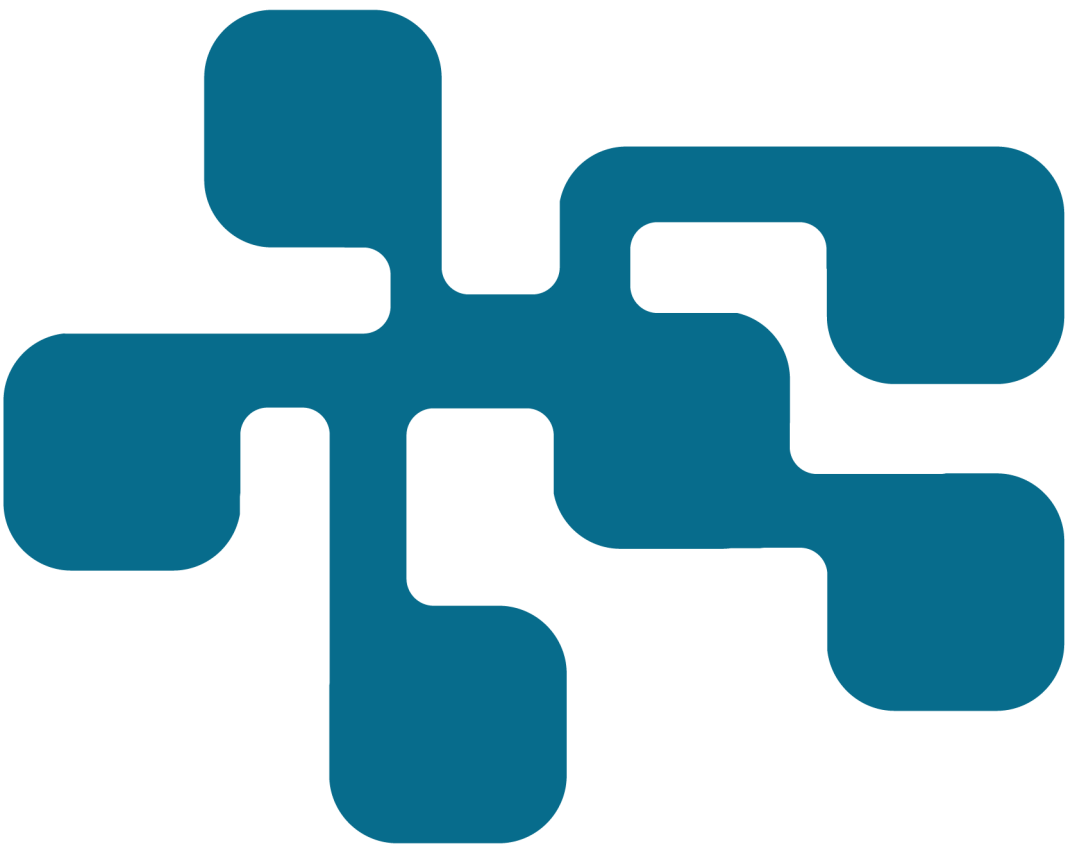
NCS3 - Kryptografiska funktioner inom industriella informations- och styrsystem

