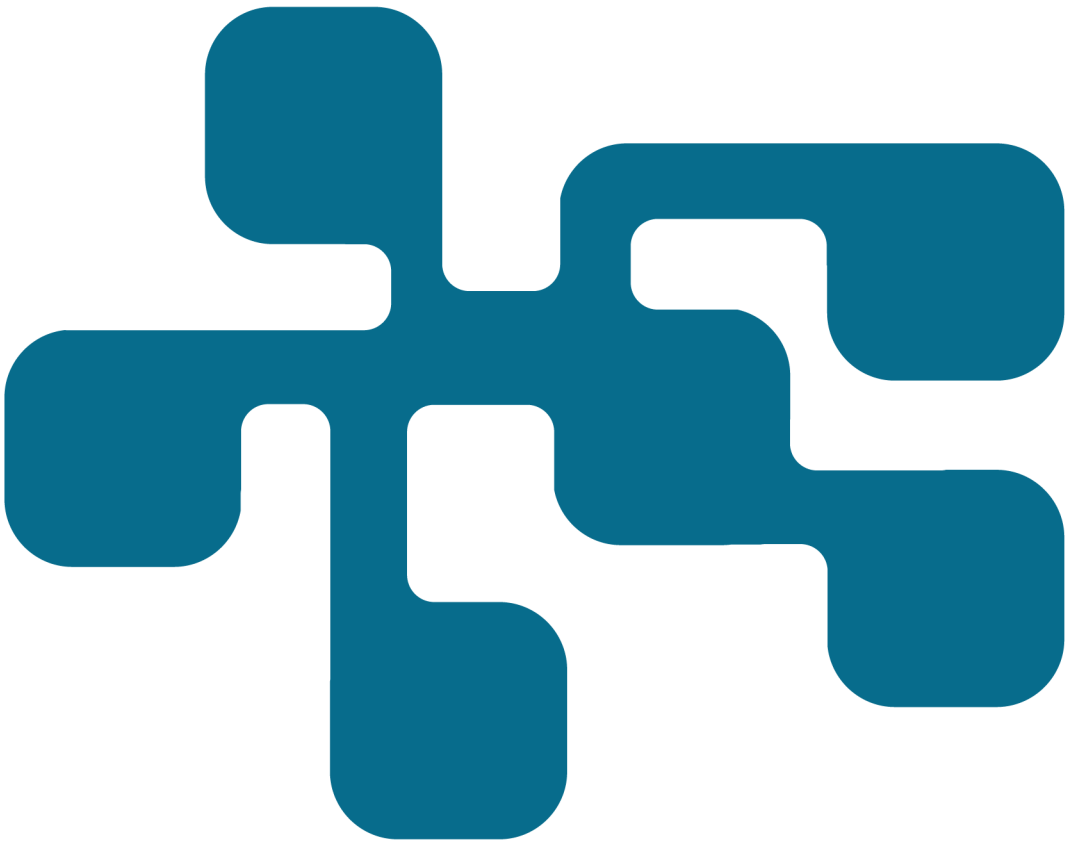
NCS3 - Komponenter på avstånd

Säkerhetsbeaktanden för direkt adresserbara trådlöst nätverks-anslutna komponenter i industriella informations- och styrsystem

Christian Valassi, Martin Karresand

FOI
MSB



FOI-R--4757--SE
MSB 2018-03310
ISSN 1650-1942

April 2019

Christian Valassi, Martin Karresand

Komponenter på avstånd

Säkerhetsbeaktanden för direkt adresserbara trådlöst nätverks-anslutna komponenter i industriella informations- och styrsystem

Titel	Komponenter på avstånd
Title	Security Implications for Wireless Components in ICS
Rapportnr/Report no	FOI-R--4757-SE
Månad/Month	April
Utgivningsår/Year	2019
Antal sidor/Pages	49
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E72353
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Antalet enheter i industriella informations- och styrsystem som ges direkt anslutningsmöjlighet till publika nätverk har ökat explosionsartat de senaste tre åren. Mellan år 2018 och 2020 förväntas en nära fördubbling av antalet enheter till cirka 7,5 miljarder stycken. Utmärkande för dessa enheter är ett fokus på tillförlitlighet snarare än IT-säkerhet, samt begränsade resurser gällande bland annat beräkningskapacitet, minne och batteritid.

Kryptografiska algoritmer är en viktig del i säker kommunikation och används för både kryptering och autentisering av kommunikationen, men adderar också till enhetens arbetsbörda. Det innebär i sin tur att enheten många gånger saknar tillräckligt med resurser för att hantera dessa algoritmer. Funktionalitet för direkt nätverksuppkoppling hos enheter med begränsade resurser kan därför få säkerhetsmässiga konsekvenser eftersom beräkningskapaciteten endast räcker till för att utföra enhetens normala arbetsuppgifter.

Även mer generella aspekter kring säkerhetsrisker i samband med direkt trådlös nätverksanslutning av resursbegränsade enheter är viktiga att belysa. Det blir exempelvis allt vanligare att de kommunikationskretsar som används för att ge anslutningsmöjlighet även innehåller funktionalitet för flera andra kommunikationsprotokoll. Dessa tilläggsprotokoll utgör då potentiella vägar in för en angripare, särskilt i de fall då systemägaren inte känner till att sådan funktionaliteten finns.

Denna rapport beskriver säkerhetsaspekter som bör beaktas för direkt trådlöst nätverksanslutna system innehållande enheter med begränsade resurser. Baserat på de säkerhetsaspekter som beskrivs samt hot och risker som existerar för dessa system, diskuteras ett antal rekommendationer för att erhålla effektiv IT-säkerhet för dessa typer av enheter. Studiens informationsinsamling baseras på en litteraturgenomgång av vedertagna standarder, olika relevanta tekniker för kommunikation, angreppstyper, hot och risker samt skydd mot dessa. Denna informationsinsamling utgör grunden för de rekommendationer och slutsatser som rapporten beskriver. Rapporten innehåller även en ordlista med relevanta IT-säkerhetsbegrepp för direkt trådlöst nätverksanslutna system och resursbegränsade enheter.

Nyckelord: Direkt nätverksanslutna system, resursbegränsade enheter, beräkningssnål kryptering

Summary

The amount of microcontrollers in industrial control systems that are directly connected to public networks has risen dramatically in the last three years. This increase is expected to continue, nearly doubling the amount of units from year 2018 to 2020 to 7.5 billion. Two characteristic properties for such units are their focus on safety rather than security and also their low resources regarding computing power, RAM and battery life.

Cryptographic algorithms are an important part of secure communications because they are used for both encryption and authentication, but they can seldom be applied on units with limited processing power. Networking capability in such units therefore can cause security related consequences, because there is not enough inherent resources for the unit to handle such complicated tasks.

There are also more general aspects of IT security risks related to directly network connected units of limited resources that should be discussed. There is a trend towards integrating different communication protocols into a single component, which for instance allow wireless communication capability. These components therefore become potential attack vectors, especially if the system owner is not aware of the extra functionality and thus cannot act to mitigate it.

This report describes security aspects that should be taken into account when discussing directly wireless network connected systems containing units with limited resources. The report presents a number of recommendations based on security aspects, threats and risks related to these types of systems. The study utilized a literature review as the primary method for data collection pertaining to established standards, relevant communication technologies, and means of attack as well as threats, risks and the defence against these. The collected information constitutes the foundation for recommendations and conclusions made in the study. The report also contains a glossary of IT security concepts relevant to directly wireless network connected systems and resource-limited components.

Keywords: Directly network connected systems, Resource-limited units, Lightweight cryptography

Innehållsförteckning

1. Inledning

Antalet enheter som kopplas upp mot nätverk har ökat dramatiskt de senaste åren och förväntas fortsätta att öka i samma takt även i framtiden. Gartner (2017) förutspår att företagsnyttjande av *Internet-of-Things*-enheter (IoT) kommer öka från cirka 4 miljarder enheter 2018 till 7,5 miljarder år 2020. Dessa IoT-enheter utgör dock bara en delmängd av alla de mikrokontrollenheter som används i företagsverksamheter, vilket exempelvis inkluderar enheter i cyber-fysiska system, *Smart Grids*, fordonsnätverk, sensornätverk och sjukvård (National Institute of Standards and Technology (NIST) 2017).

Denna rapport behandlar direkt trådlöst nätverksanslutna system av resursbegränsade enheter[1]. Termen direkt trådlöst nätverksanslutna system avser i denna rapport enheter (mikrokontrollenheter) och system med trådlös anslutningsmöjlighet som är direkt adresserbara från publika nätverk. Dessa enheter är ofta resursbegränsade gällande beräknings- och lagringsförmåga samt batteritid och används framförallt inom IoT, cyberfysiska system och inbyggda system.

Resursbegränsningen för dessa enheter orsakar en rad olika problem. Till exempel medför det att kryptografiska algoritmer, som utgör grunden i säkra kommunikationsprotokoll, inte kan användas utan att avsevärt försämra kommunikationens bandbredd. I vissa fall kan de resursbegränsade enheternas processorer helt enkelt inte hantera kryptografiska algoritmer och relaterade beräkningar i rimlig tid, vilket innebär att algoritmerna inte kan användas. Problematiken ökar genom det faktum att dessa enheter ofta drivs av batterier, vilket innebär en begränsning i driftstid. Processorintensiva kryptografiska algoritmer och funktioner påverkar driftstiden så mycket att det i många fall inte kan anses vara rimligt eller möjligt att acceptera (Burg, Chattopadhyay & Lam 2018; NIST 2017).

Resursbegränsade enheter används inom många olika verksamhetsområden, allt från industriella processer till kardiovaskulär övervakning i människokroppen. Det innebär att enheterna har möjlighet att övervaka och till viss del styra känsliga processer. Detta motiverar i sin tur att dylika enheter, utöver rigorös kvalitetssäkring, även beläggs med ett adekvat cybersäkerhetsskydd i syfte att minska risken för att en potentiell antagonist kan påverka enheterna.

Vidare konstrueras många multifunktionskretsar (*chipset)* av ekonomiska skäl med flera olika inbyggda kommunikationskanaler som standard. En delmängd

[1] Se Bilaga A Ordlista

av dessa kanaler stängs sedan av beroende på vilket protokoll den köpande organisationen önskar använda. Det kan ge allvarliga konsekvenser för systemens cybersäkerhet om dessa kanaler i själva verket förblir påslagna eller kan återaktiveras.

1.1 Mål och syfte

Totalförsvarets forskningsinstitut (FOI) har inom ramen för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3) fått i uppdrag av *Myndigheten för samhällsskydd och beredskap* (MSB) att belysa de säkerhetsmässiga problem som finns med direkt trådlöst nätverksanslutna industriella informations- och styrsystem i syfte att ge beslutsfattare och kravställare av system en förbättrad förståelse för och möjlighet att kravställa en adekvat säkerhetsnivå för dylika system.

1.2 Avgränsningar

Denna studie avgränsar sig till att beskriva direkt trådlöst nätverksanslutna system i form av enheter med begränsade resurser. Sådana enheter, till skillnad från stationära och bärbara datorer samt servrar, kräver särskild hänsyn relaterat till IT-säkerhet då konventionella säkerhetsmekanismer ofta är för resurskrävande.

Studien tar bara upp typexempel på funktionalitet hos multifunktionskretsar eftersom en fullständig marknadsöversikt skulle bli för omfattande för uppdraget. Likaså ändras ofta kretsarnas specifikationer. Även det faktum att tillverkarna av industriella informations- och styrsystem i många fall kan tänkas köpa in de kretsar som för tillfället erbjuder den efterfrågade funktionaliteten till lägst pris resulterar i ett varierande kretsinnehåll i enheterna. Detta har även spelat in i valet av avgränsning.

