerhetsloggar (SFSL_SKY) har samma matchning givet en snäv tolkning; autentisering (SFBK_AUT), åtkomstkontroll (SFBK_ÅTK), kontroll av indata för skadlig kod (SFSK_KIN) och kontroll av utdata för skadlig kod (SFSK_KUT) har en bättre matchning för KSF2 Öppen[9].

[9] SFBK_UID, SFIS_HRD och SFIS_INT har ingen motsvarighet i KSF2.

Tabell 11. Matchning av KSF2 öppen mot KSF3. Siffrorna i tabellen förmedlar hur många krav som matchade i relation till antalet krav i varje kategori.

	KSF2 Öppen					
	Snäv tolkning			Vid tolkning		
KSF3-kategori	**Grund**	**Utökad**	**Hög**	**Grund**	**Utökad**	**Hög**
SFBK	*11/20*	*11/28*	*12/33*	*13/20*	*17/28*	*20/33*
SFBK_ADM	0/1	0/3	0/5	0/1	0/3	0/5
SFBK_AUT	8/13	8/17	8/19	10/13	14/17	16/19
SFBK_UID	0/2	0/2	0/2	0/2	0/2	0/2
SFBK_ÅTK	3/4	3/6	4/7	3/4	3/6	4/7
SFGK	*1/4*	*1/6*	*1/7*	*1/4*	*1/6*	*1/7*
SFGK_FEL	0/2	0/3	0/4	0/2	0/3	0/4
SFGK_TID	1/2	1/3	1/3	1/2	1/3	1/3
SFID	*1/16*	*1/22*	*1/23*	*1/16*	*1/22*	*1/23*
SFID_ANA	1/8	1/13	1/14	1/8	1/13	1/14
SFID_DAT	0/8	0/9	0/9	0/8	0/9	0/9
SFIS	*2/9*	*2/20*	*2/24*	*6/9*	*13/20*	*14/24*
SFIS_HRD	0/2	0/4	0/7	0/2	0/4	0/7
SFIS_INT	0/1	0/3	0/3	0/1	0/3	0/3
SFIS_KIN	1/4	1/6	1/7	4/4	6/6	7/7
SFIS_KUT	1/2	1/7	1/7	2/2	7/7	7/7
SFOA	*0/2*	*0/3*	*0/3*	*0/2*	*0/3*	*0/3*
SFOA_KBL	0/2	0/3	0/3	0/2	0/3	0/3
SFRS	*0/2*	*0/2*	*0/2*	*0/2*	*0/2*	*0/2*
SFRS_REG	0/2	0/2	0/2	0/2	0/2	0/2
SFSK	*10/15*	*10/19*	*10/21*	*10/15*	*10/19*	*11/21*
SFSK_EXE	6/6	6/6	6/7	6/6	6/6	7/7
SFSK_KIN	2/2	2/4	2/4	2/2	2/4	2/4
SFSK_KUT	2/2	2/2	2/2	2/2	2/2	2/2
SFSK_RIK	0/2	0/3	0/4	0/2	0/3	0/4
SFSK_UPD	0/3	0/4	0/4	0/3	0/4	0/4
SFSL	*5/15*	*6/24*	*6/27*	*12/15*	*17/24*	*19/27*
SFSL_ANA	1/8	1/11	1/11	8/8	11/11	11/11
SFSL_OAV	0/0	0/1	0/3	0/0	1/1	3/3
SFSL_REG	3/4	3/5	3/6	3/4	3/5	3/6
SFSL_SKY	1/3	2/7	2/7	1/3	2/7	2/7
Totalt	**30/83**	**31/124**	**32/140**	**43/83**	**59/124**	**66/140**

3.4 Diskussion

KSF3 använder två parametrar för att härleda relevanta krav: exponering och konsekvensnivå. Konsekvensnivån bestäms entydigt av den sekretessnivå informationen i systemet har. Det är därför lätt att tro att KSF3 enbart handlar om sekretess och att alla andra IT-säkerhetskrav återstår att identifiera, men så är inte fallet. KSF3 inkluderar flera krav som syftar direkt till att säkerställa informations riktighet samt en större mängd krav som syftar till att ge spårbarhet i systemen.

Analysen av den empiri som funnits tillgänglig för denna studie pekar på att under hälften (43%) av kraven i säkerhetsmålsättningarna svarade mot direkta krav i KSF3. Bland de tillkommande kraven finns krav som syftar till att ge såväl sekretess, riktighet tillgänglighet som spårbarhet. Det finns också krav som inte är direkta IT-säkerhetskrav utan snarare är krav som syftar till att ge användbarhet och interoperabilitet. Mer än en fjärdedel av de tillkommande kraven är allmänna formuleringar på hög nivå som syftar till att ge säkerhet generellt, till exempel genom att skydda mot inbrott. Andelen krav som utgörs av allmänna formuleringar är ännu högre för de krav som motiveras av antagonistiska hot. Av dessa är många krav på så hög nivå att det är svårt att se hur det skulle kunna gå att undvika att uppfylla dem. Ett exempel är ”Förhindra att sekretessklassat materiel kommer obehörig tillhanda.”.

Även om mer än hälften av kraven i de analyserade säkerhetsmålsättningarna inte matchar krav i KSF3 är det svårt att se hur KSF3 ska förändras för att fler av de tillkommande kraven ska kunna identifieras med enkla metoder. Högnivåkrav bedöms som ointressanta att få med i en säkerhetsmålsättning; krav kopplade till användning av vissa specifika produkter (t.ex. andra nationers krypton) är svåra att generalisera och förutse; många av de krav som handlar om användbarhet eller flexibilitet fanns med i KSF2 och är inte längre nödvändiga enligt KSF3; flera krav är designbeslut (t.ex. om systembehörigheter) som är svåra att generalisera. Bland de tillkommande kraven verkar det enklast och mest behövt med modeller för att prediktera tillgänglighetskrav.

Av tillgänglighetskraven syftade två tredjedelar till att skydda mot antagonistiska hot och mer än hälften handlar om skydd av fysiska artefakter såsom byggnader, strömförsörjning och kablar. Kraven handlar främst om kraftförsörjning, robusta kommunikationsalternativ, administrationsmöjligheter och driftövervakning samt skydd mot inbrott eller konventionella vapen. En utökning av KSF3 med krav som täcker in detta tillsammans med parametrar som styr när kraven behöver uppfyllas bedöms vara värdefullt vid framtagande av säkerhetsmålsättningar. Förslagsvis används konsekvensen *avbrottets längd* som huvudsaklig parameter för att identifiera krav att uppfylla. Ett ytterst preliminärt förslag på hur detta skulle kunna parameteriseras presenteras i Tabell 12.

Tabell 12. Tentativt förslag för att identifiera tillgänglighetskrav.

	Stor konsekvens vid avbrott under sekunder	**Stor konsekvens vid avbrott under minuter/timmar**	**Stor konsekvens vid avbrott under timmar/dagar**
Administration och övervakning	God ändringshantering och analys av driftloggar i förebyggande syfte.	24/7-övervakning och möjlighet att administrera direkt.	Detaljerade driftloggar och förebyggande underhåll av fysiska komponenter.
Robust kommunikation	Redundanta kommunikationsmedium, robusta protokoll och skydd mot överbelastning av informationsutbyte.	Alternativa kommunikationslösningar och skydd mot överbelastning av informationsutbyte.	God planering av markarbeten och förmåga att ta fram alternativa kommunikationsmedium.
Kraftförsörjning	Avbrottsfri reservkraft.	Reservkraft (dieselaggregat eller liknande).	Reservkraft (dieselaggregat eller liknande).