CHRISTIAN VALASSI, DAVID LINDAHL, LARS WESTERDAHL

FOI
MSB



FOI-R--4596--SE
MSB 2017-1623
ISSN 1650-1942

Maj 2018

Christian Valassi, David Lindahl, Lars Westerdahl

Kryptografiska funktioner inom industriella informations- och styrsystem

Titel	Kryptografiska funktioner inom industriella informations- och styrsystem
Title	Cryptographic functions in industrial control systems
Rapportnr/Report no	4596
Månad/Month	Maj
Utgivningsår/Year	2018
Antal sidor/Pages	45
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ej FoT
Projektnr/Project no	E72201
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Industriella informations- och styrsystem står idag inför komplexa utmaningar i takt med att dessa, traditionellt isolerade, system blir allt mer uppkopplade mot publika och osäkra nätverk. Industriella informations- och styrsystem kontrollerar och övervakar fysiska processer. Dessa processer kan sällan avslutas i förtid utan att detta innebär stora ekonomiska konsekvenser för den ägande organisationen. Att dessa system sällan kan stängas ner i kombination med en livslängd som ofta överskrider 20 år, leder till att systemen ofta opererar med utdaterad teknik, vilket i sin tur innebär en större sårbarhet för cyberangrepp. Eftersom dessa system har en inverkan i det fysiska rummet kan konsekvenserna av ett framgångsrikt cyberangrepp få katastrofala konsekvenser inte bara ekonomiskt, utan även fysiskt och kan i värsta fall leda till att människoliv går förlorade. Detta sammantaget gör att det är av stor vikt att skydda dessa system mot cyberangrepp.

Denna rapport undersöker behov, nyttjande samt relevans av kryptografiska funktioner som skydd mot cyberangrepp. Rapporten innehåller två typer av informationsinsamling: litteraturstudier respektive intervjuer. Två litteraturstudier genomfördes för att (1) identifiera lagkrav och standarder för kryptografiska funktioner inom industriella informations- och styrsystem. (2) Identifiera vilka kryptografiska funktioner som är lämpliga att implementera i kontexten av industriella informations- och styrsystem. Intervjuer genomfördes med två operatörer inom branscher med olika skyddskrav samt en intervju med en leverantör av styrsystemskomponenter. Resultatet av litteraturstudierna och intervjuerna leder till en rekommendation att all extern trafik samt lagrad data krypteras. Intervjuernas respondenter motsätter sig kryptering av de interna nätverken då detta avsevärt försvårar övervakning. Istället läggs stor vikt på autentisering av kommunikation i de interna nätverken.

Nyckelord: Kryptering, kryptografiska funktioner, säker kommunikation, industriella informations- och styrsystem

Summary

Industrial control systems (ICS) face complex challenges as these, traditionally isolated, systems are becoming more and more connected to unsecure public networks. Industrial control systems control and monitor physical processes which seldom can be terminated prematurely without great economic consequence to the owning organisation. The fact that these systems can rarely be shutdown, in combination with a system life span that often exceeds 20 years, means that industrial control systems often operate with outdated technology; which in turn causes them to have greater exposure, and be more vulnerable to cyber-attacks. These systems impact the physical space – a successful cyber-attack on an industrial control system can therefore have catastrophic consequences, not just economic but physically, and can in the worst case cause the loss of human life. This is why it is essential to protect industrial control systems from cyber-attacks.

This report examines the need, use, and relevance of cryptographic functions as means of protection against cyber-attacks. The report is based on two types of information collection: literature studies and interviews. Two literature studies were conducted in order to (1) identify legal requirements and standards for cryptographic functions in industrial control systems. (2) Identify which cryptographic functions are appropriate to implement in the context of industrial control systems. Interviews were conducted with two operating organisations in industries with differing protection requirements, as well as one interview with a supplier of control system components. The results of the literature studies and the interviews leads to the recommendation to encrypt all external network traffic and stored data. The interview respondents were opposed to encryption of the internal networks as this significantly complicates monitoring of these networks. Instead they place great emphasis on authenticating communication in the internal networks.

Keywords: Encryption, Cryptographic functions, Secure communications, Industrial control systems