Rapporten beskriver endast trådlösa kommunikationsprotokoll eftersom dessa inte går att isolera på samma sätt som trådbunden kommunikation och därmed utgör ett större hot vid direktanslutna system. För att angripa trådbunden kommunikation krävs det att angriparen har fysisk tillgång till nätverket där kommunikationen sker eller till en enhet i det nätverket.

Vidare beskrivs inte alla trådlösa kommunikationsprotokoll som existerar. Istället har ett bekvämlighetsurval gjorts baserat på teknikens nuvarande utbredning samt avsedda användningsområden och utgör därför typexempel. Eftersom de grundläggande principerna för trådlös kommunikation på generell nivå är lika för alla tekniker är de övergripande hoten och riskerna i stort sett lika mellan de tekniker som redovisas i rapporten och de som utelämnats.

Rapporten tar inte heller upp generella IT-säkerhetsprinciper och praxis för härdning av datorsystem. Dessa gäller dock även för industriella informations- och styrsystem samt direkt trådlöst nätverksanslutna system och resursbegränsade enheter och bör alltid beaktas.

1.3 Genomförande

Den genomförda studiens primära datainsamlingsmetod var en litteratur-genomgång av relevanta tekniker för trådlös kommunikation, mikrostyrenheter och IoT såväl som allmänna risker, hot och sårbarheter för dessa, samt hur IT-säkerhet kan erhållas. Teknikerna som inkluderas i rapporten uppskattas vara de mest använda baserat på deras marknadsandelar.

1.4 Läshänvisning

Läsare som är bekanta med trådlösa kommunikationsprotokoll samt hård- och programvara för mikrostyrenheter och enheter med begränsade resurser kan bortse från kapitel 2. Det finns även en ordlista i Bilaga A med förklaringar av vissa relevanta termer.

2 Teknisk bakgrund

Följande avsnitt beskriver relevanta trådlösa tekniker för direkt adresserbara komponenter, i form av kommunikationsprotokoll samt vanligt förekommande hårdvara.

2.1 Trådlös teknik

Detta avsnitt beskriver vanligt förekommande kommunikationsprotokoll för trådlös kommunikation, styrkor och svagheter för dessa samt vad som är viktigt att beakta i användandet av varje protokoll. Tabell 1 listar protokollen med tillhörande frekvensband, överföringshastighet och räckvidd. Det bör noteras att de räckvidder som anges i tabellen är teoretiska, gäller under normal-förhållanden och inte tar hänsyn till antennstorlek eller omgivning. Skillnaderna i räckvidd, påverkas starkt av vilken antennlösning som väljs.

Standard	Frekvens	Överföringshastighet (nedlänk)	Räckvidd
Bluetooth	2,4 GHz	2 Mbit/s	100 m
UMTS 3G	0,9–2,1 MHz	2 Mbit/s	15 km
LTE Cat-0	0,9–3,6 GHz	10 Mbit/s	300 m
LTE Cat-NB1	0,4–1,9 GHz	250 kbit/s	15 km
LTE-A	0,45–2,6 GHz	1 Gbit/s	15 km
IEEE 802.11 a/b/g/n/ac	2,4 eller 5 GHz	11–7000 Mbit/s	30–250 m
Sigfox	0,9 GHz	100 bit/s	30 km

Tabell 1. *Ett urval av vanligt förekommande tekniker för trådlös kommunikation (Burg et al. 2018)*

Av Tabell 1 framgår att området grovt kan delas in i långdistanslösningar och närområdeslösningar. För att trådlöst nå längre än några hundra meter krävs

någon form av mobil telekommunikationsteknik. Övriga protokoll lämpar sig bättre för kommunikation i närområdet, även om exempelvis IEEE 802.11-lösningar kan nå längre än 20 kilometer med riktantenner och förstärkare. En diskussion kring valet av kommunikationsprotokoll återfinns i kapitel 5.

Olika lösningar använder varierande frekvenser baserat på användningsområde. Högre frekvenser når generellt en kortare sträcka än lägre frekvenser. Högre frekvenser har dock generellt sett en högre bandbredd, det vill säga hur mycket data som kan överföras per tidsenhet. Ett frekvensutrymme kan delas in i olika kanaler för att undvika att sändare stör ut varandras kommunikation. Dock finns det ofta ett visst överlapp mellan kanalerna, så risken för störningar bör beaktas.

2.1.1 Mobil telekommunikation

Telekommunikation sker idag primärt genom 3G eller 4G. Föregångaren 2G används fortfarande till viss del, men diskuteras inte i denna studie då tekniken håller på att fasas ut. Studien beskriver inte heller 5G eftersom strukturen för denna teknik inte är fastställd och användandet ännu är mycket begränsad. Den kommande 5G-tekniken tas dock kortfattat upp i kapitel 5.

2.1.1.1 Universal Mobile Telecommunications Service (UMTS) 3G

Universal Mobile Telecommunications Service (UMTS) är en global telekommunikationsstandard som vanligtvis benämns som 3G. Standarden baseras på föregångaren *Global System for Mobile communications* (GSM), eller 2G, och standardiserades år 2001 av *3rd Generation Partnership Project* (3GPP). Den stora skillnaden mellan 3G och dess föregångare är dataöverföringskapaciteten som är cirka 40 gånger högre för 3G. Dessutom ger 3G en högre nivå av inbyggd säkerhet, genom att användarenheter kan autentisera det nätverk mot vilket de ansluter.

2.1.1.2 Long Term Evolution (LTE)

Standarden *Long Term Evolution* (LTE) kan ses som steget efter 3G inom mobil telekommunikation. LTE ska dock inte likställas med 4G, vilket är en delstandard benämnd LTE Advanced (LTE-A). LTE benämns ibland istället som 3.9G. LTE delas upp i 20 *användarkategorier* (*User Equipment*, UE) med olika prestandakrav och hastigheter för att tillgodose olika typer av enheters möjlighet att hantera kommunikation. Den främsta anledningen till dessa kategorier är att basstationer ska veta vilken prestanda och överföringshastighet som kan

hanteras av den mottagande parten i kommunikationen för att således kunna kommunicera med olika typer av enheter på ett korrekt sätt[2].

LTE Advanced (LTE-A)

LTE Advanced (LTE-A), mer känt som 4G, är fjärde generationens telekommunikationsstandard som definieras av 3GPP. Skillnader mellan föregångaren 3G och 4G är förutom dataöverföringshastighet och räckvidd även att 4G är fullständigt IP-baserad istället för IP kombinerat med signalsystem (SS7).

LTE Category-0 (LTE Cat-0)

Ett växande behov av att kunna tillgodose kommunikation för system med lägre prestanda, exempelvis IoT-enheter, har resulterat i en dedikerad LTE-kategori (LTE Category-0). I denna kategori är låg strömförbrukning och lägre prestandakrav centralt snarare än en hög dataöverföringshastighet.

LTE Category-Narrowband 1 (LTE Cat-NB1)

Likt LTE Cat-0 har LTE Category-Narrowband 1 (LTE Cat-NB1) utvecklats med inriktning på låga prestandakrav, men till en ännu lägre nivå. Till skillnad från LTE Cat-0 fokuserar denna kategori på inomhustäckning och har en ytterligare lägre överföringshastighet i syfte att spara energi och öka driftstiden för de batteridrivna enheter som LTE Cat-NB1 riktar sig till.

Jämfört med andra LTE-kategorier har LTE Cat-NB1 en relativt hög fördröjning i kommunikationen (1,6–10 sekunder), vilket innebär att denna kategori inte lämpar sig för system med realtidskrav eller nära-realtidskrav.

2.1.1.3 Access Point Name (APN)

Access Point Name (APN) är ett protokoll som används för att adressera en gateway mellan mobila nätverk så som 3G eller 4G och andra typer av dator-nätverk som exempelvis internet. En APN-inställning på klientsidan utgörs primärt av två attribut: *nätverksidentifierare* och *operatörsidentifierare*. Det första attributet specificerar vilket externt *paketdatanätverk* (PDN) som den *Gateway GPRS Support Node* (GGSN)[3] eller *PDN-Gateway* (PGW)[4] som

[2] Cablefree https://www.cablefree.net/wirelesstechnology/4glte/lte-ue-category-class-definitions/

[3] En televäxel som används inom mobil datakommunikation för 3G nätverk. Kan ses som en IP-router då denna utför all routing mellan klientenheten och IP-baserade nätverk.

[4] Innehåller samma funktionalitet som GGSN men är en senare implementation specificerat för 4G och är bakåtkompatibel mot äldre nätverkstyper (2G/3G).

används är kopplad mot samt det nätverk eller den tjänst som klientenheten vill ansluta till. Operatörsidentifieraren är ett valfritt attribut som definierar operatörens *paketdomän* där supportnoden finns placerad. Dessa attribut används sedan av teleoperatören så att rätt IP-adresser tilldelas enheten, att rätt säkerhetsmetodik används och att enheten ansluter till rätt gateway.

Det finns även möjlighet för organisationer att använda egna privata APN där klientenheter, istället för att ansluta till internet, ansluter direkt till en organisations privata nätverk. En privat APN möjliggör, till en högre grad än utan APN, säker kommunikation eftersom organisationen kan kontrollera vilka enheter som kan ansluta via dess APN till det privata nätverket. Vidare kan en privat APN kompletteras med *VPN* för att skydda kommunikationen mellan klientenheterna och den APN-gateway anslutningen sker mot (Communications-Electronic Security Group 2015).

2.1.2 Bluetooth

Bluetooth är en standard för trådlös kommunikation inom en relativt liten radie (ursprungligen cirka 10 meter) som sedermera utökats till cirka 100 meter för *Class 1*. På senare år har det dock visat sig att maximalavståndet för kommunikation med Bluetooth kan utökas långt över vad som specificeras i standarden med hjälp av signalförstärkare[5].

Bluetooth Low Energy (BLE) är en version av Bluetooth-standarden som innehar en lägre energiförbrukning än huvudstandarden. Detta innebär att enheter med begränsade resurser, bland annat gällande batteritid, kan använda BLE utan att enhetens driftstid avsevärt förkortas.

Bluetooth tillhandahåller både sekretess och autentisering av enheter. Sammankoppling av enheter sker i tre faser med hjälp av en av fyra möjliga autentiseringsmetoder. De fyra autentiseringsmetoderna är: Numerisk jämförelse, Just Works, PIN-kod samt Out of Band (OOB). I Numerisk jämförelse visar båda enheter ett sexsiffrigt numeriskt värde på sina respektive skärmar. Användarens uppgift blir att jämföra de båda värdena för att se att de stämmer överens och sedan bekräfta detta så att enheterna kan börja kommunicera. Just works används i de fall där en eller båda enheter som ska sammankopplas inte har en skärm att presentera information på. Rent tekniskt fungerar autentiseringen på samma sätt som i föregående metod bara att det numeriska värdet sätts till sex nollor. I PIN-kodsalternativet presenteras en

[5] Exempelvis AIRcable http://www.aircable.net/extend.php

numerisk kod på en av enheterna som användaren ska skriva in i den andra enheten. OOB, den fjärde metoden, tillåter användandet av andra kommunikationsprotokoll, exempelvis *Near Field Communication* (NFC), för att hitta och koppla samman enheter. Eftersom NFC verkar på extremt korta avstånd går det bra att använda protokollet för att bedöma rimliga avstånd till enheter som ska upptäckas och sammankopplas (Loveless 2018; Ren 2017).