4 Att uppfylla KSF3 i praktiken

KSF3 är omfattande och de funktionella säkerhetskraven täcker in en avsevärd del av alla funktionella informationssäkerhetskrav som ställs på IT-system. Syftet med KSF3 är inte att nå en optimal avvägning mellan säkerhet och kostnad utan att uppnå tillräcklig säkerhet till en rimlig kostnad – som det står i KSF3 ska ”tillräckliga skyddsåtgärder föreligga”. KSF3 kommer att behöva realiseras med hjälp av säkerhetskomponenter och med anledning av detta är det intressant att få en bättre förståelse för hur olika KSF3-krav kan realiseras i praktiken. Syftet med detta avsnitt är att ge sådan förståelse genom att föreslå hur kraven i KSF3 kan realiseras med hjälp av vanliga säkerhetskomponenter på enklast möjliga sätt för ett fiktivt system.

Projektgruppen för rapporten har tillsammans identifierat lösningar för de funktionella säkerhetskraven i KSF3. Det fiktiva systemet i fråga är ett fleranvändarsystem med funktioner för att behandla information inom systemet och funktioner för att dela information med andra system. Avsnitt 4.1 redovisar antaganden och 4.2 beskriver metoden för att nå fram till de lösningar som bedöms tillfredsställa kraven. Avsnitt 4.3, 4.4 och 4.5 redovisar vilka säkerhetslösningar som bedöms krävas för att uppnå grundläggande, utökad respektive hög nivå på de funktionella säkerhetskraven.

4.1 Antaganden och avgränsningar

Utgångpunkten för analysen av hur KSF3 kan realiseras i praktiken var ett fiktivt system med följande enkla funktionalitet:

- Systemet ska tillåta flera användare att arbeta och dela information med varandra genom vanliga kontorsapplikationer.
- Systemet ska göra det möjligt att utbyta information/data med andra system genom nätverksuppkoppling.

Utöver detta finns flera faktorer som kan anses relevanta, exempelvis

- vilken informationssäkerhetsklass informationen i systemet har
- om användarna av systemet har rätt att läsa all information i systemet
- vilken informationssäkerhetsklass det andra systemet har ackrediterats för.

Eftersom sådana faktorer påverkar vilken nivå av funktionella säkerhetskrav som krävs lämnades de öppna. Istället identifierades lösningar som projektgruppen tror tillmötesgår alla tre nivåer av funktionella säkerhetskrav som finns i KSF3. I

de få fall där kraven beror direkt på någon av dessa faktorer (som krav på skydd mot röjande signaler) redovisas samtliga möjliga lösningar.

4.2 Metod

En grundtanke i metoden var att kommersiella systemkomponenter och fritt tillgängliga systemkomponenter (t.ex. med öppen källkod) skulle användas i så hög utsträckning som möjligt[10]. Detta då sådana komponenter förmodades kräva mindre resurser att införskaffa och underhålla. Efter en översiktlig genomgång av kravmassan valdes en plattform baserad på Windows som utgångspunkt. Utifrån detta gick projektgruppen tillsammans igenom de funktionella säkerhetskraven och noterade vilka tekniska eller administrativa lösningar som skulle tillmötesgå kraven. Dessa lösningar kunde antingen vara tillämpningar av funktionalitet som redan identifieras (t.ex. att använda Windows inbyggda logghantering), tillföra en ny komponent (t.ex. ett kommersiellt antivirusprogram) eller utföra en manuell åtgärd (t.ex. kopiera filer manuellt). Ett annat metodval var att fokusera på konkreta lösningsförslag. I praktiken realiserades detta genom att (i den mån det var möjligt) föredra tekniska lösningar snarare än administrativa rutiner. I många fall tillgodoser en lösning flera krav i KSF3, ibland inom olika delar av KSF3. När möjliga lösningar hade identifieras gicks de därför igenom för att hitta den enklaste uppsättningen lösningar som tillfredställe respektive nivå. I detta ingick att reda ut eventuella beroenden mellan kraven.

Två forskare utförde oberoende bedömningar av hur varje krav i KSF3 (totalt 148 stycken) kan realiseras i praktiken enligt förutsättningarna beskrivna ovan och systemet beskrivet i Avsnitt 4.1. En workshop med tre av gruppens forskare genomfördes sedan för att nå samstämmighet i bedömningarna, vilket var en huvudsakligen rättfram aktivitet då samstämmigheten var mycket hög. Vid behov konsulterades experter på olika systemkomponenter som projektgruppen inte besatt tillräcklig kunskap kring och i vissa fall tog gruppen hjälp av Försvarsmakten för att tolka KSF3-kraven.

Det finns vissa problem med den metod som använts. Ett av dessa är att terminologin och begreppen i KSF3 inte alltid förstods av projektgruppen. Till exempel behövdes förklaringar av begreppen ”normalisering” (av säkerhetsloggar) och ”säkert tillstånd”, och en precisering behövdes för att förstå omfattningen av kraven relaterade till riktighetskontroll. Projektgruppen skickade en lista med alla sådana oklarheter till en expert på Försvarsmakten med stor insyn i KSF3. Kartläggningsarbetet av de motsvarande KSF3-kraven utfördes när svar (och därmed förståelse) erhållits. Det är dock inte omöjligt att andra krav missförståtts utan att projektgruppen insett det. Utöver detta saknar projektgruppen erfarenhet av

[10] Notera att denna grundtanke ibland står i konflikt med de assuranskrav som också är en del av KSF3, men som denna studie inte har tagit hänsyn till.

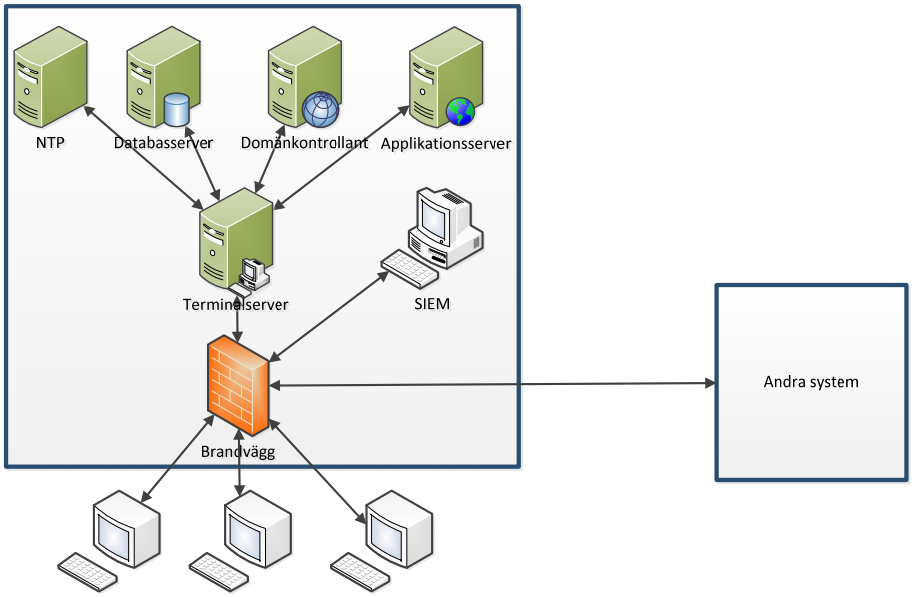
MUST:s bedömningar av lösningars tillräcklighet. Texterna har tolkats efter våra förutsättningar och utan gissningar av vilken tolkning MUST skulle göra. Sist men inte minst har ingen hänsyn tagits till assuranskraven i KSF3 under denna genomgång. Det är fullt möjligt att vissa assuranskrav mer eller mindre omöjliggör att vissa typer av komponenter används på det sätt som de gör i de förslagna lösningarna. Till exempel för att leverantörer inte kan ge den insyn i produkterna som krävs för att klara högre assuransnivåer.