Innehållsförteckning

1 Inledning

Kryptografiska funktioner har länge använts inom flertalet datorrelaterade områden, framförallt för att tillhandahålla konfidentialitet. Dessa funktioner har dock fler användningsområden såsom autenticitet och riktighet i information. Ett datorrelaterat område som dock länge legat efter i nyttjandet av kryptografiska funktioner som informationsskydd är industriella informations- och styrsystem. Detta beror på att industriella informations- och styrsystem länge har haft en begränsad hotbild från antagonistiska aktörer genom att de använt egna eller dedikerade publika kommunikationssystem samt i stor utsträckning använt egenutvecklad teknik. I dagsläget är det dock vanligare att känd och kommersiellt tillgänglig informationsteknik används i dessa system och att de kommunicerar över publika nätverk. Detta resulterar i att systemen har en högre grad av exponering jämfört med tidigare och därmed fler möjligheter för en antagonist genom en större attackyta. Kommande tekniker och lösningar för exempelvis industriell tillämpning av sakernas internet (eng. *Internet of Things*) och digitalisering ökar sannolikt exponeringen av dessa system ytterligare. Det torde därför finnas ett behov av att skydda den information som hanteras inom industriella informations- och styrsystem.

Informationssäkerhet, det vill säga förmågan att skydda information, beskrivs ofta genom egenskaperna *konfidentialitet*, *riktighet* och *tillgänglighet*. Konfidentialitet avser förmågan att hemlighålla information från obehöriga läsare. Med riktighet avses förmågan att kunna upptäcka om informationen har förändrats från den lämnade avsändaren tills dess att en behörig läsare öppnar (dekrypterar) informationen. Tillgänglighet avser förmågan att få fram information till en behörig läsare när läsaren behöver informationen. Egenskaperna konfidentialitet, riktighet och tillgänglighet är troligtvis mer kända under sina engelska benämningar: *confidentiality*, *integrity* och *availability*.

Traditionellt har konfidentialitetsbehoven ofta dominerat över 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 processen, det vill säga den funktionalitet som systemen levererar, det som är kritiskt. Ett avbrott i informationsflödet kan därför leda till katastrofala konsekvenser avseende människoliv eller stora ekonomiska förluster för processägaren. Detta innebär att för industriella informations- och styrsystem så har egenskapen tillgänglighet stor betydelse.

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 undersöka behovet och nyttjandet av kryptografiska funktioner inom industriella informations- och styrsystem. Studien ska besvara vilka kryptografiska lösningar som är lämpliga att använda i industriella informations- och styrsystem.

1.2 Genomförande

Inledningsvis genomfördes en litteraturstudie i syfte att identifiera formella krav på säker kommunikation från lagstiftare och branschorganisationer. Samtidigt genomfördes en litteraturgenomgång av existerande kryptografiska funktioner, för att identifiera och beskriva relevanta kryptografiska funktioner i kontexten av industriella informations- och styrsystem.

Därefter genomfördes en intervjuserie med frågor baserade på de inledande litteraturstudierna samt mer allmänna frågor. Intervjufrågorna återfinns i sin helhet i Bilaga A. Syftet med intervjuserien var att identifiera behov och lösningar från operatörs- respektive leverantörsperspektiv. Respondenterna bestod av två operatörer inom olika branscher och en leverantör av styrsystemskomponenter.

1.3 Läshänvisning

I kapitel två ges en översiktlig beskrivning av hotbilden mot industriella informations- och styrsystem samt en beskrivning av relevanta regelverk och standarder. I kapitel tre beskrivs grundläggande tekniker och tillämpningar av kryptografiska funktioner. I kapitel fyra beskrivs utmaningar med att hantera kryptografiska funktioner under dess livstid. Resultat från intervjuer presenteras i kapitel fem och diskuteras i kapitel sex. Rapporten sammanfattas med slutsatser i kapitel sju.

Läsare som är väl bekanta med kryptografiska funktioner och dess vanligaste tillämpningar hänvisas direkt till kapitel fem.

2 Behov av säker informations-hantering för industriella informations- och styrsystem

Datorisering av industriella informations- och styrsystem har medfört system som i stort liknar IT-system i uppbyggnad och innehåll. Behovet av att hålla ner kostnader har i flera fall inneburit lösningar som premierar kommersiellt tillgängliga komponenter framför egenutveckling. Detta har även påverkat hur system kommunicerar, inledningsvis över vilket media men efterhand även på vilket sätt som exempelvis information tillgängliggörs för de som driver systemet.