Sammankoppling av enheter med Bluetooth omfattar, som tidigare nämnts, tre faser. I den första fasen upptäcker de båda enheterna vilken funktionalitet den andra har genom att läsa av varandras *Attribution Protocol*-värden (ATT). Genom dessa värden bestäms bland annat vilken autentiseringsmetod som ska användas. I fas två genereras antingen en kortsiktig nyckel (eng. *Short Term Key* (STK)) eller en långsiktig nyckel (eng. *Long Term Key* (LTK)) beroende på vilka ATT-värden[6] som enheterna använder. STK genereras genom att enheterna kommer överens om en tillfällig nyckel (eng. *Temporary Key* (TK)) tillsammans med ett antal slumpmässiga siffervärden. I fas tre används nyckeln som genererades i fas två för att distribuera resterande nycklar som behövs för att kommunicera mellan enheterna. Om en LTK inte genererades i fast två så genereras den nu i fas tre istället (Loveless 2018).

2.1.3 IEEE 802.11

IEEE 802.11 (802.11) är en samling kommunikationsstandarder som skapats och underhålls av *Institute of Electrical and Electronics Engineers* (IEEE) och specificerar implementation av trådlösa lokala nätverk (WLAN) för datorkommunikation. Protokollen i samlingen är de mest använda datornätverksstandarderna för trådlös kommunikation och är gemensamt kända som *wifi*.

802.11b var den första standarden i samlingen som blev allmänt vedertagen följt av 802.11a, 802.11g, 802.11n och 802.11ac. En del standarder i samlingen specificerar små ändringar för att utöka livslängden av andra existerande standarder och en del som exempelvis 802.11i specificerar stödjande teknik. 802.11i-standarden specificerar säkerhetsprotokollet *Wi-Fi Protected Access* (WPA och WPA2) som används för att säkra kommunikationen i trådlösa nätverk.

[6] STK används för LE *Legacy Pairing* och LTK för LE *Secure Connections*

2.1.4 Sigfox

Sigfox är en patentskyddad teknologi som ägs av ett företag med samma namn. Företaget Sigfox bygger och tillhandahåller kommunikationsinfrastruktur och samarbetar med olika nätverksoperatörer i de länder som har Sigfox-täckning.

En av fördelarna med Sigfox-teknologin är att den är kompatibel med många andra vanligt använda kommunikationstekniker som exempelvis 2/3/4G, wifi och Bluetooth. Andra fördelar inkluderar bland annat låga kostnader och låg energikonsumtion, vilket är särskilt positivt för resursbegränsade enheter som drivs med batteri. Samtidigt är en av nackdelarna att kundorganisationer inte själva äger infrastrukturen och är helt beroende av leverantören för att säkerställa att framtagna krav uppfylls. Kunder kan inte heller optimera kommunikationen eller förbättra täckningen eftersom att nätverkets bandbredd delas med andra Sigfox-kunder. Vidare innebär den låga överföringshastigheten att Sigfox inte är lämpligt för enheter med överföringskrav utöver en daglig avläsning av mindre mätvärden eller överföringsbehov med strikta tidskrav.

2.2 Hårdvara

Den fysiska hårdvara som bygger upp resursbegränsade enheter innefattar allt från simpla integrerande kretsar till chipset med en typisk dators alla komponenter, ett så kallat *System-on-a-Chip* (SoC). Till skillnad från den traditionella moderkortsbaserade arkitekturen för datorer, där alla komponenter är separata och integreras via moderkortet, integrerar ett SoC alla dessa komponenter direkt på chipet. Ofta innehåller en SoC även analoga kopplingsmöjligheter till sensorer och styrkretsar utanför enheten. Dylika anslutningar har minst en digital-till-analog- och analog-till-digitalomvandlare eftersom de måste kunna hantera och bearbeta signaler via de analoga in- och utgångarna. I vissa fall kan en kabel kopplad till en analog-till-digitalomvandlare fungera som en antenn och därmed utgöra en attackvektor genom att det går att skicka signaler direkt in i omvandlaren som får enheten att agera på felaktiga signaler (Zhang 2010; Obaidat, Anpalagan & Woungang 2012).

Ett SoC innehåller ofta flera olika kommunikationstekniker i syfte att kunna möta varierande kundbehov. Eftersom SoC-arkitekturen integrerar alla komponenter i samma chip är det inte kostnadseffektivt att tillverka olika chip för varje kommunikationsteknik. Problematiken som uppstår till följd av detta är att en SoC kan ha ytterligare funktionalitet som en kund inte är medveten om. Detta beror på att leverantören av produkten konfigurerar produkten för olika användningsområden och därmed stänger av funktionalitet som inte används. Avstängningen ska dock inte likställas med att kommunikationskanalen inte

finns, möjligheten finns fortfarande att återaktivera avstängda kommunikationskanaler.

Utökad och okänd funktionalitet är i grunden en kontraktsfråga där kontraktet bör specificera att sådana kommunikationskanaler måste uppges av tillverkare eller leverantör. Kunden bör dessutom, trots försäkran om att oanvända kommunikationsfunktioner är avstängda, agera för att säkra komponenter och kommunikation som om dessa funktioner vore aktiva.

En sökning baserad på ett bekvämlighetsurval visar att flera utrustnings-tillverkare för industriella informations- och styrsystem erbjuder multipla trådlösa tekniker i samma enhet. Dock var det svårt att hitta några tekniska specifikationer av hur dessa tekniker är skyddade. Eftersom sökningen inte är heltäckande och för att varken framhålla eller peka ut någon specifik tillverkare publiceras inte mer detaljerade resultat än vad som presenteras i detta avsnitt. Det vi kan konstatera är att det inte är ovanligt att erbjuda olika trådlösa kommunikationsmöjligheter i samma enhet, men att det talas mindre om säkerhetsutmaningar kring detta. Om de multipla kommunikationsteknikerna härrör från användning av SoC, eller om de är specifikt tillagda har inte gått att utröna.

3 Hot och risker

Informationssäkerhet, det vill säga förmågan att skydda information, beskrivs ofta genom egenskaperna *sekretess*, *riktighet* och *tillgänglighet*. Sekretess avser förmågan att hemlighålla information från obehöriga läsare. Med riktighet avses förmågan att kunna bevara informationen i ursprungligt skick. Tillgänglighet avser förmågan att kunna visa information för en behörig läsare när läsaren efterfrågar informationen. Egenskaperna sekretess, riktighet och tillgänglighet är mer kända under sina engelska benämningar: *confidentiality*, *integrity* och *availability*.

Traditionellt har sekretessbehov ofta dominerat över behov av riktighet och tillgänglighet. Detta har exempelvis inneburit att det är bättre att ett informationssystem stänger av sig om det hamnar i ett osäkert läge, än att riskera att skyddad information röjs. För industriella informations- och styrsystem är processtyrningen, det vill säga den funktionalitet som systemen levererar, det som är kritiskt. Ett avbrott i informationsflödet kan beroende på vilken typ av fysisk process som styrs leda till katastrofala konsekvenser avseende människors hälsa, förstörd utrustning eller ekonomiska förluster för processägaren. Detta innebär att egenskapen tillgänglighet har stor betydelse för industriella informations- och styrsystem. Det är i detta avseende även viktigt att säkerställa varifrån information kommer och att denna inte ändrats under färd, således är även riktighet en viktig säkerhetsaspekt för industriella informations- och styrsystem.

En säkerhetsegenskap som hänger tätt ihop med riktighet är autentisering, som avser förmågan att kontrollera riktighet. Konceptet används främst vid kommunikation där parternas verkliga identitet måste styrkas, det vill säga riktigheten i deras angivna identiteter (inloggningsuppgifter). Autentisering kan dock även avse riktigheten hos den övriga information som skickas (exempelvis mätvärden och styrinstruktioner).

Majoriteten av de problem som existerar för enheter med begränsade resurser beror just på dessa enheters begränsade resurstillgång. Säkerhetsmekanismer designas och optimeras i regel för stationära datorer och servrar vars resurser fortfarande inte är oändliga, men mycket större än för resursbegränsade enheter (NIST 2017). Det finns dock ett antal andra aspekter och problem att beakta som relaterar mer till den kommunikationsteknik och de protokoll som används, exempelvis gällande autentisering och riktighet. Följande avsnitt beskriver bland annat sårbarheter för trådlös kommunikationsteknik, sårbarheter i hårdvara samt administrativa problemställningar.

3.1 Trådlös kommunikation och kommunikationsprotokoll

Trådlös kommunikation är naturligt osäker på grund av att dataöverföring sker med hjälp av radiovågor, vilka inte går att isolera på samma sätt som trådbunden kommunikation. För att angripa trådbunden kommunikation krävs det att angriparen har fysisk tillgång till nätverket eller enheter däri. För trådlös kommunikation krävs det endast att angriparen är inom räckhåll för de radioutsändningar som kommunikationen består av. Räckvidden kan dessutom utökas med exempelvis signalförstärkare och antenner. Detta gäller både för angrepp på sekretess och tillgänglighet, det vill säga avlyssning och störning.

Tidigare sätt att hantera säkerhet inom radiokommunikation har byggt på att tillgången till hårdvara begränsats av kostnad och komplexitet. Denna typ av säkerhetslösning, som bygger på att ett system är dyrt, svårhanterligt eller hemligt är en förlegad princip som ofta benämns *security by obscurity*. Dylika lösningar bör undvikas.

Enligt NIST (2012) är trådlösa nätverk ofta bristfälligt konfigurerade ur säkerhetssynpunkt i syfte att underlätta för användare och administratörer. NIST rekommenderar därför att dessa nätverk krypteras samt att övervakning och skanning av trådlösa nätverk sker regelbundet. Detta för att upptäcka möjliga angrepp och sårbarheter, exempelvis oregelbunden nätverkstrafik, obehöriga accesspunkter eller felkonfigurerade enheter.

Trådlös kommunikation är exponerad för passiva angrepp i form av avlyssning där en angripare helt enkelt lyssnar på kommunikation i nätverket. Denna angreppstyp motiverar kryptering av kommunikationen för att på så sätt motverka att en angripare kan läsa innehållet i kommunikationen trots att den snappas upp. Kryptering av kommunikationen i nätverket ger dock inte ett fullständigt skydd då det enligt NIST (2012) är möjligt att utvinna en betydande mängd information genom att analysera flödet av meddelanden mellan kommunicerande parter. Detta angrepp kallas *trafikanalys* och är passivt, vilket innebär att det sker genom avlyssning och därmed är svårt att upptäcka.

Trådlös kommunikation är särskilt känslig för *denial-of-service* (DoS) eller *störningsangrepp*, vilket även detta beror på att kommunikationen sker med radiovågor. Trådlös kommunikation medför att störningssändare kan placeras inom nätverkets räckvidd för att störa ut kommunikationen. Sådana störsändare kan vara mycket enkelt uppbyggda och billiga att framställa. Störningar i kommunikationen behöver dock inte vara avsiktliga utan kan även uppstå genom att legitima enheter stör ut varandra, exempelvis vid felaktig kanal-tilldelning. Störningsangrepp kan i värsta fall resultera i att kommunikationen till systemet helt slås ut och systemet blir omöjligt att hantera från distans.

Förutom störningsangrepp, finns ett antal andra aktiva angreppstyper mot trådlös kommunikation. En angripare kan exempelvis utföra *återspelningsattacker* vilka innebär att angriparen kopierar ett meddelande mellan två kommunicerande parter och skickar samma meddelande igen till den mottagande parten i kommunikationen. En angripare kan även ansluta sig emellan två kommunicerande parter, läsa eller ändra meddelanden och sedan vidarebefordra dem (Man-in-the-Middle, MitM)., exempelvis med hjälp av.