På grund av ovanstående bör läsaren tolka resultatet med försiktighet och se det som ett riktmärke för en generös tolkning snarare än en absolut sanning. Resultatet ska absolut inte förväxlas med ett utlåtande från MUST – detta är enbart projektgruppens tolkning av kraven.

4.3 Uppfyllnad av funktionella säkerhetskrav på grundläggande nivå

De grundläggande funktionella säkerhetskraven i KSF3 är 83 till antalet. En tänkbar lösning som realiserar dessa krav innefattar en Windows-miljö där systemet i fråga exponeras mot vanliga (av MUST godkända) kontorsmaskiner via en terminalserverlösning (Figur 2). Kontorsmaskinerna ansluts till systemet via en switch kopplad till en brandvägg (t.ex. en Färist D200). Brandväggen är konfigurerad att enbart tillåta trafik från kontorsmaskinerna till terminalservern (och t.ex. inte till varandra) och enbart genom de protokoll som krävs för att få fullgod åtkomst till den virtuella maskin som erbjuds av terminalservern. Förutom att säkra upp systemet genom virtuella maskiner med avskalad funktionalitet gör terminalservern det möjligt att sätta tidsbegränsningar på sessioner oavsett om de är aktiva eller ej (vilket SFBK_AUT.3 rör). Behörighetskontroll kan med fördel (men måste inte) ske med hjälp av en domänkontrollant i systemet. På de virtuella maskinerna som användarna kopplar upp sig mot finns, förutom den applikationsprogramvara de behöver, säkerhetsfunktioner erbjudna av ett vanligt antivirusprogam och de inbyggda säkerhetsfunktioner som finns i en modern Windows-maskin. Dessa inbyggda funktioner inkluderar bland annat autentisering, hantering av användarrättigheter, vissa loggverktyg och skydd mot exploatering av svagheter i minneshantering. Utöver detta krävs att kommunikation med andra system genomförs via brandväggen i fråga, och ett antal enklare administrativa procedurer för att hantera uppdateringar och backuper. Ett centralt system för att hantera loggar, ofta kallat *security information and event management* (SIEM) system, behövs för att genomföra korrelationsanalyser av loggar från flera olika säkerhetskomponenter. Det måste nödvändigtvis dock inte köpas in ett fullfjädrat kommersiellt SIEM utan kan lösas med egenskapade skript. Ett alternativ vore att nyttja det SIEM-system som för närvarande håller på att utvecklas av FMTM (inom ramen för Försvarsmaktens centraliserade logghanteringsprojekt).

En mer utförlig beskrivning av hur dessa komponenter kan möta kraven i KSF3 ges under rubrikerna nedan.



Figur 2. Realisering av KSF3:s grundkrav.

4.3.1 Inbyggda Windowsfunktioner

Windows-miljöer kommer med flera säkerhetsfunktioner som kan aktiveras av systemadministratörer och som autentiseringsmekanismer kan skydda mot obehörig förändring. Bland dessa ingår

- hantering av autentisering, konton och behörigheter
- loggning av system och applikationer
- rapportering av installerad programvara
- säkerställande av systemgemensam tid
- integritetskontroller (t.ex. Trusted Platform Module [TPM] och applikationsvitlistning)
- dataexekveringsskydd (t.ex. Data Execution Prevention [DEP] och Adress Space Layout Randomization [ASLR]).

Med en ordentlig konfiguration uppfyller de inbyggda funktionerna i Windows mer en tredjedel av KSF3:s grundkrav. Detta inkluderar så gott som samtliga

krav kopplade till behörighetskontroll (SFBK), kraven på härdning (SFIS_HRD) och delar av kraven för möjliggöra detektion av intrång (SFID_DAT.4-6). I en Windows-miljö kan det även säkerställas att alla klienter använder samma tid som en särskilt utvald NTP-server[11] (SFGK_TID). Denna NTP-server kan exempelvis finnas i en Windows 2012-server. Att ge säkerhetsattribut, såsom lösenord, skydd mot obehörig avläsning och modifikation när dessa lagras eller transporteras i systemet (SFBK_AUT.10) kan ske med hjälp av krypteringsmekanismer såsom Windows inbyggda Encrypting File System (EFS)[12] eller de som finns inbyggda i Microsoft Office-paketet[13].

4.3.2 Terminalserver

Ett antal krav kan bli problematiska att möta om säkerhetsrelevant information finns lagrad lokalt och är möjlig att komma åt utan att centrala funktioner kan säkerställa status på systemet. Det kan till exempel vara svårt att kontrollera tiden för sessioner och säkerställa att information som finns lagrad lokalt på en hårddisk inte flyttas till andra system. En lösning på detta är att låta användare som vill interagera med systemet koppla upp sig mot det via en terminalserver. Terminalservern exponerar virtuella maskiner som användare kan nyttja för interaktion med applikationer i systemet. Med andra ord, den fysiska maskinen som användaren nyttjar fungerar bara som ett skal för att interagera med en av systemets godkända maskiner. Terminalservern bör vara konfigurerad på ett säkerhetsmässigt tillfredsställande sätt. Bland annat bör den inte innehålla mer mjukvara och funktioner än vad som behövs och ingen information ska kunna kopieras mellan den virtuella maskinen användaren är ansluten till och maskinen användaren ansluter från. Med en sådan lösning är det rimligt att anta att ingen säkerhetsrelevant information sparas på den anslutande maskinens sekundärminne (dvs. hårddisk) och att det inte går att arbeta med information i systemet utan att det övervakas av centrala säkerhetsfunktioner.

4.3.3 Antivirus/HIPS

Ett vanligt antivirusprogram eller ett så kallat *Host Intrusion Prevention System* (HIPS) bidrar till att möta krav på att kontrollera indata (SFIS_KIN och SFSK_KIN) och utdata (SFSK_KUT) till systemet samt de krav som handlar om att skydda mot skadlig kod (SFSK_EXE). En normal antiviruslösning kan även spara vad som anses vara säkerhetsrelevanta händelser, göra dessa tillgängliga för analys på det sätt som krävs och tillåter även i viss utsträckning tillägg och

[11] http://support2.microsoft.com/kb/816042
[12] http://windows.microsoft.com/en-us/windows/encrypt-decrypt-folder-file#1TC=windows-7
[13] https://support.office.com/en-au/article/Password-protect-documents-workbooks-and-presentations-ef163677-3195-40ba-885a-d50fa2bb6b68

anpassning av analysen[14] (SFID_ANA, SFSL_ANA och SFSL_REG). Antivirusprogrammen skulle behöva finnas på alla maskiner i systemet.

4.3.4 Brandvägg/NIPS

En modern avancerad brandvägg eller ett så kallat *Network Intrusion Prevention System* (NIPS) kontrollerar nätverkstrafik för särskilda mönster eller egenskaper baserat på header-information (t.ex. MAC, IP och portar) och/eller datapayload (SFIS_KIN och SFSK_KIN, SFSK_UT). Om skadlig kod eller normal trafik matchar regelverket i produkten blockeras trafiken. Likaså är det möjligt att med en modern brandvägg spara loggar från all trafik som flödar genom brandväggen. Nätverksloggar behöver genereras med systemgemensam tid och därför synkas med Windows-miljön. Ett alternativ vore att låta brandväggen själv agera NTP-server och sköta den systemgemensamma tiden, något som exempelvis en Färist D200 klarar. I övrigt skulle brandväggen behöva kontrollera syntaxen på data som flödar igenom och söka igenom data för att identifiera skadlig kod. Detta är typisk standardfunktionalitet i moderna brandväggar och nätverksbaserade intrångspreventionssystem (IPSer)[15]. Ifall information som skickas ut ur systemet behöver vara trafikskyddad löses det förmodligen enklast med någon av Försvarsmaktens godkända lösningar för trafikskydd.