I detta kapitel beskrivs en övergripande hotbild mot industriella informations- och styrsystem, samt en översikt över de regelmässiga krav och standarder som syftar till att säkerhetsställa konfidentialitet, riktighet och tillgänglighet.

2.1 Hotbild

Myndigheten för samhällsskydd och beredskap (MSB) beskriver i *Vägledning till ökad säkerhet i industriella informations- och styrsystem* (MSB 2014) hotbilden enligt följande:

> *Gränserna mellan traditionella/administrativa IT-system och industriella informations- och styrsystem håller på att suddas ut i och med en ökad integrering mellan dessa olika system. För att uppnå hög flexibilitet och effektivitet görs industriella informations- och styrsystem även i allt högre grad tillgängliga via Internet och andra publika nätverk. Dagens industriella informations- och styrsystem bygger dessutom allt mer på samma teknik som vanliga IT-system och drabbas därmed av samma säkerhetsproblem. Resultatet av denna utveckling är en ökad attackyta och radikalt förändrad riskbild.*

Det är rimligt att anta att den information som används för att styra kritisk infrastruktur måste skyddas mot angrepp. Men hur ska informationen skyddas och vad är hoten?

Det finns ett antal grupper av aktörer som kan tänkas utgöra hot mot industriella informations- och styrsystem och de organisationer som driver dem. Den första hotkategorin är enskilda individer som av någon anledning angriper system. Det kan vara personligt motiverade individer det vill säga personer som är eller har varit anställda av organisationen men som nu valt att agera mot den, så kallade

insiders. De kan också vara individer som blivit värvade eller hotade av kriminella organisationer eller främmande makt.

Politiskt motiverade angripare kallas *hacktivister*. Att använda datorer i politisk aktivism, har blivit allt vanligare och angriparna tenderar att vara löst sammansatta grupper av individer som utför angrepp mot ett gemensamt övergripande mål. Ofta är syftet med angreppen i första hand att få uppmärksamhet för det politiska mål gruppen agerar för, även om riktade sabotage kan förekomma.

Industrispionage förekommer frekvent inom de flesta branscher som nyttjar industriella informations- och styrsystem. Verizon (2018) noterade i sin årliga dataintrångsrapport att så mycket som 47 % av alla rapporterade angrepp mot tillverkningssektorn var ett resultat av industrispionage. Industrispionage utförs till största del av främmande makt antingen direkt eller via ombud.

Terrorister har historiskt till stor majoritet fokuserat på fysiska angrepp; sällan riktade mot industrier, utan istället mot en befolkning eller statliga institutioner. Det är i nuläget svårt att sia om vilka ändamål cyberterrorism kan komma att tjäna, om cyberterrorism ens blir en relevant hotfaktor. Däremot kan IT-brottslighet användas för andra ändamål än terror, exempelvis kan utpressningsmjukvara (eng. *ransomware*) vara ett medel för ekonomisk vinning.

Organiserad brottslighet inom cybervärlden är något som de senaste åren fått mycket publicitet i takt med att antalet storskaliga attacker ökat. Framförallt har dessa angrepp utgjorts av utpressningsmjukvara där ett stort antal organisationer och individer drabbats. Motivet för denna typ av organiserad brottslighet är i regel ekonomisk vinning, exempelvis som vid angreppet mot Uber (Richter 2017). Dock finns även en rad andra tänkbara motiv, exempelvis ren förstörelse både digitalt och fysiskt.