Angrepp mot trådlösa nätverk underlättas av ett relativt nytt koncept för radiokommunikation, *Mjukvarudefinierad radio* (eng. Software-defined radio, SDR), där signalbehandling och andra uppgifter som tidigare hanterats av hårdvara numera hanteras av mjukvara. Hårdvara för SDR kan köpas för några tusental kronor och kopplas till en standarddator med gratis programvara. Detta innebär att i stort sett vad som helst kan spelas in, spelas upp och framställas vad gäller radiotrafik. Användaren har full kontroll över vågformen, det vill säga det som sänds. I förlängningen innebär detta exempelvis att en användare kan fånga upp radiosändningar, ändra innehållet och sedan skicka dem vidare till den ursprungliga mottagaren.

Varken återspelningsattacker eller MitM-angrepp kan normalt motverkas med kryptering eftersom att angriparen inte behöver veta innebörden av meddelanden för att förändra dessa eller skicka samma meddelande igen. Notera dock att förändring av ett krypterat meddelande i praktiken innebär att det förstörs och blir oläsligt för mottagaren, så till vida inte angriparen har tillgång till krypteringsnyckeln. Teoretiskt sett gäller detta inte för de korta numeriska meddelanden som vanligt förekommer inom industriella informations- och styrsystem. I det fallet kan innehållet mycket väl förändras och fortfarande vara läsligt, men med förändrad innebörd. Beroende på hur krypteringsfunktionen är implementerad kan det dock finnas skydd mot förändring av meddelandet. *Sekvensnumrering* av meddelanden samt *autentisering*[7] kan användas mot dessa typer av angrepp.

En annan typ av MitM-angrepp innebär att angriparen utger sig för att vara en auktoriserad enhet eller användare på nätverket för att på så sätt få tillgång till rättigheter av en betrodd enhet eller användare. NIST (2012) beskriver en angreppstyp som liknar det föregående, där en angripare placerar egna *accesspunkter*[8] i nätverket som konfigureras för att uppträda som betrodda enheter i nätverket. Detta kan ge angriparen en *bakdörr* in i nätverket genom att

[7] Notera att kryptografiska funktioner kan användas för autentisering.

[8] Eng. Rogue access point

kringgå gränsskydd såsom brandväggar. Om andra enheter i sin tur omedvetet ansluter till angriparens accesspunkt, kan angriparen få tillgång till dessa enheter och manipulera dem och deras kommunikation. Det är även möjligt att utföra angrepp genom att tvinga fram användning av en tidigare version av ett kommunikationsprotokoll med fler och kända svagheter.

3.1.1 802.11

I oktober 2017 publicerades beskrivningen av ett allvarligt angrepp mot WPA2, som dittills ansetts vara säkert (Vanhoef 2017). Det allvarliga med angreppet var att det slog mot en grundfunktion i WPA2 kring nyckelutbytet och därmed var i stort sett alla enheter som använde WPA2 sårbara. Senare visade det sig att skadan var störst inom företagssfären och att många enklare hemmanätverk inte var sårbara då de inte använde den speciella nyckelutbytesfunktion som utnyttjades för angreppet.

I januari 2018 annonserades WPA3 som ersättare till nuvarande WPA2. WPA3 kommer att använda 128/192-bitars AES-kryptering som standard, till skillnad från 64/128 i dagens WPA2. Vidare kommer WPA3 även att förändra hanteringen av nyckelutbyten i syfte att ytterligare förbättra säkerheten. Säkerhetsmässigt bör i nuläget WPA2 alltid väljas över WPA eller WEP, då säkerheten i dessa protokoll i jämförelse är bristfällig. Den närmsta framtiden lär visa hur WPA3 förhåller sig till WPA2, exempelvis gällande prestandakrav, eftersom standarden ännu inte används i någon större omfattning. Säkerhetsmässigt är WPA3 teoretiskt bättre än WPA2 då det ger ett starkare skydd mot bland annat *brute force*-angrepp och angrepp mot nyckelutbyten. Den längre nyckellängden är dock negativ för resursbegränsade enheter.

3.1.2 Bluetooth

Det är inte bara 802.11 som har problem med säkerheten. Även Bluetooth har, trots säkerhetsmekanismer för sekretess och autentisering, visat sig vara sårbar för angrepp flertalet gånger under de senaste 15 åren. Den senaste uppsättningen av sårbarheter är en samling som kollektivt kallas *BlueBorne* (Seri & Vishnepolsky 2017).

BlueBorne uppdagades av säkerhetsföretaget Armis (Seri & Vishnepolsky 2017) som i sin beskrivning av sårbarheterna skriver att BlueBorne kan användas som en attackvektor för att till fullo ta kontroll över en enhet. BlueBorne påverkar datorer och mobiltelefoner så väl som IoT-enheter. Sårbarheterna medför att en antagonist kan utföra angrepp mot enheter även om dessa inte är sammanlänkade med antagonistens egen enhet eller inte är satta i upptäckbart läge. Eftersom spridningen av ett sådant angrepp sker trådlöst, direkt mellan enheter,

är det svårt att skydda sig. Dessutom har Bluetooth-processer generellt höga rättigheter i alla operativsystem. Konsekvenserna av ett framgångsrikt angrepp kan därför bli stora för den utsatta parten. Angreppsättet är också attraktivt för antagonister eftersom det kan användas för flertalet olika motiv så som cyberspionage, data stöld, *ransomware* eller skapandet av *botnets.*

En försvårande faktor vad gäller skyddet mot BlueBorne är att existerande säkerhetsmekanismer, såsom brandväggar och ändpunktsskydd, fokuserar på att blockera attacker som sprids via IP-anslutningar och är därför inte designade för att hantera de typer av attacker som BlueBorne utgör. För närvarande är det bästa skyddet mot dylika typer av angrepp att uppdatera alla enheter med Bluetooth-funktionalitet till den senaste versionen av standarden, att införa och strikt följa en policy för inaktivering av Bluetooth där så är möjligt, samt att skanna enheter för Bluetooth-relaterade sårbarheter.

3.1.3 Mobil telekommunikation

Mobil telekommunikation lider också av sårbarheter och privata APN, en av de funktioner som framhålls som säkerhetshöjande, har också brister. Privata APN ska inte betraktas som helt säkra, särskilt för enheter som är placerade i utsatta miljöer där organisationen i fråga inte har fullständig fysisk kontroll över utrustningen. I de flesta fall kommer en klientenhet att ansluta till det nätverk den kan, vilket i sin tur exempelvis innebär att om en antagonist kan byta ut en enhets SIM-kort kan denne få enheten att ansluta till ett nätverk som antagonisten kontrollerar. Antagonisten kan sedan analysera och se all trafik som enheten skapar, vart den försöker ansluta, om portar öppnas, om trafiken krypteras samt information som relaterar till autentisering av enheten för en privat APN (CESG 2015; Munro 2017).

Autentisering mot en APN över ett 3G nätverk använder ett äldre protokoll som lagrar autentiseringsvärdet i en sammanfogad MD5-hashsumma (Message Digest algorithm 5), där klientens lösenord ingår. MD5 har sedan en tid visat sig vara osäker att använda då den har en för låg kollisionsresistens och går att knäcka, särskilt gällande korta och svaga lösenord (Wang et al. 2004). En antagonist kan alltså knäcka hashsumman och stjäla en enhets inloggningsuppgifter och själv använda dessa och enhetens SIM-kort för att på så sätt kompromettera organisationens interna nätverk. Det bör även noteras att fördelarna med en privat APN avsevärt minskar om en enhet samtidigt tillåts ansluta mot publika (trådlösa) nätverk (CESG 2015; Munro 2017).

Ett sätt för organisationer att skydda sig mot ovanstående hot är att nyttja inbäddade SIM-kort (eSIM) då dessa löds fast på enhetens chipset och således är svårare för en antagonist att avlägsna och byta ut utan att skada chipsetet eller SIM-kortet. Vidare bör långa och komplicerade lösenord nyttjas, samt bytas ut

efterhand i syfte att försvåra arbetet tidsmässigt för en antagonist att knäcka dessa. Varje enhet bör även tilldelas separata inloggningsuppgifter för att inte riskera att alla enheter komprometteras om en enhets lösenord knäcks.

Tjänster som kan nås via APN bör vara avskilda från övriga delar av de interna nätverken för att inte riskera att en antagonist får tillgång till hela kontorsnätverket och i synnerhet inte till kontrollnätverket. Det bör antas att vem som helst som har tillgång till ett av organisationens SIM-kort också har tillgång till organisationens privata APN och därifrån agera för att minimera potentiella konsekvenser av denna risk (Munro 2017).

3.2 Hårdvarurelaterade sårbarheter

Följande avsnitt beskriver sårbarheter i hårdvara som kan användas i resursbegränsade enheter.

3.2.1 Dolda kanaler

En dold kanal (eng. *covert channel)* är en form av angrepp som involverar missbruk av mekanismer som inte är designade för kommunikation, men som trots det har förmåga att kommunicera, på ett sätt som inte tillåts av organisationens säkerhetspolicy. Skapandet av dolda kanaler kräver, förutom omfattande programmeringskunskap, även direkt tillgång till systemet som är källan för kommunikationen. Detta innebär i sin tur att dessa kanaler endast kan installeras via skadlig kod, fysisk tillgång eller genom tillgång till administratörsrättigheter. Dolda kanaler behöver inte skapas av en potentiell antagonist utan kan vara ett resultat av felaktigheter eller svagheter i systemets design. De flesta dolda kanaler går att åtgärda i efterhand, men vissa kan utgöra en väsentlig del av systemets funktion och kan således inte tas bort utan att systemet måste designas om (Zander, Armitage & Branch, 2007; Okhravi, Bak & King 2010; NIST 2013).

Angrepp relaterade till dolda kanaler är svåra att hantera eftersom det primära sättet att upptäcka dem är genom att analysera systemets prestanda och resursanvändning, vilket blir allt svårare i takt med att datorer blir allt mer resurseffektiva. Förutom att analysera resursåtgång och prestanda kan dolda kanaler även upptäckas genom att analysera datorns källkod (Zander et al. 2007; NIST 2013).

I industriella informations- och styrsystem kan dolda kanaler finnas i den programkod som körs på olika enheter. Det gäller då främst sådana dolda kanaler som tillkommit av misstag, eller på grund av ändrade kommunikationsmönster eller nya anslutningar som inte var aktuella när koden skrevs. Det är

därför viktigt att göra en genomgång av den aktuella programkodens beteende när en enhets fysiska eller logiska förutsättningar förändras.

3.2.2 Sidokanaler

En sidokanal (eng. *side channel)* uppstår när en legitim kommunikationskanal oavsiktligt avger information. Detta beror ofta på den fysiska implementationen av hårdvaran där kommunikationen färdas snarare än svagheter i tekniken. Den information som via sidokanaler läcker ut kan sedan snappas upp av en potentiell antagonist som från denna kan härleda kryptografiska nycklar eller annan skyddsvärd information.

Det finns flera olika typer av angrepp som alla kategoriseras som sidokanals-attacker. Det ska dock noteras att majoriteten av dessa angrepp kräver fysisk tillgång till den enhet som angrips.