4.3.5 Samlad logghantering (SIEM)

Redan på den grundläggande nivån finns krav att händelsekedjor ska skapas och följas i logganalysverktygen (SFID_ANA.6), sammanföring av flera olika komponenter (SFSL.4) samt möjlighet att söka och sortera på godtyckligt attribut (SFSL_ANA.8). För detta krävs samlad logghantering. En vanlig lösning på sådant är så kallade SIEM-system. Ett SIEM-system sammanför flera olika loggar i en databas för att utföra korrelationsbaserade analyser på loggar. Den bakomliggande tanken är att få bättre lägesbild och minska antalet falsklarm. Falsklarm är vanliga problem för enskilda detektorer såsom antivirus och NIPS och genom att korrelera flera loggkällor mot varandra kan bättre precision uppnås.

Ett enkelt SIEM-system kan skapas genom att föra in flera loggar i en databas med ett enkelt gränssnitt men färdiga lösningar finns att tillgå på marknaden. Försvarsmakten (närmare bestämt FMTM) håller för närvarande på och utvecklar ett SIEM-system för Försvarsmakten med den kommersiella produkten ArcSight som grund. Detta system kan vara en framtida lösning – det enda kravet som

[14] Se till exempel möjligheterna till anpassning i Symantec Endpoint Protection och McAfees produkter.
[15] Det finns till exempel i produkter från Trend Micro, FireEye och Palo Alto Networks.

skulle ställas då är att de relevanta loggarna formateras på ett sätt som SIEM-installationen kräver.

4.3.6 Manuella procedurer

Alla tekniska lösningar behöver kompletteras med olika manuella procedurer av olika omfattningar. De allra flesta av dessa procedurer kan med fördel i mer eller mindre omfattning automatiseras i form av enkla skript.

- Stöd för riktighetskontroller av mjukvarufiler och konfiguration finns ibland, men inte alltid, i vanliga Windows-installationer. Exempelvis finns det inbyggda riktighetskontroller i form av certifikat för utvecklare och uppdatering av vissa mjukvaror såsom Windows, men detta är inte fallet för alla mjukvaror eller säkerhetsuppdateringar. I sådana fall krävs manuellt arbete och specialskräddade verktyg, såsom för att verifiera att en hashsumma för en säkerhetskopia stämmer med den rätta versionens hashsumma.
- Vissa analysmodeller och moduler för normalisering av loggdata finns i SIEM-system såsom ArcSight, men att använda dessa kräver omfattande manuellt arbete för att vara funktionsdugligt. Det krävs också arbete med att exponera alla loggar på ett tillfredsställande sätt till SIEM-systemet.
- Vanlig IT-administration krävs för att installera och drifta IT-miljön på ett funktionsdugligt sätt. Exempelvis krävs det omfattande handpåläggning för att uppfylla kraven kring behandling av säkerhetsloggar på ett tillfredsställande sätt och för att konfigurera både brandvägg och terminalserver.
- Vanliga applikationer som används i system måste (om de inte redan är konfigurerade) konfigureras för att rapportera signifikanta händelser till en behandlingsbar plats såsom maskinloggen i Windows.
- Det finns få säkerhetslösningar som per default kan skapa ett säkert tillstånd om de felar (SFGK_FEL). För detta krävs det därför manuell handpåläggning, såsom en rutin (eller alternativt programkod) för att blockera nyttjande av en virtuell maskin om definitionsfilen för dess antivirus inte är uppdaterad eller liknande.

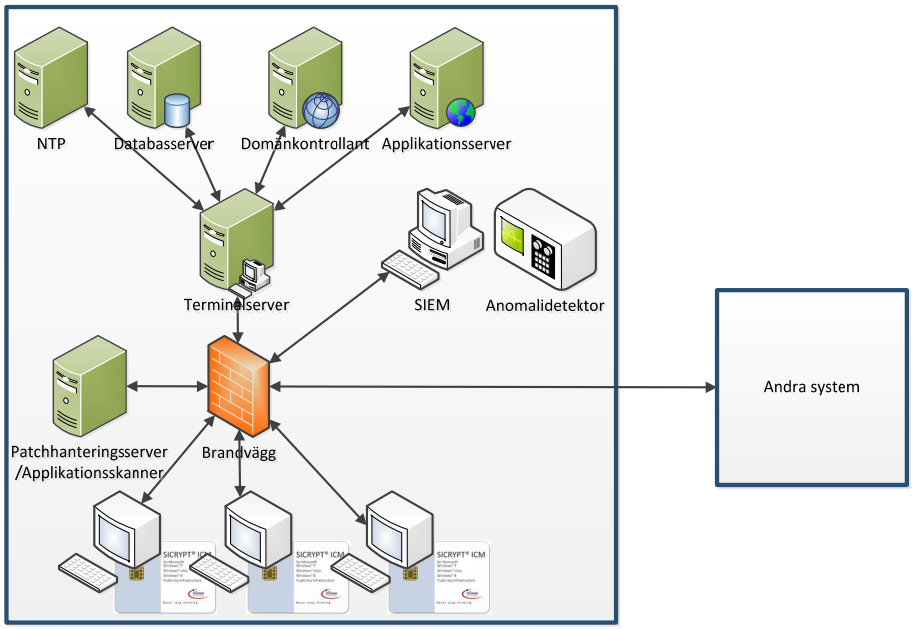
4.4 Uppfyllnad av funktionella säkerhetskrav på utökad nivå

På den utökade nivån finns 124 krav, 41 fler än den grundläggande nivån. Två grundläggande krav (SFID_DAT.8 och SFIS_INT.1) försvinner eftersom de

ersätts av mer krävande formuleringar men i övrigt är alla grundläggande krav kvar. I korthet handlar de 43 nya kraven om

- separation av roller/behörigheter (SFBK_ADM.2-3)
- autentisering och sessionshantering (SFBK_AUT.14-17)
- skyddsmärkning av objekt (SFBK_ÅTK.5-6)
- tidssynkronisering med externa säkerhetstjänster (SFGK_TID.3)
- realtidsanalys av loggar (SFID_ANA.9-13 och SFSL_ANA.10-11) och gemensam analysfunktion för loggar (SFID_DAT.9-10)
- omfattning och hantering av säkerhetsloggar och driftloggar (SFSL_OAV.1, SFSL_REG.5 och SFSL_SKY.4-7)
- bättre härdning av maskiner (SFIS_HRD.3-4)
- procedurer för att verifiera riktigheten på systemet (SFSK_RIK.3 och SFSK_UPD.4)
- starkare autentisering av intern kommunikation (SFIS_INT.2-4)
- mer kontroll och begränsning på informationsutbyte (SFOA_KBL.3, SFSK_KIN.3-4, SFIS_KIN.5-6 och SFIS_KUT.3-7).