Främmande makts aktiviteter inom cyberkrigföring, cyberspionage och cyberverksamhet generellt, har under de tio senaste åren fått allt större uppmärksamhet i media, se exempel Lagner (2013), Macaskill och Dance (2013) samt Sanchez (2015). Även industriella informations- och styrsystem är mål för dessa angrepp då systemen kan utgöra kritisk infrastruktur. Cyberangrepp är väldigt attraktivt för stater eftersom de för med sig möjligheten att rimligt förneka inblandning i angreppet. Det är mycket svårare att knyta ett cyberangrepp till en främmande makt jämfört med ett fysiskt angrepp. Motivet för en främmande makt, förutom själva cyberkrigföringen, kretsar mycket kring kartläggning och spionage mot andra nationer i det egna närområdet. Detta inkluderar även industrispionage för att kartlägga sårbarheter och attackytor för att planera ett tillvägagångssätt om ett angrepp bedöms som nödvändigt.

2.2 Lagar, förordningar och föreskrifter

Historiskt har kraven på skydd av information inom industriella informations- och styrsystem inte reglerats i lag. Detta kan komma att ändra sig efter att det så kallade NIS-direktivet (NIS-utredningen 2017) träder i kraft. I direktivet anges att relevanta myndigheter kommer att få behörighet att reglera vilka säkerhetsmekanismer som ska användas för att skydda informationen i viss kritisk infrastruktur. Kryptering finns omnämnt som ett exempel på säkerhetsmekanism, men i dagsläget finns det inget som säger under vilka omständigheter eller hur troligt det är att ett lagkrav kommer att komma på att använda kryptering i industriella informations- och styrsystem.

2.3 Standarder

Standarder, riktlinjer och rekommendationer är inte tvingande på samma sätt som lagar, förordningar och föreskrifter. De är å andra sidan mer konkreta i betydelsen att de kan beskriva teknik och tekniska lösningar. I de flesta fall handlar det dock om ramverk, vilket innebär att tekniken och kraven är översiktligt beskrivna och behöver anpassas till den verksamhet som läsaren själv representerar.

Standarder och rekommendationer publiceras oftast av internationella organisationer såsom *International Organization for Standardization* (ISO), *International Electronic Commission* (IEC) och *National Institute of Standards and Technology* (NIST). På nationell nivå publicerar även flera bransch-organisationer rekommendationer. De sistnämnda är ofta förtydliganden av standarder och innehåller mer branschspecifika exempel. En övergripande observation när det gäller standarder är att det finns fler standarder för informationssystem än för industriella informations- och styrsystem.

IEC har fastställt en serie standarder under namnet *IEC 62443 Security for Industrial Automation and Control Systems* (ISA u.å.). Standarden togs ursprungligen fram av *International Society for Automation* (ISA), vilka förvaltar standarden. IEC 62443 tar upp säkerhetsmålsättningar och vilka motmedel som kan användas, exempelvis kryptering och kryptografiska funktioner för autentisering. Standarden är lik ISO 27000-serien (SIS u.å.) i det att den är ett stöd vid kravställning och riskbedömning, men ställer inga specifika krav på använd teknik.

NIST SP800-82 Guide to Industrial Control Systems (ICS) Security (NIST 2015b) tar upp kryptering och kryptografiska funktioner som ett verktyg för att bevara konfidentialitet och åstadkomma säker inloggning. I dokumentet rekommenderar NIST att starka autentiseringsfunktioner såsom certifikat (se avsnitt 3.2.2) används, samt att lagrad data och extern kommunikation krypteras. För trådlösa lokala nätverk (WLAN) trycks särskilt på att kryptering bör

användas, men att det inte får ha en negativ påverkan på tillgängligheten av data för de komponenter som kommunicerar över nätverket.

Mer specifika regler avseende nyckelhantering i kryptosystem beskrivs i NIST SP 800-130 (NIST 2013b). I SP-800-130 presenteras och diskuteras ett antal relevanta områden som bör beaktas när ett kryptografiskt nyckelhanteringssystem designas. Publikationen presenterar även en rad krav som måste uppfyllas under utvecklingen av industriella informations- och styrsystem.