Timing attacks är en form av sidokanalsangrepp där en angripare analyserar den tid det tar för enheten att beräkna kryptografiska algoritmer. Detta är möjligt eftersom tiden det tar för en dator att genomföra logiska operationer kan variera beroende på inmatning. Genom att mäta den tid det tar att genomföra en operation kan en angripare rekonstruera den inmatning och de nycklar som använts av den kryptografiska algoritmen. Ett relativt effektivt skydd mot dylika angrepp är att implementera *tidsbeständiga operationer*[9] där alla operationer tar lika lång tid att genomföra, vilket effektivt omöjliggör timing attacks. En följdeffekt är dock att en fördröjning introduceras i beräkningen av de kryptografiska algoritmer som används (Genkin, Shamir & Tromer 2014; Adomnicai et al. 2016).

En annan typ av sidokanalsattack baseras på elektromagnetisk strålning som enheter ger ifrån sig. Varje operation som utförs av en dator avger elektro-magnetisk strålning, på olika frekvenser beroende på vilken operation som utförs. För dessa angrepp intresserar sig angriparen endast för de frekvenser som associeras med kryptering och ignorerar övriga frekvenser.

Principiellt finns det två typer av angrepp som baseras på elektromagnetisk strålning: *Simpel Elektromagnetisk Analys (SEMA)* och *Differentiell Elektromagnetisk Analys (DEMA).* I SEMA-angrepp kan angriparen härleda kryptografiska nycklar direkt från de elektromagnetiska spår som avges. Dessa

[9] Eng. Constant-time operations

angrepp är speciellt effektiva mot asymmetriska kryptografiska implementationer, men kräver att angriparen har ingående kunskap om den kryptografiska algoritm som används, samt implementationen av denna.

I de fall där SEMA inte genererar tillräckligt med information eller inte kan genomföras är istället DEMA ett alternativ. DEMA är mer komplex att genomföra, men är effektiv mot symmetriska kryptografiska implementationer och kräver inte lika ingående kunskap om algoritmen eller implementationen av denna. För att skydda sig mot dylika typer av angrepp finns primärt två motåtgärder varav den första är fysiska motmedel där den elektromagnetiska strålning som avges reduceras eller maskeras för att försvåra upptäckandet av densamma. Exempelvis kan en *Faraday-bur* användas för att minska avgiven strålning, alternativt kan meningslöst ”brus” adderas till signalen för att maskera denna. Den andra typen av motåtgärd görs vid implementationen av den kryptografiska algoritmen, exempelvis genom att nyttja processavbrott eller slumpmässig *klockcykel* hos processorn (Koeune & Standaert 2005; Adomnicai et al. 2016; Martinasek, Zeman & Trasy 2012).

Vid en första anblick kan hotet från sidokanaler verka irrelevant för industriella informations- och styrsystem, men beroende på hur den elektromagnetiska miljön i övrigt ser ut runt omkring enheterna kan det mycket väl gå att utföra angreppen på distans. De relativt långsamma processorerna som enheterna har, tillsammans med de förhållandevis repetitiva uppgifter som utförs gör det enklare att detektera signaler. Även oskyddade ledningar som är åtkomliga från utsidan kan avge strålning (fungera som en antenn) och användas för att angripa utrustning på insidan. Ett korrekt skalskydd är därför av vikt och måste upprätthållas vid nyinstallation för att skydda både enheter och ledningar däremellan. Likaså bör den elektromagnetiska miljön beaktas vid högriskinstallationer.

3.2.3 Okänd funktionalitet

Som tidigare beskrivits i avsnitt 2.2 tillverkas många chipsets med flera inbyggda kommunikationskanaler som av tillverkaren, leverantören eller den köpande organisationen stängs av beroende på vilken kommunikationskanal som enheten ska använda. Om ett chipsets alternativa kommunikationskanaler inte är avstängda på ett korrekt sätt eller av någon anledning slås på, kan detta resultera i informationsläckage eller innebära att enheten i fråga blir ett fotfäste i nätverket för en potentiell antagonist.

En kanal kan även medvetet lämnas påslagen utan att kunden informeras. Den främsta anledningen till att göra detta är att leverantören vill ha en alternativ väg in för att kunna erbjuda mer omfattande service och underhåll på distans. I det

fallet bygger säkerheten mycket på att kanalen hålls hemlig vilket, som bekant, är en förlegad princip.

3.3 Administrativa problemställningar

Följande två avsnitt beskriver problematik med övergången från IPv4 till IPv6 samt allmänna problem kring implementation och kvalitetssäkring av mjukvara.

3.3.1 Övergång till IPv6

Även om den standard för kommunikation över internet (IPv6) som ska ersätta den nuvarande standarden (IPv4) inte är specifikt inriktad på trådlös kommunikation är den värd att omnämnas. IPv6 i sig har inte några svagheter som inte redan finns i IPv4, men det radikalt annorlunda sätt som IPv6 är tänkt att fungera på medför att det krävs ett nytt tankesätt kring säkerhet i system. I och med att IPv4 har för liten adressrymd har olika lösningar för att dölja bakomliggande nätverk tagits fram, till exempel *Network Address Translation* (NAT). Den är inte tänkt att vara en säkerhetsfunktion, men ger i praktiken ett visst skydd för de bakomliggande enheterna genom att de inte går att nå utifrån mer än via en specifik punkt (till exempel en brandvägg). I IPv6 är adressrymden mycket större, vilket medför att varje enhet kan få en egen globalt unik adress och därmed bli direkt adresserbar från hela internet. Detta är också meningen med IPv6, men om ett byte till IPv6 sker utan en ordentlig konsekvensanalys och dessutom i kombination med trådlös teknik (nyinstallerad eller befintlig) uppstår lätt säkerhetsluckor (Karresand 2017). Framförallt beror detta på att enheten får en adress som gör den unikt adresserbar från hela internet och i kombination med radiovågornas spridning blir det enklare att få åtkomst till enheten.

3.3.2 Implementation och kvalitetssäkring

Enligt Kaspersky (2014) var så mycket som 23 % av alla incidenter i industriella informations- och styrsystem ett resultat av mjukvarufel. Många typer av implementationsfel beror på låg kodkvalitet. Specifikt innebär detta att koden i fråga exempelvis innehåller buggar samt osäkra och onödiga funktioner. För att undvika dessa fel är det därför nödvändigt att arbeta med ett mål om kvalitetssäkring snarare än ett mål om leveranshastighet. Praktiskt innebär detta att noga testa all kod, åtgärda buggar, testa igen, åtgärda nya buggar och så vidare tills programmet är funktionellt korrekt (Ferguson, Schneier & Kohno, 2011).

Det är även viktigt att inse att ett funktionellt korrekt program inte nödvändigtvis är ett säkert program. Program tenderar att vara komplexa vilket kan

medföra oförutsedda egenskaper. Dessa egenskaper kan vara väldigt svåra att upptäcka vid tester av programvaran. Ett säkert program bör därför inte innehålla fler funktioner än de som är absolut nödvändiga för programmets syfte (Ferguson, Schneier & Kohno 2011; Saltzer & Shroeder 1975).

Gällande resursbegränsade enheter finns det eventuellt adderad problematik i den begränsade minnesrymd och beräkningskapacitet som dessa enheter innehar. Detta kan i sin tur innebära att skrivningen av programkod måste optimeras för att kunna exekveras på enheten. Resultatet av detta kan bli att säkerhetsfunktionalitet måste begränsas ytterligare.

Det finns flertalet metoder och arbetssätt för att kvalitetssäkra och säkerställa programvara. I praktiken finns det dock inga garantier då ett litet fel i kod eller implementation kan påverka säkerheten i en individuell enhet som i sin tur kan få konsekvenser för hela systemets säkerhet.

4 Säkerhet och hantering av risker

De säkerhetshot som beskrivits i föregående kapitel kan till viss del hanteras, vilket minskar riskerna. I detta kapitel beskrivs säkerhetstillämpning för de kommunikationsprotokoll som tas upp i avsnitt 2.1, samt specifika beaktanden för enheter med begränsade resurser.

4.1 Standarder

NIST beskriver i *Report on Lightweight Cryptography* (2017) ett delområde av kryptografiska funktioner, på svenska översatt till *beräkningssnål kryptografi*. Detta delområde specificerar användningen av kryptografiska funktioner för enheter med begränsade resurser.

Många kryptografiska standarder och funktioner har designats och optimerats för stationära och bärbara datorer samt servrar, vilket medför att dessa inte enkelt kan appliceras på enheter med mer begränsade resurser. Grundtanken med beräkningssnål kryptering är att använda existerande algoritmer och funktioner, men i mer effektiva och enkla format. Det innebär exempelvis kortare nyckellängder eller mindre blockstorlekar i syfte att öka effektiviteten och minska kostnaden för att använda dessa funktioner utan att nämnvärt försämra den erhållna säkerheten.

International Electrotechnical Commission (IEC) har fastställt en serie standarder under namnet *IEC 62443 Security for Industrial Automation and Control Systems* (ISA u.å). Standardserien beskriver bland annat ett antal säkerhetsmålsättningar, krav och motmedel som kan användas inom industriella informations- och styrsystem. IEC 62443 är snarlik ISO 27000-serien (Swedish Standards Institute (SIS) u.å.) genom att de båda är ett stöd vid kravställning och riskbedömning, men IEC 62443 ställer inga specifika krav på använd teknik exempelvis i form av vilka algoritmer som bör användas. Standarden beskriver istället ett antal principiella, välkända, säkerhetsmekanismer samt hur beslutsfattare och säkerhetsansvariga bör resonera kring dessa i relation till de hot och sårbarheter som identifieras. Identifikation sker genom utförandet av risk- och sårbarhetsanalyser (RSA), vilka finns beskrivna i standarden. Standardserien tar upp ett antal punkter som är relevanta för direkt trådlöst nätverksanslutna system. Dessa beskrivs som ett antal säkerhetsåtgärder i form av krav, exempelvis nätverkssegmentering i syfte att reducera exponering för organisationens nätverk genom att begränsa möjligheten för en angripare att röra sig från särskilt exponerade enheter i nätverket till mer skyddsvärda delar av nätverket. I standarden uttrycks även vikten av att isolera kritiska systemdelar från andra, mindre skyddsvärda resurser. Vidare beskriver standardserien

nödvändigheten av flerfaktorautentiseringsfunktioner för alla nätverksbaserade operationer som involverar en mänsklig användare. För mjuk- och hårdvaru-autentisering beskrivs krav på funktion hos systemet för att identifiera och autentisera alla enheter och mjukvarukomponenter som agerar i kontroll-nätverket samt att principen om *minsta möjliga behörighet*[10] strikt tillämpas. Utöver den uppsjö av krav som standardserien innehåller, beskrivs även hur utförandet av effektiv RSA kan uppnås. Beskrivningen avhandlar vanliga orsaker till svagheter i nätverk, där trådlösa accesspunkter nämns som en vanlig källa till problem, speciellt de accesspunkter som nyttjar kommunikationsteknik med låg eller icke-existerande inbyggd säkerhet.

IEC har även, tillsammans med *International Organization for Standardization* (ISO), tagit fram en standard för beräkningssnåla kryptografiska funktioner (ISO/IEC 29192–1: 2012). Standarden beskriver olika kategorier av begränsningar relaterade till kryptering, begränsningar som ofta återfinns hos enheter med begränsade resurser. Standarden nämner bland annat energiförbrukning, kommunikationsbandbredd och storlek på minne som exempel på begränsande faktorer. För att en kryptografisk mekanism ska accepteras som beräkningssnål kräver standarden att mekanismen är skräddarsydd för att hantera en kombination av begränsningar (SIS 2012).