I detta avsnitt redovisas hur de 43 nya kraven kan realiseras med lösningen för grundkraven som utgångspunkt. En översikt av lösningsförslagen beskrivs i Figur 3. De huvudsakliga förändringarna jämfört med Figur 2 är att datorerna som nyttjas för att koppla upp sig mot terminalservern numera även måste vara en del av systemet (och uppfylla dess IT-säkerhetskrav), att användare måste nyttja aktiva kort för att logga in, att en anomalidetektor behöver analysera information i systemet, att det finns en dedikerad patchhanteringsserver samt att det finns ett system för märkning av objekt. Om information av sekretess H/C eller H/S ska hanteras av systemet (snarare än bara H/R) krävs också inspektion av kabeldragning (SFOA_KBL.3) och skydd mot röjande signaler (RÖS, SFRS_REG).



Figur 3. Realisering av KSF3:s utökade krav.

4.4.1 Nya krav hanterbara av lösningen för grundkrav

En stor mängd av de utökade kraven tillgodoses redan av systemet som sattes upp för grundkraven. Exempelvis kan särskilda roller skapas i ett Windows Active Directory (AD) eller på en helt vanlig dator som har olika privilegier rörande olika administrationsroller, program, filer och mappar (SFBK_ADM.2 och SFIS_HRD.3). Det går också att låsa ute maskinadministratören (”superuser”, SFBK_ADM.3). Tidssynkronisering med externa säkerhetstjänster (SFGK_TID.3) kan möjliggöras både av en brandvägg (t.ex. Färist D200) eller den inbyggda NTP-servern i en Windows server. SIEM-systemet möjliggör realtidsanalys av loggar (SFID_ANA.9-13 och SFSL_ANA.10) och en gemensam analysfunktion för loggar (SFID_DAT.9-10). En brandvägg/NIPS, såsom en Färist D200, hanterar kontroll och begränsning på informationsutbyten (SFOA_KBL.3, SFSK_KIN.3-4, SFIS_KIN.5-6 och SFIS_KUT.3-7). Terminalservern hanterar de tillkommande kraven på autentisering och sessionshantering (SFBK_AUT.15-17), exempelvis kan sessioner ges en tidsbegränsning. Windowsfunktionerna för behörighetskontroll gör det möjligt att binda förändringar av objekt med skyddsvärde till den utförande användaren (SFSL_OAV.1). Win-

dowssystem stödjer även Kerberos[16], vilket skyddar intern kommunikation i systemet mot otillbörlig manipulation och avlyssning (SFIS_INT.2-4).

4.4.2 Tunna klienter

På grund av att informationssäkerhetsklassad information (H/R – H/S) hanteras av system som kräver KSF3:s utökade krav blir det komplicerat att betrakta maskinerna som används av systemanvändare som externa eftersom det på den utökade nivån tillkommer krav på aktiva kort för autentisering (se Avsnitt 4.4.3). Att de numera är en del av systemet innebär bland annat att de måste vara härdade. Ett sätt att realisera detta är att konfigurera dem som tunna klienter, exempelvis genom Windows Thin PC – en nedlåst variant av Windows 7 som ger den funktionalitet som krävs för att starta en session till terminalservern.

4.4.3 Aktivt kort (TEID)

För att uppfylla SFBK_AUT.14 krävs det att förstärkt inloggning görs med ett av MUST godkänt aktivt kort (också kallat smart kort). Inom Försvarsmakten kallas korten för förstärkt inloggning TEID-kort. I det fiktiva systemet kan de aktiva korten användas för att autentisera användare av de tunna klienterna inom systemet. Den kryptografiska funktionen i de smarta korten ersätter därmed lösenordsinloggningen som används på den grundläggande nivån och kopplas på samma sätt ihop med i systemets domänkontrollant.

4.4.4 Patchhanteringsserver och applikationsskanner

Två relativt krävande krav rörande riktighet tillkommer med KSF3:s utökade kravmassa: SFSK_UPD.4 kräver att systemet automatiskt ska kunna kontrollera att all installerad mjukvara överensstämmer med leverantörens aktuella versioner och SFSK_RIK.3 kräver att riktigheten för alla mjukvaror och relevanta konfigurationer automatiskt ska kunna verifieras. Dessa krav kan naturligtvis lösas genom omfattande rutiner. Men automatisering är att föredra före omfattande rutiner, bland annat för tillförlitligheten. I den föreslagna lösningen används därför ett dedikerat patchhanteringssystem (med funktioner för applikationsskannande), möjligtvis med en tillkommande sårbarhetsscanner[17], för att spåra vilka mjukvaror som finns installerade i systemet och hur dessa motsvarar de versioner som leverantörer erbjuder. Exempel på sådana system är Symantec Patch Management Solution och Secunia CSI.

[16] Ett protokoll som möjliggör sekretess och riktighet för nätverkskommunikation genom symmetriskt krypto.

[17] Ett verktyg för att automatiskt utvärdera alla mjukvarusårbarheter (och därmed även identifiera mjukvaror) i ett nätverk.

4.4.5 Anomalidetektor

Kravet SFSL_ANA.11 kräver att analysverktyget ska kunna detektera avvikelser från identifierade användningsmönster och händelsefrekvenser. Detta kräver att relevanta säkerhetsfunktioner, såsom SIEM-verktyget eller ett nätverksintrångs-detekteringssystem, har möjlighet att analysera anomalier i systemet. Kravet SFID_ANA.12 anger att dessa säkerhetsfunktioner ska baseras på en profil över hur normala mönster ser ut. Systemet kan till exempel tränas med reguljär (icke-skadlig) trafik för att sedan kunna särskilja på sådan trafik och illvillig trafik, såsom skadlig kod. I den föreslagna lösningen läggs denna funktionalitet som en modul i SIEM-systemet. Ett alternativ skulle vara att placera en dedikerad fristående anomalidetektor i systemet. McAfee Network Threat Behavior Analysis är till exempel en sådan fristående lösning som undersöker nätverkstrafik. Men en fristående lösning skulle inte möta kraven på att analyser ska ske på den samlade mängden loggar (SFID.ANA.9).

4.4.6 Märkning av objekt

Stöd för märkning av objekt behöver finnas i de applikationer som ska skapa information i systemet (SFBK_ÅTK.5). Detta kan till exempel göras genom insticksmoduler i ordbehandlare och meddelandesystem. Givet att märkningen sparas som en del av filer säkerställs att endast behöriga användare kan ändra märkningen samtidigt som riktigheten i filen säkerställs. Kravet SFBK_ÅTK.6 om riktighetsskydd av märkning är därmed uppfyllt.

4.4.7 Manuella procedurer

På samma sätt som för de grundläggande kraven krävs det diverse olika manuella procedurer för att komplettera de förordade tekniska lösningarna, i synnerhet:

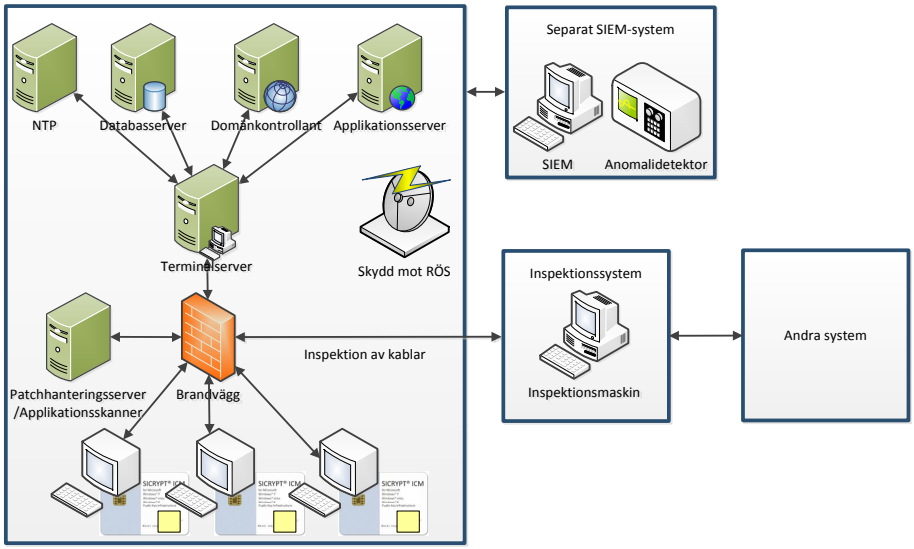
- Onödiga funktioner (dvs., attackyta) bör identifieras och tas bort från systemet (SFIS_HRD.4).
- IT-administration kring hantering av säkerhetsloggar rörande lagring, säkerhetskopiering och rapportering (SFSL_SKY.4-7) samt konfiguration av loggningsverktyg (SFSL_REG.5).
- Det måste finnas en rutin eller ett skript för att upptäcka felande säkerhetsfunktionalitet (vilket behövs för att bedöma om ett definierat säkert tillstånd ska initialiseras, SFGK_FEL.3).