Branschmässiga rekommendationer kan ta upp specifika mål som är relevanta för branschen i sig själv. När det gäller IT och industriella informations- och styrsystem ställs sällan några specifika krav. Branschmässiga publikationer är ofta starkt färgade av ISO 27000, men även IEC 62443. I Svenska Kraftnäts (SvK) publikation *IT-säkerhetsarkitektur* (SvK 2015) trycks, precis som i NIST SP800-82 på behovet av kryptering vid extern kommunikation. I publikationen nämns specifikt IPsec och SSL/TLS som tekniker för skapandet av krypterade tunnlar (eng. *Virtual Private Network, VPN*).

För mer specifika krav har vissa branscher tagit fram riktlinjer för IT-säkerhet, exempelvis SvK. I *Tekniska riktlinjer IT-säkerhet* (SvK 2010) ställs krav på krypterad kommunikation över externa nätverk, men endast som ett bör-krav över lokala nätverk. Det trycks även på att endast kända och publikt granskade kryptolösningar ska användas. Leverantörer får inte använda egenutvecklade eller stängda kryptolösningar i levererade säkerhetsfunktioner.

Branscher som saknar rekommendationer eller som har mindre detaljerade rekommendationer behöver inte nödvändigtvis vara mer utsatta. Inom kärnkraftsbranschen, vilken inte saknar rekommendationer men där rekommendationerna är övergripande, är skyddsfunktioner primärt baserade på fysisk separation och då är behovet av att kunna kommunicera skyddat begränsat.

3 Kryptografiska funktioner

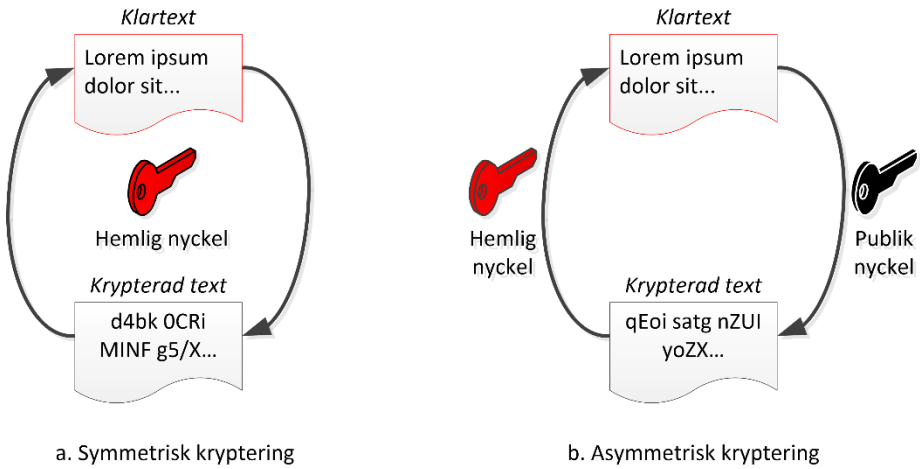
Kryptografi innebär konvertering av data till ett format som är obegripligt för en obehörig användare, vilket möjliggör säker lagring och överföring av data. Dessa kodade data kan endast läsas och begripas av behöriga användare som innehar rätt kryptografiska nyckel för att dekryptera dessa kodade data.

Det finns flertalet olika typer av kryptografiska funktioner, vissa av dem är generella och kan således implementeras i många olika typer av system; andra funktioner är mer specialiserade och lämpar sig endast för vissa typer av system. De kryptografiska funktioner och metoder som beskrivs i detta kapitel är applicerbara inom industriella informations- och styrsystem. Det är viktigt att förstå att kryptografiska funktioner aldrig kan skydda mot alla typer av hot på egen hand. Kryptografiska funktioner måste i regel kombineras med andra typer av säkerhetsmekanismer. Kryptografiska funktioner är främst ämnade att lösa problem gällande konfidentialitet och riktighet, snarare än tillgänglighet. Det är därför viktigt att veta om den del av systemet som ämnas skyddas faktiskt har behov av konfidentialitet, eftersom kryptografiska funktioner ofta försämrar prestanda och tillgänglighet i systemet de appliceras i.