Vidare beskriver standarden ett antal krav som ställs på beräkningssnåla kryptografiska funktioner för att erhålla en minsta accepterade säkerhetsnivå. Standarden specificerar att minsta accepterade nyckelstorlek är 80-bitar och anger även att både symmetriska och asymmetriska mekanismer kan användas. Det nämns även att resistens mot sidokanalsangrepp kan vara relevant för vissa applikationer av beräkningssnål kryptering och att medel för att minska risken för sådana angrepp varierar beroende på applikation. Samtidigt anges att sådana krav ligger utanför standardens omfattning (SIS 2012).

ISO/IEC 29192–1: 2012 beskriver ett antal fysiska och logiska implementationskrav för beräkningssnåla kryptografiska mekanismer. De fysiska egenskaperna som bedöms inkluderar den fysiska storleken av den kryptografiska modulen och modulens energiförbrukning. Jämförelse och fastställande av energiförbrukning kan dock vara svårt eftersom det finns ett beroende till andra fysiska egenskaper som exempelvis chipsetstorlek. För att användare ska kunna fatta välinformerade beslut kräver standarden att leverantörer för dessa chipset eller moduler utförligt dokumenterar testerna för mätning av energikonsumtion. Standarden kräver bland annat att chipstorlek,

[10] Eng Principle of Least Privilege (Saltzer & Schroeder 1975).

cykler, bitar per cykel, energi och energi per bit specificeras för att användare ska ges möjlighet välja den mekanism som är bäst lämpad för deras behov. Liknande krav ställs på mjukvaruimplementationer av beräkningssnåla kryptografiska algoritmer. Krav på bland annat att programkodstorlek, minnesstorlek och exekveringshastighet specificeras för användaren. Standarden beskriver även ett antal åtråvärda attribut för beräkningssnåla mekanismer som bland annat inkluderar fördröjning i kommunikation, vilket är särskilt relevant för industriella informations- och styrsystem, samt prestandan för mekanismen gällande hantering av korta indatavärden (SIS 2012).

4.2 Säker kommunikation

Graden av skydd som bör appliceras på information varierar beroende på skyddsvärdet i kommunikationens innehåll. Exempelvis är det för smarta elmätare inte centralt att kryptera kommunikationen på samma sätt som det är viktigt att se till att elmätaren och information som denna skickar autentiseras av det centrala systemet. Det vill säga att det viktiga är att se till at den information som skickas inte ändras under färd samt att identiteten hos avsändaren verifieras. Detta stämmer för många verksamhetsområden där IoT och andra enheter med begränsade resurser används, framförallt inom industriella informations- och styrsystem.

Frågan om adekvat skydd av information är i första hand en policyfråga där skyddsvärdet i kommunikationens innehåll måste beaktas. I de fall där särskilt skyddsvärd information kommuniceras är kryptering ofta det bästa alternativet att tillgå.

4.2.1 Kryptering

Kryptering kan appliceras på praktiskt taget alla kommunikationsprotokoll, antingen genom att möjligheten redan finns inkluderad i protokollet, eller att den läggs som ett lager ovanpå det ursprungliga protokollet, exempelvis med *Internet Protocol Security* (IPsec). Kryptering kommer dock att introducera en fördröjning i kommunikationen, vilket för vissa system helt enkelt inte är acceptabelt. I andra fall, vilket är extra relevant för enheter med begränsade resurser, finns det inte tillräckligt med beräkningskapacitet i den inbyggda processorn för att kunna exekvera komplicerade kryptografiska algoritmer med rimlig fördröjning. Ett annat problem för resursbegränsade enheter är att kryptografiska funktioner även påverkar batteritiden och förkortar således enhetens driftstid eftersom de beräkningar som utförs konsumerar ström. För resursbegränsade enheter, exempelvis batteridrivna, finns beräkningssnåla kryptografiska funktioner att tillgå (se avsnitt 4.1). Ett annat alternativ kan vara

att undersöka om den skyddsvärda informationen kan färdas via ett annat kommunikationsmedium eller från en annan enhet med större resurser.

4.2.2 Autentisering

Det är sällan önskvärt att kryptera kommunikation i interna nätverk eftersom detta påverkar möjlighet till övervakning av kommunikationen, vilket är viktigt i industriella informations- och styrsystem. I dessa nätverk är det istället viktigare att autentisera enheter och upprätthålla riktighet för meddelanden som skickas. Kryptografiska hashfunktioner utgör grunden i både digitala signaturer och *Message Authentication Codes* (MAC), som båda är användbara inom industriella informations- och styrsystem gällande autentisering och riktighet. Flertalet vanligen använda hashfunktioner har visat sig ha låg kollisionsresistens och bör därför inte längre användas (exempelvis MD5 och SHA-1), istället rekommenderas bland annat SHA-2 och SHA-3 (NIST 2015).

4.2.3 Nätverkssegmentering

Det har redan tidigare i avsnitt 4.2 resonerats om att det inte alltid är informationen i kommunikationen som är viktigast att skydda. I vissa fall är det viktigare att skydda andra delar av nätverket mot korrupta enheter som kan använda sig av legitima kommunikationsmedel för att sprida skadlig kod eller ta över andra mer kritiska enheter i nätverket.

Enheter med begränsade resurser är särskilt utsatta för att bli startpunkter för en angripare i ett nätverk. Detta eftersom sådana enheter ofta befinner sig i anslutning till nätverkets yttre gräns och dessutom ofta är fysiskt utlokaliserade på platser där det är svårt för den ägande organisationen att implementera effektiv fysisk åtkomstkontroll. Dessa enheter är även utsatta eftersom deras inneboende resurser är begränsade vilket innebär att sedvanliga skyddsmekanismer eventuellt inte kan användas, vilket gör dem mer sårbara för angrepp än andra enheter.

Ett skydd för att undvika problematik med propagerande angrepp är att segmentera nätverk. I praktiken innebär segmentering att nätverket delas upp i olika delar eller *zoner* av varierande antal, men där en av zonerna alltid utgörs av de enheter som är kritiska för verksamhetens uppgift. Denna zon innehåller rigorösa säkerhetsfunktioner, speciellt vad gäller kommunikation med enheter utanför zonen, och kan även helt isoleras från andra delar av nätverket i syfte att upprätthålla kritisk funktionalitet även under pågående störningar eller angrepp. I praktiken begränsar nätverkssegmentering en antagonists möjligheter att logiskt röra sig från lättåtkomliga enheter till nätverkets kritiska komponenter. I trådlösa sammanhang kan segmenteringen implementeras genom avgränsningar

i bland annat använda kanaler (frekvenser), nätverksnamn (SSID) och begränsning av utsändningsvinklar med hjälp av riktantenner.

5 Diskussion

En organisation bör i regel basera säkerhetsrelaterade beslut, exempelvis policyer och krav, på vedertagna säkerhetsstandarder. I ett system som inte är tydligt avgränsat från omvärlden, varken fysiskt eller logiskt, blir säkerhetsrelaterade problem dock snabbt komplexa att lösa. Ett exempel på denna komplexitet kan vara en enhet som anslutits till ett internt system från en plats utanför systemets fysiska lokaler. Logiskt befinner sig den behöriga enheten i systemet, men fysiskt utanför, vilket medför att det fysiska skyddet som normalt ingår i helheten inte är applicerbart. De standarder som diskuterades i avsnitt 4.1 utgör en grund för att fatta säkerhetsrelaterade beslut i dylika situationer, men är författade på en relativt hög abstraktionsnivå. Detta gör att de kan behöva kompletteras, exempelvis i situationer som kräver nyttjandet av en specifik säkerhetsmekanism så som en viss krypteringsalgoritm.

En av de generellt sett viktigaste aspekterna i beslutsprocessen för en upphandling eller ett inköp är kravställningen av den produkt eller tjänst som ska tillhandahållas, så även gällande trådlös kommunikation. FRA (2017) beskriver att nyttjande av extern kompentens för att hantera kravställning, implementation och drift är vanligt förekommande då organisationer i regel önskar att minimera storleken av den egna IT-avdelningen för att istället upphandla många av dess funktioner. Resultatet blir ofta en intern kompetensförlust, inte minst säkerhetsmässigt. Organisationer bör istället sträva efter att internt behålla nyckelpersonal, speciellt avseende kravställning och säkerhetsstyrning. Sådan personal innehar både viktig teknisk kunskap, verksamhetskunskap och är troligtvis även mer insatta i organisationens mål om en välfungerande IT-miljö än en extern part. Nyttjande av säkerhetsfunktioner som levereras av samma externa part som hanterar IT-drift bör i möjligaste mån undvikas eftersom leverantören i så fall kommer att granska sig själv. Om intern kompetens inte kan erhållas bör organisationen anlita oberoende säkerhetsexperter för kvalitetssäkring och kravställning gentemot tjänsteleverantörer.

Generellt kan inte sägas att någon av de kommunikationstekniker som beskrevs i avsnitt 2.1 är bättre än någon annan. Vilken teknik som lämpar sig bäst när och var beror på vilka behov och krav som ställs på kommunikationen. Exempelvis har 4G (LTE-A) en väldigt hög överföringshastighet jämfört med Sigfox, men den potentiella fördelen spelar ingen roll om enheterna som nyttjar kommunikationen inte klarar av att hantera 4G:s höga hastigheter. Den höga hastigheten kan till och med bli ett hinder snarare än en fördel i vissa situationer eftersom enheterna inte kan hantera mer än en viss mängd kommunikation och därför riskerar att överbelastas (DoS).

På samma sätt som för 4G:s höga hastigheter innebär den låga överförings-hastigheten och det delade nätverket för Sigfox att denna teknik inte lämpar sig för kommunikation med periodvisa uppdateringar inom relativt korta intervall. Bluetooth å sin sida lämpar sig inte väl för kommunikation mellan enheter på ett större avstånd än 100 meter.

Den nya 5G-teknik som är under utveckling innebär på en hög nivå inte någon större förändring vad gäller säkerhetsaspekter jämfört med äldre tele-kommunikationsteknik, dock med ett viktigt undantag i form av att många av de svagheter som äldre telekommunikationsteknikerna har kommer att vara åtgärdade i 5G. Dock kvarstår de rent arkitektoniska sårbarheter som kommer sig av användning av trådlös teknik. Det är tänkt att 5G ska erbjuda högre överföringshastighet, lägre fördröjning och en utökad förmåga att hantera många samtidiga enheter. Denna förmåga i kombination med en eventuell övergång till IPv6 (vilket mycket väl kan komma att krävas för att det ska vara möjligt att använda 5G) kommer att ställa höga krav på systemägarna för att hantera och förändra systemen på ett säkert sätt i och med att många nya faktorer samverkar till att ge helt nya attackvektorer för angripare.

Det inledande stycket i avsnitt 4.2 diskuterar graden av skydd som bör appliceras på information som kommuniceras relaterat till skyddsvärdet av informationen. Beslutsfattare och kravställare bör klargöra både för sig själva och för leverantören vilken grad av skydd som är nödvändig för informationen i fråga. Samma avsnitt beskriver samtidigt att det för enheter med begränsade resurser ofta är riktighet och autentisering av kommunikationen och dess parter som är viktig, snarare än sekretess i form av kryptering. Kryptografiska funktioner utgör ofta ett problem för dessa typer av enheter och kan således prioriteras ned till fördel för riktighets- och autentiseringsfunktioner i de fall där kommunikationen har ett lågt skyddsvärde.

För enheter med begränsade resurser som hanterar kommunikation med ett högt skyddsvärde är kryptering troligtvis ändå nödvändigt. Det finns då ett flertal alternativ att tillgå, exempelvis kan konceptet av beräkningssnål kryptering som beskrevs i avsnitt 4.1 och i NIST (2017) med fördel användas i dessa situationer. Finns detta alternativ inte att tillgå eller av andra anledningar inte bedöms som relevant eller genomförbart, kan en mellanliggande enhet med större kapacitet att hantera kryptografiska funktioner anslutas till den resursbegränsade enheten. Detta är dock ett alternativ som ökar komplexiteten av lösningen i och med att antalet enheter i systemet riskerar att öka markant samt att kostnaderna för organisationen troligtvis ökar.