4.5 Uppfyllnad av funktionella säkerhetskrav på hög nivå

På den högsta nivån finns det 140 krav, 16 fler än på den utökade nivån. Sex av de utökade kraven försvinner och 22 tillkommer. Inga nya typer av krav tillkommer, men kraven blir skarpare på flera områden. Skillnaderna jämfört med utökad nivå är främst

- striktare krav på behörighetshantering och separation av roller (SFBK_ADM.4-6)
- starkare autentisering och kontinuerlig behörighetskontroll (SFBK_AUT.18-20 och SFBK_ÅTK.7)
- mer ingående härdning av systemet (SFIS_HRD.5-7)
- ännu mer skydd och kontroll av kommunikation (SFOA_KBL.4, SFIS_INT.5, SFIS_KIN.7-8)
- automatiska kontroller av riktigheten i systemet (SFSK_EXE.7, SFSK_RIK.4, SFSK_UPD.5) istället för manuella
- krav på oavvislighet (SFSL_OAV.2-3, SFSL_REG.6)
- krav på fristående system för logganalys (SFID_ANA.14).

I detta avsnitt redovisas hur de 22 nya kraven kan realiseras med lösningen för utökade krav som utgångspunkt. En översikt av lösningsförslagen beskrivs i Figur 4. De huvudsakliga förändringarna gentemot den tidigare presenterade lösningen är att applikationssandboxar, TAK-kort (istället för TEID), inspektionssystem, samt ett separat SIEM-system behövs.



Figur 4. Realisering av KSF3:s krav på hög nivå.

4.5.1 Nya krav hanterbara av lösningen för utökade krav

På samma sätt som att flera av de utökade kraven hanteras av lösningen för grundkrav uppfylls ett antal krav på hög nivå av lösningen för utökade krav. Rörande behörighetskontroll så kan en Windows Active Directory (AD) åtkomstkontrollera olika roller separat, såsom identitetsadministration och åtkomsträttigheter (SFBK_ADM.5), samt behörighetskontroll och administration av säkerhetslogg (SFBK_ADM.6). Ett vanligt Windowssystem kan också binda förändringar av mjukvarufiler och relevanta konfigurationer som omfattas av riktighetskontroll till de användare som utför förändringarna (SFSL_OAV.2). Terminalservern tillsammans med Windows AD möjliggör avslut av pågående sessioner för subjekt som fått sina konton låsta eller säkerhetsattribut revokerade (SFBK_AUT.19).

Ett vanligt Windowssystem innefattar även diverse funktioner som gör det svårare att nyttja sårbarheter i mjukvara (t.ex. stack cookies, safe SEH, ASLR, DEP, heap spray-försvar och applikationsbrandväggar), vilket tillfredsställer SFIS_HRD.5. Windows-systemet innefattar också en Kerberos-lösning som hjälper till att skydda information vid kommunikation mellan distribuerade komponenter inom systemet mot obehörig åtkomst och manipulation (SFIS_INT.5). Moderna Windows-system erbjuder också vad som kallas Dynamic Access Control som gör det möjligt att definiera regler för åtkomstkontroll baserat på resursers attribut samt File Server Resource Manager som kan begränsa var olika filer får placeras i systemet (t.ex. i vilken mapp). Så vitt projektgruppen vet kan dessa

användas för att möta kraven på att objekts märkning ska styra åtkomst (SFBK_ÅTK.5) givet visst konfigurationsarbete.

Patchhanteringsservern/applikationsskannern innehåller funktioner för att kontrollera att all installerad mjukvara överensstämmer med aktuella versioner från leverantören och att dessa mjukvarufiler uppfyller krav på riktighet (SFSK_UPD.5), samt att verifiering av mjukvarufiler och konfigurationer sker löpande och att endast godkända resultat accepteras för användning (SFSK_RIK.4). Vitlistningsverktyget Applocker och TPM finns förinstallerade i Windows 7 och senare. Dessa uppfyller tillsammans med patchhanteringsservern/applikationsskannern kravet på att endast kod som tillhör systemet och vars riktighet verifierats ska accepteras för exekvering (SFSK_EXE.7).

Systemet för märkning av objekt möjliggör att endast behöriga användare har access till objekt med olika märkningar (SFBK_ÅTK.7). Synkningen mot Windows AD möjliggör även spårbarhet om data exporteras ut från systemet genom att logga all utförsel (SFSL_OAV.3). Detta märkningssystem ska också kunna nyttjas för att märka information som passerar in i systemet (SFIS_KIN.7).

4.5.2 Applikationssandboxar

Ett krav som tillkommer för härdning är att samtliga mjukvarutjänster ska vara isolerade från varandra och det övriga systemet genom upprätthållandet av en restriktiv resursåtkomstpolicy (SFIS_HRD.6). Vi tolkar detta som att en applikation inte ska känna till vilka andra applikationer som finns, inte kunna läsa vad dessa gör, eller kunna skriva till minnesplatser som dessa nyttjar. Ett sätt att lösa detta är att placera applikationer i särskilda sandlådor, ett slags virtuella containrar som enbart exponerar den lilla funktionalitet som applikationen absolut behöver av operativsystemet för att exekvera. Detta kommer per default[18] för Windows 8:s applikationer, men detta är inte fallet för vanliga desktopapplikationer. Ett exempel på en sandboxapplikation som kan realisera denna lösning i Windows-miljöer är Sandboxie[19].

4.5.3 Aktivt kort (TAK)

För att uppfylla SFBK_AUT.18 krävs att stark autentisering med ett av MUST godkänt aktivt kort av typen TAK nyttjas. På samma sätt som för uppfyllnad av utökade IT-säkerhetskrav används TAK-kort i särskilt konfigurerade datorer inom systemet vilka är anslutna mot en terminalserver. TAK-kort i kombination med Windows AD och existerande loggfunktioner löser kravet på att all aktivitet

[18] Gäller alla appar utom Internet Explorer 10.
[19] http://www.sandboxie.com/

som systemet genomför för en användares räkning ska knytas till den genom stark autentisering fastställda identiteten (SFBK_AUT.20).

4.5.4 Separat samlad logghantering (SIEM)

Det tillkommande analyskravet SFID_ANA.14 kräver att analyser ska ske i ett annat system än det övervakade, men att detta kan ligga i en avgränsad del av det skyddade systemet i fråga. I vår lösning ligger denna funktionalitet i ett system direkt knutet till det skyddade systemet. Men om det tidigare diskuterade SIEM-systemet som utvecklas av FMTM kan hantera sekretessbelagd data av tillräckligt hög nivå skulle denna funktionalitet också kunna vara placerad där.