I detta kapitel presenteras grundläggande kryptografiska funktioner, vilka direkt eller indirekt kan användas i industriella informations- och styrsystem.

3.1 Symmetrisk och asymmetrisk kryptering

Symmetrisk och asymmetrisk kryptering är två grundläggande metoder för att skapa säker kommunikation som båda innefattar användning av nycklar (Figur 1). I denna bemärkelse är en nyckel en parameter som bestämmer resultatet av en kryptografisk algoritm. Den stora skillnaden mellan de två metoderna är att symmetrisk kryptering använder en gemensam hemlig nyckel medan asymmetrisk kryptering använder två nycklar, en publik och en privat. Denna skillnad medför implikationer för den grad av säkerhet som erhålls och komplexiteten i användandet.



a. Symmetrisk kryptering

b. Asymmetrisk kryptering

Figur 1 Principbilder över symmetrisk och asymmetrisk kryptering

Både symmetrisk och asymmetrisk kryptering har styrkor och svagheter. De huvudsakliga fördelarna med symmetrisk kryptering är att själva krypterings- och dekrypteringsförloppet är snabbt samt att det finns en hög tilltro till symmetriska lösningar. En nackdel med symmetrisk kryptering är att alla som kommunicerar använder en gemensam nyckel. Det medför att det ställs stora krav på att nyckeln hemlighålls för utomstående och det medför också att om nyckeln röjs måste alla byta ut sin nyckel.

I asymmetrisk kryptering finns två nycklar per användare – en publik nyckel som vem som helst kan använda för att kommunicera med nyckelns ägare och en hemlig nyckel som nyckelägaren använder för att dekryptera meddelanden. Då den publika nyckeln endast används för att kryptera meddelanden kan den spridas godtyckligt, medan den hemliga nyckeln måste skyddas. För att kunna kommunicera med flera parter behöver avsändaren publika nycklar till alla som denne vill kommunicera med.

Asymmetrisk kryptering är dock beräkningstung, vilket innebär att det tar längre tid att kommunicera med denna metod. Det är därför vanligt att asymmetriska nycklar och certifikat används för att upprätta en kommunikation och att en symmetrisk nyckel skapas och utbyts specifikt för detta tillfälle. En sådan symmetrisk nyckel kallas för sessionsnyckel då den bara används så länge som kommunikationen varar.

3.2 Autentisering

Som tidigare nämnt är kryptering främst ett medel för att erhålla och säkerställa konfidentialitet, vilket är ett typiskt användningsområde för verksamheter där

information är det som är skyddsvärt. Detta är inte alltid fallet för industriella informations- och styrsystem. I industriella informations- och styrsystem är en stor del av kommunikationen styrsignaler och mätvärden där det inte är konfidentialitet som är centralt, utan istället tillgänglighet autenticitet och korrekthet. Det är således viktigare att säkerställa var informationen kommer ifrån och att denna inte har ändrats under färd, än att se till att ingen kan avlyssna och förstå kommunikationen.

Autentisering används inte bara för trafik i nätverk, det kan även användas för att säkerställa identiteten hos användare. Den traditionellt mest använda formen av autentisering i detta sammanhang är användarnamn och lösenord. På grund av den mänskliga faktorn ses dock detta inte längre som ett tillförlitligt sätt att säkerställa identitet då människor tenderar att använda lösenord som är lätta för en angripare att forcera (WP Engine 2015).

När det gäller autentisering beskrivs möjligheterna att autentisera en användare (eller ett system) med faktorerna någonting som användaren vet, har eller är. Lösenord är ett exempel på något som en användare vet. Exempel på någonting en användare kan ha är ett aktivt kort eller en RFID-tagg. Biometriska funktioner såsom avläsning av fingeravtryck, är någonting som användaren är. För att uppnå en stark autentisering kombineras minst två av faktorerna vet, har eller är. Några vanliga lösningar idag är kombinationen avläsning av ett aktivt kort och en PIN-kod, eller ett lösenord kombinerat med en kod som exempelvis erhålls via en mobiltelefon. Tvåfaktorautentisering är oftast att föredra ur säkerhetssynpunkt, men det är fortfarande vanligt med delade konton med ett delat lösenord, särskilt hos administratörer (Butler 2012).