Denna rapport har beskrivit och diskuterat hur standarder kan utgöra stöd i beslutsfattande, hantering och tillhandahållande för direkt trådlöst nätverksanslutna system innehållande resursbegränsade enheter. Av dessa

standarder är IEC 62443 den som är mest mångsidig avseende informationssäkerhet, utan att direkt omnämna direkt trådlöst nätverksanslutna system med begränsade resurser. Standarden beskriver vanliga säkerhetsfunktioner med breda applikationsområden som exempelvis flerfaktor-autentisering och nätverkssegmentering. Samtidigt beskrivs även mer administrativa åtgärder såsom kravställning och RSA. Tack vare sin mång-sidighet är standarden relevant att beakta för alla säkerhetsaspekter relaterade till industriella informations- och styrsystem och så även för direkt trådlöst nätverksanslutna system med begränsade resurser.

6 Slutsats och rekommendationer

Direkt trådlöst nätverksanslutna system präglas av säkerhetsmässiga problem på grund av de begränsade interna resurser som enheterna i dessa system har. Rapportens litteraturgenomgång har dock visat att det finns standarder, specialiserade säkerhetsmekanismer, protokoll och hårdvara som kan nyttjas i syfte att förbättra IT-säkerheten i dessa typer av system. Nedan ges ett antal rekommendationer som utökar och förstärker MSB:s rekommendationer[11] angående säkerhet i kritisk infrastruktur.

- Administrativa beslut i form av policyer och i förlängningen krav-ställning bör utgå ifrån organisationens behov, men baseras på vedertagna säkerhetsstandarder. Om intern kompetens inte kan erhållas för kravställning bör organisationen anlita säkerhetsexperter som är helt separerade från, och i övrigt oberoende av, de leverantörer som upphandlingen innefattar.
- Gällande kommunikationsprotokoll kan inte sägas att något av de protokoll som i rapporten beskrivits är bättre än något annat. Valet av protokoll kan därför baseras på organisationens behov och de krav som ställs på kommunikationen.
- Det är viktigt att tänka på att det kan finnas dolda kommunikations-möjligheter i SoC-baserad utrustning. Det är därför nödvändigt att säkerställa redan tidigt i inköpsprocessen att tillverkaren eller system-leverantören har kontroll på och hanterar de kommunikationstekniker som kan finnas inbyggda i utrustningen. De tekniker som inte används bör inaktiveras och säkerställas att de inte kan slås på av misstag eller på distans.
- Leverantören kan ha specifik teknik påslagen för att ha möjlighet att utföra tjänster såsom automatisk uppdatering och underhåll på distans. Sådana tjänster bör specificeras och hanteras vid upprättande av kontrakt. Interna rutiner baserade på säkerhetsanalyser och policyer bör också upprättas för att hantera tillgång till de egna systemen.
- Trådlös kommunikation är generellt mindre tillförlitlig än trådburen. Likaså är det svårare att garantera en maximal fördröjning i trådlösa

[11] https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/IndustriSCADA/Rekommendationer-och-rad/

nätverk än i trådade. Trådlös teknik lämpar sig därför sämre för system med realtidskrav på kommunikationen, eller för samhällskritiska system med höga krav på tillförlitlighet.

- Graden av skydd som bör appliceras på informationen som cirkulerar i systemet bör baseras på informationens skyddsvärde. Skyddsvärdet kan även påverka vilket kommunikationsprotokoll som är bäst lämpat att använda.
- I de fall där kryptering av kommunicerad information är nödvändig är konceptet beräkningssnål kryptering ett alternativ att tillgå. Om detta inte är möjligt finns andra alternativ, exempelvis kan en mellanliggande enhet som hanterar kryptering och dekryptering användas. Detta ökar dock både kostnaden och komplexiteten i lösningen eftersom fler enheter och mjukvaror måste administreras och uppdateras.
- Nätverkssegmentering är en viktig skyddsåtgärd för direkt trådlöst nätverksanslutna system, särskilt i de fall där säkerhetsmekanismer på enhetsnivå är begränsade eller obefintliga. I dessa fall bör nätverkssegmentering appliceras i syfte att skydda systemets kritiska delar från angrepp som går via enheter med begränsade resurser.
- IEC 62443 är en mångsidig standard som bör beaktas i alla säkerhets-relaterade uppdrag relaterat till industriella informations- och styrsystem.

Referenser

Adomnicai, A., Lac, B., Canteaut, A., Fournier, J., Masson, L., Sirdey, R. & Tria, A. (2016). On the importance of considering physical attacks when implementing lightweight cryptography. I *Lightweight Cryptography Workshop 2016*. Gaithersburg (MA), USA 17–18 oktober 2016. https://www.nist.gov/sites/default/files/documents/2016/10/17/adomnicai-paper-lwc2016.pdf

Burg, A., Chattopadhyay, A. & Lam, K. (2018). Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. *Proceedings of the IEEE*, 106(1), ss.38–60. DOI: 10.1109/JPROC.2017.2780172

Communications-Electronic Security Group (CESG) (2015). *End User Devices Security Guidance: Enterprise Considerations.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/391360/End_User_Devices_Security_Guidance_-_Enterprise_considerations.pdf

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE transactions on Information Theory*, 22(6), ss.644–654. https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B08.pdf

Federal Office for Information Security (BSI) (2018). *Cryptographic Mechanisms: Recommendations and Key Lengths* (BSI TR-02102-1). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7

Ferguson, N., Schneier, B., & Kohno, T. (2011). *Cryptography engineering: design principles and practical applications*. John Wiley & Sons.

Försvarets Radioanstalt (FRA) (2017). *Åtgärdsförslag: Angrepp via tjänsteleverantörer.* Stockholm: FRA. https://forsvaretsradioanstalt.se/download/18.60b3f8fa16488d849a5106/1531472534288/Atgardsforslag-Angrepp-mot-tjansteleverantorer.pdf

Gartner (2017). Gartner Says 8.4 Billion Connected ”Things” Will Be in Use in 2017, Up 31% From 2016. *Gartner*, 7 februari. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 [2018-10-22]

Genkin, D., Shamir, A. & Tromer, E. (2014). RSA key extraction via low-bandwidth acoustic cryptanalysis. I *CRYPTO 2014, Proceedings of the 34th Annual Cryptology Conference*. Santa Barbara (CA), USA 17–21 augusti 2014,

ss.444–461. https://link.springer.com/content/pdf/10.1007/978-3-662-44371-2_25.pdf

International Society of Automation (ISA) (u.å.). *ISA99, Industrial Automation and Control Systems Security.* https://www.isa.org/isa99/ [2018-10-22].

Karresand, M. (2017). *Risker med IPv6 inom industriella informations- och styrsystem* (FOI MEMO 6114). Stockholm: FOI.

Kaspersky (2014). Industrial Security – Cyberthreats to ICS systems: You Don't Have to be a Target to Become a Victim. Kapsersky Labs. https://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf

Koeune, F. & Standaert, F-X. (2005). A Tutorial on Physical Security and Side-Channel Attacks. I Aldini, A., Gorrieri, R. & Martinelli, F. (red.) *Foundations of Security Analysis and Design III*. Berlin, Heidelberg: Springer, ss.78–108. https://doi.org/10.1007/11554578

Loveless, M. (2018). Understanding Bluetooth Security. *Decipher.* https://duo.com/decipher/understanding-bluetooth-security [2019-03-25]

Martinasek, Z., Zeman, V., & Trasy, K. (2012). Simple electromagnetic analysis in cryptography. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems,* 1 (1), 13–19.

Munro, K. (2017). Hacking IoT vendors & smart cars via private APNs. 23 oktober, *Pen Test Partners* [blogg]. https://www.pentestpartners.com/security-blog/hacking-iot-vendors-smart-cars-via-private-apns/ [2019-03-21]

National Institute of Standards and Technology (NIST) (2012). *SP800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)* (SP800-153). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2013). *SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53 rev. 4). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2015). *SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* (SP800-131Ar1). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2017). *IR 8114 Report on Lightweight Cryptography* (IR8114). Gaithersburg: NIST.

Obaidat, M. S., Anpalagan, A. & Woungang, I. (Eds.). (2012). Handbook of green information and communication systems. Academic press. https://doi.org/10.1016/C2011-0-04359-4

Okhravi, H., Bak, S. & King, S. T. (2010). Design, implementation and evaluation of covert channel attacks. I *HST'10, 2010 IEEE International Conference on Technologies for Homeland Security*. Waltham (MA), USA 8–10 november 2010, ss. 481-487. DOI: 10.1109/THS.2010.5654967

Ren, K. (2017). Bluetooth Pairing Part 5 – Legacy Pairing – Out of Band. *Bluetooth Blog*. https://blog.bluetooth.com/bluetooth-pairing-part-5-legacy-pairing-out-of-band [2019-03-25]

Rodríguez, J. (u.å.). Most common attack vector over Critical Infrastructures. *Atos* [blogg], 26 januari. https://www.cipsec.eu/content/most-common-attack-vector-over-critical-infrastructures [2019-01-14]

Saltzer, J.H. & Schroeder, M.D. (1975). The Protection of Information in Computer Systems. I *Proceedings of the IEEE*, 63(9), ss. 1278-1308. DOI: 10.1109/PROC.1975.9939.

Seri, B. & Vishnepolsky, G. (2017). *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks*. Palo Alto: Armis.

Stevens, M., Bursztein, E., Karpman, P., Albertini, A. & Markov, Y. (2017). The first collision for full SHA-1. I CRYPTO 2017, Proceedings of the 37th Annual International Cryptology Conference. Santa Barbara (CA), USA 20–24 augusti 2017, ss.570-596. https://doi.org/10.1007/978-3-319-63688-7

Swedish Standards Institute (SIS) (2012). *Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General* (ISO/IEC 29192-1:2012). Stockholm: SIS.

Swedish Standard Institute (SIS) (u.å.). *ISO 27000 Informationssäkerhet.* https://www.sis.se/iso27000/ [2018-10-22].

Valassi, C., Lindahl, D. & Westerdahl, L. (2018). *Kryptografiska funktioner inom industriella informations- och styrsystem* (FOI-R--4596--SE). Stockholm: FOI.

Vanhoef, M. (2017). *Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse*. https://www.krackattacks.com/ [2018-01-14].

Wang, X., Feng, D., Lai, X. & Yu, H. (2004). Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. https://eprint.iacr.org/2004/199.pdf

Zander, S., Armitage, G., & Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials*, 9(3), 44–57. DOI: 10.1109/COMST.2007.4317620

Zhang, P. (2010). *Advanced industrial control technology*. William Andrew. https://doi.org/10.1016/C2009-0-20337-0

Bilaga A Ordlista

Asymmetrisk kryptering är en metod för att hantera krypterad kommunikation mellan två parter som inte tidigare har kommit överens om en gemensam hemlighet (till exempel ett lösenord). För detta behövs ett nyckelpar (två kryptografiska nycklar som är sammanlänkade) för varje part bestående av en privat och en publik nyckel. Trots att nycklarna är sammanlänkade ska det i praktiken vara omöjligt att använda den publika nyckeln för att härleda den privata nyckeln för en användare. Den privata nyckeln hålls alltid hemlig av innehavaren. Med hjälp av den publika nyckeln kan vem som helst kryptera ett meddelande så att bara innehavaren av den privata nyckeln i nyckelparet kan öppna det.