4.5.5 Inspektionssystem

Det tillkommande kravet på kontroll av indata (SFIS_KIN.8) kräver att all information som passerar in till systemet ska verifieras i minsta beståndsdel och att komplexa dataformat måste konverteras till enklare format innan kontroll. I praktiken innebär detta att någon typ av inspektionsstation måste genomsöka all data som passerar in till systemet. Vår lösning realiserar detta genom ett särskilt inspektionssystem som har nätverkskopplingar både till det skyddade systemet och till Försvarsmaktens övriga relevanta system. Om någon typ av datapayload ska skickas in till systemet måste den först skickas till inspektionssystemet. Väl där bryts den ner till ett analyserbart format och genomgår automatiserade tester. När testerna är genomförda och payloaden är godkänd kan den sändas in till systemet. Ett exempel på ett system som kan användas för detta ändamål är FireEyes Multi-Vector Virtual Execution (MVX) engine.

4.5.6 Kabelinspektioner och RÖS

Det tillkommande kravet rörande kabelinspektioner (SFOA_KBL.4) innebär att kommunikation utan godkänt signalskydd ska utgöras av optisk fiberkabel, förläggas inom sektionerat område och vara inspekterbara i hela sin sträckning. Detta hanteras genom inspektioner i vår lösning.

Då information av lägst klass H/C ska behandlas av systemet så tillkommer även kraven på RÖS (SFRS_REG.1-2) i samma eller högre omfattning än för de utökade kraven givet H/C.

4.5.7 Manuella procedurer

På samma sätt som för de utökade kraven krävs det diverse olika manuella procedurer för att komplettera de föredragna tekniska lösningarna, i synnerhet:

- Det behöver skapas skript som låser användarinteraktion om någon utvald säkerhetsfunktion är avstängd eller ur funktion (t.ex. genom att synka användarkonton, egenskaper för antivirus och sessionsrevokering i terminalservern) (SFGK_FEL.4).
- Det krävs manuellt arbete med systemhärdning (SFIS_HRD.7).
- Det krävs manuellt arbete för att definiera vilka systemhändelser som ska loggas (SFSL_REG.6).
- Det krävs även arbete för att möta kravet som säger att det inte ska finnas en ”superuser”-roll eller liknande i systemet som har tillgång till allt i systemet (SFBK_ADM.4). Precis som på utökad nivå kan sådana roller göras otillgängliga för användare. Det går naturligtvis också att dela upp rättigheter på olika sätt – till exempel genom att se till att domänadministratörer inte är administratörer på alla maskiner.

4.6 Diskussion

I Avsnitt 4.3 till 4.5 beskrivs förslag på lösningar för de funktionella säkerhetskrav som KSF3 ställer för system som är på grundnivå, utökad nivå eller hög nivå. I detta avsnitt diskuteras resultatet av den analysen och de implikationer som olika krav i KSF får för vilka lösningar som är godtagbara.

Det konstaterades i Avsnitt 2.1 att den modell som KSF3 bygger på (exponering/konsekvens) är väl i linje med etablerad säkerhetsteori. De funktionella säkerhetskraven i KSF3 är också enkla att förstå bakgrunden till och de allra flesta är i sig okontroversiella och oproblematiska att förstå. Den granulära indelningen av krav är också ett lyft eftersom det minskar antalet krav som består av flera delkrav. Men även om kraven överlag är begripliga finns det behov av exempel och förklaringar i flera delar av KSF3. Till exempel är det inte uppenbart vad ett definierat säkert tillstånd är, eller när en lösning är tillräcklig för att ge oavvislighet.

Som tidigare nämnts ska de lösningar som föreslås i Kapitel 4 på de olika nivåerna inte förväxlas med en officiell beskrivning av hur de bör lösas eller en beskrivning av en tillräcklig lösning. Av personer bättre införstådda än projektgruppen i hur KSF3 ska tolkas och omsättas i praktiken kan vårt förslag antingen ses som ett rimligt och bra förslag på en generell lösning, eller som ett tydligt tecken på svårigheten att utläsa vad kraven egentligen syftar till att uppnå. Det kan noteras att lösningarna hade varit snarlika även om miljön hade baserats på Linux, men då med flera fristående komponenter och mer integrationskod.

Analysen pekar på att de flesta funktionella säkerhetskrav i KSF3 kan lösas med typiska IT-säkerhetsprodukter. Om assuranskraven kan hanteras innebär detta att COTS-produkter i form av mjukvara för antivirus, intrångsdetektion, logganalys

och autentisering med mera kan lösa stora delar av Försvarsmaktens generella IT-säkerhetsbehov. Det finns dock vissa undantag som inte är enkla att realisera med vanliga säkerhetsprodukter och krav som tycks erbjuda oproportionerligt lite säkerhet givet den insats de kräver. Sådana besvärliga krav inkluderar: märkning av objekts känslighet, möjlighet att följa händelsekedjor i loggar, separation av rättigheter, krav på möjlighet att avsluta pågående sessioner och krav på hantering av felsäkert läge.

Det är svårt att som utomstående värdera den riskanalys som ligger till grund för KSF3 och därmed hur rimliga kraven är i förhållande till sin kostnad. Vissa krav på den grundläggande nivån känns dock obalanserade. På grundläggande nivå finns exempelvis krav på analys av flera olika typer av loggar i ett analysverktyg som kan hantera händelsekedjor. Detta tolkades av projektgruppen som att ett avancerat logganalysverktyg behöver vara tillgängligt. Dessutom finns det krav på att pågående sessioner ska kunna avslutas. Den enklaste lösningen som kunde identifieras för att avsluta pågående sessioner var användning av terminalservrar. Även om dessa krav ger bättre säkerhet förefaller det dyrt att kräva sådant för system som hanterar information på lägsta konsekvensnivå. Denna information är sannolikt offentliga handlingar som lämnas ut på begäran. Med det sagt är det tydligt att de tre nivåerna i KSF3 fyller sitt syfte väl och anpassar säkerheten efter risknivån.

Vår rekommendation är att KSF3 kompletteras med ett antal designmönster och produkter som möter krav i KSF3. Även om en sådan katalog inte kan inkludera alla tänkbara lösningar som möter kraven på ett tillfredsställande sätt skulle det med stor sannolikhet hjälpa användare av KSF3. Exempel på vad en katalog kan inkludera är vilket loggformat som är att föredra, analysverktyg som möter kraven i KSF3 samt vilka inbyggda säkerhetsfunktioner som möter de krav som finns på komponentassurans.

5 Slutsatser och rekommendationer

Även om analysen av tillkommande krav baserades på ett begränsat och icke-representativt urval av säkerhetsmålsättningar (fem stycken) är det tydligt att det KSF3 täcker in inte är begränsat till enbart sekretess utan även täcker in merparten av de riktighetskrav och spårbarhetskrav som ställs på IT-system i Försvarsmakten. Eftersom lösningar som ger skydd av sekretess och riktighet (t.ex. skydd mot skadlig kod) också hjälper till att skydda systemens tillgänglighet finns det få IT-säkerhetskrav som explicit fokuserar på skydd av mot antagonistiska händelser som enbart påverkar tillgängligheten. Den största gruppen säkerhetskrav av liknande typ rör skydd av den fysiska miljön och kringliggande infrastruktur (t.ex. elförsörjning). Kraven på den fysiska miljön har också fokus på tillgänglighet. Med anledning av detta rekommenderas att fortsatt arbete med att utöka KSF3 fokuserar på den fysiska miljön för IT-systemet och eventuellt tillgänglighetskrav på IT-systemet.