Asymmetrisk kryptering kan även användas för autentisering genom att den privata nyckel används för att signera ett meddelanden, vars riktighet sen kan verifieras av mottagaren genom att använda den publika nyckeln (digitala signaturer). Viktigt att notera är att den privata nyckeln inte används direkt för att signera meddelanden utan att en *signeringsalgoritm* genererar en signatur från nyckeln och meddelandet. Asymmetrisk kryptering kräver mycket längre nycklar för att uppnå samma säkerhetsnivå som *symmetrisk kryptering* (Valassi, Lindahl & Westerdahl 2018).

Attackvektor är benämningen på en IT-säkerhetsrelaterad svaghet i ett system med vilken en angripare kan ta sig in eller på annat sätt åsamka skada. Det kan finnas flera sätt att angripa svagheten (utnyttja attackvektorn). Typiska exempel på attackvektorer är skadlig kod i mail, icke uppdaterade programvaror och överbelastningsattacker (Rodríguez u.å.).

Autentisering innebär att styrka sin identitet, exempelvis när ett paket hämtas från närmaste paketombud. I den digitala världen kan detta exempelvis uppnås på kryptografisk väg genom användning av en privat nyckel för att producera en signatur som bara en specifik entitet har tillgång till (Valassi, Lindahl & Westerdahl 2018).

Bandbredd är beteckningen på hur stort flöde av digital information som en nätverksenhet kan klara. Bandbredd mäts i bitar/sekund och motsvaras av en 1/8 värdet mätt i byte/sekund. Ett mått som är lättare att relatera till är storlek på filer och annan data, 100 Mbit/s motsvarar således 12,5 MByte/s.

Botnet (botnät) är en grupp datorer som tagits över av en angripare och sedan används för att utföra överbelastningsangrepp på system genom att alla datorer samtidigt kontaktar en specifik server, webbplats eller webbtjänst. Botnät kan köpas eller hyras, vilket gör det mycket lätt att utföra överbelastningsangrepp även för gemene man.

Chipset motsvarar på svenska en uppsättning av samverkande kretsar. Termen används ofta för att beteckna att olika enheter till viss del har samma komponentmässiga innehåll. Dessa enheter delar då chipset.

Cyberfysiska system är mjukvara som interagerar med fysiska komponenter och den fysiska omgivningen, exempelvis självkörande bilar eller robotar.

(D)DoS ((Distributed) Denial of Service) är en angreppsform där ett system eller en funktion överbelastas så att den får sämre *tillgänglighet*. Angreppet genomförs ofta med hjälp av ett *botnät* och är svårt att skydda sig emot eftersom angreppet många gånger inte går att skilja från stora mängder vanlig nätverkstrafik.

Direkt trådlöst nätverksanslutet system avser i denna rapport enheter och system som är trådlöst anslutna och direkt adresserbara utan mellanliggande nätverksfunktion från publika nätverk. Det vill säga att de har egen inbyggd nätverksfunktionalitet och kräver ingen extra utrustning för att ansluta till trådlösa nätverk.

Faradaybur är en inneslutning (exempelvis en väska, ett skåp eller ett rum) i metall som är speciellt tillverkad för att blockera elektromagnetisk strålning, det vill säga radiosignaler.

Flerfaktorautentisering är en form av autentisering som använder sig av minst två olika attribut. Autentiseringen kan exempelvis kräva både kunskap om ett lösenord och tillgång till ett specifikt mobiltelefonnummer till vilken en engångskod skickas via SMS. Generellt sett krävs det attribut från minst två av följande tre kategorier; något du vet (till exempel lösenord), något du är (till exempel fingeravtryck) och något du har (till exempel din mobiltelefon).

Gateway är en enhet som kopplar ihop två olika nätverk som inte delar *protokoll* med varandra.

Hashfunktioner är så kallade *envägsfunktioner* vilket innebär att det är lätt att genom en hashfunktion räkna fram en hashsumma, men svårt att räkna ut det ursprungliga meddelandet med hjälp av hashsumman. Kryptografiska hashfunktioner utgör en delmängd av alla hashfunktioner och innehar ett antal specifika attribut eller krav som inte appliceras på övriga hashfunktioner. Bland annat krävs att det ska vara omöjligt att generera originalmeddelandet med hjälp av hashsumman, utan att testa alla möjligt kombinationer (*brute force).* Ett annat krav är att det ska vara högst osannolikt att två olika meddelanden genererar samma hashsumma. Kryptografiska hashfunktioner utgör grunden för både digitala signaturer och *Message Authentication Codes* (MAC) (Valassi, Lindahl & Westerdahl).

Hashsumma är ett kondensat eller delmängd av fast längd av en större informationsmängd i syfte att möjliggöra upptäckt av förändringar i datamängder.

Härdning innebär en systematisk genomgång av ett systems IT-säkerhets-funktioner för att säkerställa högsta möjliga säkerhetsnivå.

IP-adress är den adress som varje enhet behöver inneha för att kunna kommunicera via internet eller andra *Internet Protocol* (IP)-baserade nätverk. Adressen finns i två versioner IPv4 och IPv6 (IP version 4 respektive 6). Användningen av IPv4 är fortfarande mest utbredd, men denna version innehåller för få adresser ($4{,}4*10^9$ stycken) för att varje enhet i världen ska få en unik adress och kräver därför speciallösningar för att fungera. IPv6 har å sin sida $3{,}4*10^{38}$ stycken unika adresser, vilket anses vara tillräckligt många för att räcka under överskådlig tid.

Klockcykel avser ett taktslag för klockan som reglerar en processors arbete. En processor med en klockfrekvens på 1 gigahertz (GHz) genomgår en miljard klockcykler per sekund. Äldre processorer genomförde högst en instruktion per klockcykel, detta stämmer inte för dagens processorer som klarar av att genomföra flera instruktioner per klockcykel.

Kollisionsresistens är kopplat till de olika algoritmer som används för att beräkna hashsummor. Det betecknar hur lätt det är att skapa två olika data-mängder (exempelvis dokument) som har samma hashsumma, det vill säga genererar en hashsummekollision. De två välkända hashfunktionerna MD5 och SHA1 är helt eller delvis knäckta och ska inte längre användas i IT-säkerhetsammanhang (Stevens, Bursztein, Karpman, Albertini & Markov 2017).

Sekretess avser förmågan att hemlighålla information från obehöriga läsare. Sekretess är en av de tre grundläggande IT-säkerhetsparametrar som styr i stort sett allt IT-säkerhetsarbete. Dessa tre parametrar har på engelska beteckningen CIA som står för confidentiality, integrity och availability.

Man-in-the-Middle (MitM) är en angreppstyp där en angripare sitter som en relästation mellan två system, enheter eller entiteter som kommunicerar. Resultatet blir att angriparen har möjlighet att styra, hindra och förändra allt som sänds och tas emot. Angreppet fungerar även vid krypterad kommunikation om inte sändare och mottagare *autentiserar* sig korrekt. Angriparen upprättar då en krypterad kanal åt vardera hållet och har därför full tillgång till allt som skickas trots att kommunikationen är krypterad.

Network Address Translation (NAT) är en funktion som döljer ett nätverk och alla dess IPv4-adresser för andra nätverk. På så sätt kan flera nätverk använda samma adressuppsättning, vilket gör att det går att ansluta flera enheter än vad det finns IPv4 adresser att tillgå. Det finns flera olika adressuppsättningar som är

avsedda att använda för detta och den största uppsättningen innehåller 16,8 miljoner adresser. Översättningen görs genom att en publik IP-adress på utsidan (mot andra nätverk och internet) kopplas till olika adresser på insidan med hjälp av *portar*. NAT-funktionalitet återfinns ofta i brandväggar och routrar och marknadsförs i dessa sammanhang ofta som en säkerhetsfunktion, vilket det dock inte är.

Nyckellängd är en avgörande säkerhetsfaktor vid användning av moderna, godkända, krypteringsalgoritmer. Den för närvarande rekommenderade minsta nyckellängden är 2048 bitar för asymmetrisk kryptering och 128 bitar för symmetrisk kryptering (BSI 2018). Från och med år 2023 höjs rekommendationen för asymmetrisk kryptering till minst 3072 bitar långa nycklar.

Nyckelutbyte är den process som används vid upprättande av en krypterad kommunikationslänk för att båda parter ska ha tillgång till samma nyckel (sessionsnyckel). Det finns olika processer för detta, exempelvis Diffie-Hellmans nyckelutbyte (Diffie & Hellman 1976).

Port kallas den logiska adress (65536 stycken) som läggs till IP-adressen vid användning av *Transmission Datagram Protocol* (TCP) och *User Datagram Protocol* (UDP). Ofta kopplas ett portnummer till en specifik tjänst. Exempelvis återfinns ofta webbservrar bakom port 80 vid okrypterad trafik (*HTTP*) och port 443 vid krypterad (*HTTPS*). Portar används även vid NAT.

Protokoll betecknar de regler kring kommunikation som används i datanätverk. De specificerar hur förbindelse ska upprättas. genomföras och avslutas, samt hur eventuella fel ska hanteras. Vanliga protokoll är till exempel TCP, UDP och IP.

Ransomware är programvara som kidnappar data genom att kryptera den. Dataägaren måste sedan betala en lösensumma för att få all data dekrypterad igen.

Resursbegränsad enhet avser i denna rapport en enhet av mindre storlek med begränsad beräknings- och lagringsförmåga, exempelvis IoT-enheter, cyber-fysiska system samt inbyggda system. Resursbegränsningen leder i sin tur till att dessa typer av enheter inte kan hantera standardiserade krypterings-implementationer. Exempelvis används ofta kortare nyckellängder för att enheterna ska kunna hantera kryptografiska algoritmer, vilket även reducerar enheternas erhållna säkerhetsnivå.

Riktighet avser egenskapen att information är oförvanskad när den når mottagaren och är en av de tre grundläggande IT-säkerhetsparametrar som styr i stort sett allt IT-säkerhetsarbete. Dessa tre har på engelska beteckningen CIA som står för confidentiality, integrity och availability.

Service Set Identifier (SSID) är en logisk identifierare för att avskilja olika trådlösa nätverk från varandra. SSID kallas i vardagligt för nätverksnamn.

Software-defined Radio (SDR) (*mjukvarudefinierad radio*) är ett koncept för radiokommunikation där signalbehandling och andra uppgifter som typiskt hanteras av hårdvara, istället hanteras av mjukvara i en dator.

Symmetrisk kryptering används när både avsändare och mottagare delar en gemensam hemlighet (exempelvis ett lösenord). Fördelen med symmetrisk kryptering är att den kan göras snabbare än asymmetrisk och det finns en hög tilltro till symmetriska lösningar. Ofta används asymmetrisk kryptering för att etablera symmetrisk kryptering genom att skydda den gemensamma nyckel som används i den symmetriska lösningen när denna överförs mellan kommunicerande parter (Valassi, Lindahl & Westerdahl 2018).

Tillgänglighet berör kravet på att en autentiserad användare ska ha tillgång till information när denna efterfrågas och är en av de tre grundläggande IT-säkerhetsparametrar som styr i stort sett allt IT-säkerhetsarbete. Dessa tre har på engelska beteckningen CIA som står för confidentiality, integrity och availability.

Återspelningsattack är ett angrepp där angriparen har spelat in en hel eller delar av en kommunikationssession och sedan skickar om trafiken igen. Om det angripna systemet inte är tillräckligt säkert kan det fås att acceptera angriparens kommunikation som legitim i och med att det är gammal legitim nätverkstrafik som skickas.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se