Författarna av denna rapport anser att kraven i KSF3 är betydligt bättre formulerade än merparten av de tillkommande krav som finns i de analyserade säkerhetsmålsättningarna. Kapitel 4 i denna rapport beskriver ett försök att omsätta kraven i konkreta lösningar och säkerhetskomponenter. Resultaten antyder att det finns en tydlig matchning mellan kraven och de säkerhetslösningar som är vanliga i praktiken och tillgängliga i Försvarsmakten. Om KSF3 skulle kompletteras med sådana realiseringsförslag skulle arbetet med att designa säkra IT-system kunna förenklas betydligt. Mer konkret skulle realiseringsförslagen kunna bestå av kataloger av säkerhetskomponenter som uppfyller funktionella säkerhetskrav, säkerhetskomponenter (t.ex. antivirusmjukvaror) som ackrediteras till olika nivåer, och designmönster (t.ex. terminalservrar) som kan realisera olika krav. En vision skulle kunna vara att skapa ett verktyg där systeminformation och komponenter med kända egenskaper kan beskrivas så att verktyget kan bedöma om vald design möter kraven i KSF3. Framförallt skulle assuranskraven vara enklare att hantera. Därför rekommenderas att en katalog med säkerhetskomponenter relateras till de funktionella kraven och komponentassuranskraven i KSF3 och görs tillgänglig för användare av KSF3.

Referenser

[1] Försvarsmakten, “KSF - Krav på IT-säkerhetsförmågor hos IT-system v3.0,” 2012.

[2] P. Mell, K. Scarfone, and S. Romanosky, “A Complete Guide to the Common Vulnerability Scoring System Version 2.0,” *System*, pp. 1–23, 2007.

[3] Försvarsmakten, “KSF - Krav på IT-säkerhetsförmågor hos IT-system v3.0 Assuranskrav,” 2012.

[4] M. Palviainen, A. Evesti, and E. Ovaska, “The reliability estimation, prediction and measuring of component-based software,” *J. Syst. Softw.*, vol. 84, no. 6, pp. 1054–1070, Jun. 2011.

[5] E. Pinheiro, W.-D. Weber, and L. A. Barroso, “Failure Trends in a Large Disk Drive Population.,” in *FAST*, 2007, vol. 7, pp. 17–23.

[6] G. Soundararajan, V. Prabhakaran, M. Balakrishnan, and T. Wobber, “Extending SSD Lifetimes with Disk-Based Write Caches.,” in *FAST*, 2010, vol. 10, pp. 101–114.

[7] U. Franke, “Optimal IT service availability: Shorter outages, or fewer?,” *Netw. Serv. Manag. IEEE Trans.*, vol. 9, no. 1, pp. 22–33, 2012.

[8] U. Franke, “Analysis of enterprise IT service availability: Enterprise architecture modeling for assessment, prediction, and decision-making,” 2012.

[9] E. Marcus and H. Stern, *Blueprints for high availability*. John Wiley & Sons, 2003.

[10] D. E. Morgan, D. J. Taylor, and G. Custeau, “A Survey of Methods for Improving Computer Network Reliability and Availability,” *Computer (Long. Beach. Calif).*, vol. 10, no. 11, pp. 42–50, Nov. 1977.

[11] M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti, “Control-flow integrity,” in *Proceedings of the 12th ACM conference on Computer and communications security*, 2005, pp. 340–353.

[12] P. Liu, “Architectures for intrusion tolerant database systems,” in *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, 2002, pp. 311–320.

[13] R. Sandhu, “Transaction control expressions for separation of duties,” in *Aerospace Computer Security Applications Conference, 1988., Fourth*, 1988, pp. 282–286.

[14] A. Juels and B. S. Kaliski Jr, “PORs: Proofs of retrievability for large files,” in *Proceedings of the 14th ACM conference on Computer and communications security*, 2007, pp. 584–597.

[15] K. J. Biba, “Integrity Considerations for Secure Computer Systems,” 1975.

[16] D. D. Clark and D. R. Wilson, “A comparison of commercial and military computer security policies,” in *2012 IEEE Symposium on Security and Privacy*, 1987, p. 184.

[17] G. Sivathanu, C. P. Wright, and E. Zadok, “Ensuring data integrity in storage: Techniques and applications,” in *Proceedings of the 2005 ACM workshop on Storage security and survivability*, 2005, pp. 26–36.

[18] J. D’Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings,” *Eur. J. Inf. Syst.*, vol. 20, no. 6, pp. 643–658, 2011.

[19] L. Bilge and T. Dumitras, “Before we knew it: an empirical study of zero-day attacks in the real world,” in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 833–844.

[20] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digit. Investig.*, vol. 7, pp. S64–S73, 2010.

[21] I. Jozwiak, M. Kedziora, and A. Melinska, “Theoretical and practical aspects of encrypted containers detection-digital forensics approach,” in *Dependable Computer Systems*, Springer, 2011, pp. 75–85.

[22] J. Fridrich, “Digital image forensics,” *Signal Process. Mag. IEEE*, vol. 26, no. 2, pp. 26–37, 2009.

Denna rapport beskriver två studier kopplade till version 3 av Försvarsmaktens Krav på Säkerhetsfunktioner (KSF3) – en riskhanteringsmodell och samling av IT-säkerhetskrav som har skapats av Militära underrättelse- och säkerhetstjänsten (MUST). Utöver dessa två studier har projektet även analyserat hur framgångsrik kravhantering mäts i vetenskaplig forskning.

Den första studien analyserade 13 säkerhetsmålsättningar, dokument som skall visa hur IT-system i upphandlingsfasen uppfyller MUST:s IT-säkerhetskrav. Syfte med studien var att identifiera IT-säkerhetskrav som ofta tillkommer till de krav som KSF3 föreskriver. Totalt 672 unika krav kartlades. Av dessa fanns 288 representerade i KSF3, 308 var tillkommande och 76 var för oklara för att kunna klassificeras. De tillkommande kraven var oftast av icke-fysisk karaktär (60% av kraven), hade en antagonist i åtanke (67% av kraven) och rörde tillgänglighet specifikt (15%). Nio kategorier av tillkommande krav identifierades. De vanligaste kategorierna var krav på konfigurationsmöjligheter (34%) och inbrottsskydd (17%). KSF har nyligen uppdaterats från version 2 (KSF2) till version 3 (KSF3), vilket har inneburit signifikanta förändringar rörande dess innehåll sedan de analyserade säkerhetsmålsättningarna skrevs. Vissa av KSF3-kraven var bättre representerade i de analyserade säkerhetsmålsättningarna. Exempelvis var skydd mot skadlig kod bättre representerat av säkerhetsmålsättningarna än behörighetskontroll.

Den andra studien analyserade hur de funktionella säkerhetskraven i KSF3 enklast kan realiseras med hjälp av typiska säkerhetskomponenter i ett fiktivt system med enkel funktionalitet. Forskarna bedömde att KSF3 på grundläggande nivå enklast realiserades med en Windows-baserad lösning innefattande en terminalserver, antivirus, brandvägg och ett verktyg för samlad logghantering. För KSF3:s krav på utökad nivå bedömdes det tillkomma (i huvudsak) TEID-kort, anomalidetektion, en patchhanteringsserver och stöd för märkning av objekt. TAK-kort, applikationssandlådor och mer avancerade inspektionssystem var de huvudsakliga tillkommande funktionerna för KSF3 på hög nivå. Dessutom tillkommer skydd mot röjande signaler och kabelinspektioner (dessa kan dock även vara relevanta för att uppfylla utökade krav).

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
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se