3.2.1 Kryptografiska hashfunktioner

En hashfunktion omvandlar en datamängd till ett kondensat (en hashsumma) av fast längd i syfte att möjliggöra upptäckt av förändringar i datamängden (Figur 2). Hashfunktioner är så kallade *envägsfunktioner*, vilket innebär att det är lätt att räkna fram en hashsumma men svårt att räkna ut den ursprungliga texten med hjälp av hashsumman. Denna egenskap tillämpas exempelvis vid lagring av lösenord då det är olämpligt att lagra dessa i klartext.

Figur 2 Principbild över en hashfunktion

Kryptografiska hashfunktioner utgör en delmängd av antalet hashfunktioner, då det ställs högre krav på dessa. Även om kryptografiska hashfunktioner kan användas som vanliga hashfunktioner är det primära användningsområdet autentisering. Utöver de egenskaper som gäller för vanliga hashfunktioner, exempelvis att de ska vara snabba att beräkna och att ett givet meddelande alltid ska ge samma hashsumma, ställs även följande krav på kryptografiska hashfunktioner (Cornell 2007):

- Det ska vara omöjligt att generera originalmeddelandet från dess hashsumma, utan att testa alla möjliga kombinationer.
- Det ska vara osannolikt för två olika meddelanden att generera samma hashsumma.

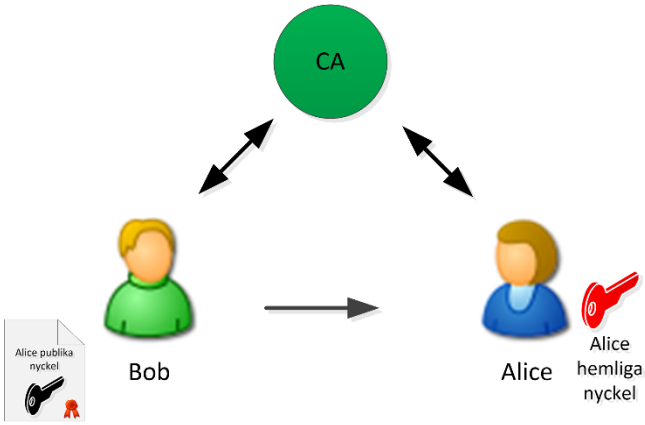
Följs reglerna för hashfunktioner och kryptografiska hashfunktioner kommer även små förändringar resultera i en annan hashsumma än för det oförändrade meddelandet.

Kryptografiska hashfunktioner utgör grunden för både digitala signaturer och *Message Authentication Codes* (MAC), som båda har applikationer inom industriella informations- och styrsystem. I dagsläget rekommenderas exempelvis användandet av SHA-2 eller SHA-3 (NIST 2015a). Hashfunktioner varar dock inte för evigt, främst på grund av att kollisioner upptäcks. Några tidigare kända hashfunktioner som idag inte rekommenderas är MD5 och SHA-1. Båda har visat sig ha en låg kollisionsresistens och bör därför inte längre användas (Stevens, Bursztein, Karpman, Albertini & Markov 2017).

3.2.2 Digitala Signaturer

Digitala signaturer är ett medel för att säkerställa ursprung och riktighet hos mottagen information. Digitala signaturer används då en mottagare vill försäkra sig om att meddelandet har sitt ursprung från den plats som det utger sig från att vara och att innehållet i meddelandet inte har ändrats.

Ett vanligt tillämpningsområde för digitala signaturer är i digitala certifikat. I dessa certifikat knyts en publik kryptonyckel och en användare samman med en digital signatur i syfte att underlätta hanteringen av publika nycklar. I X.509, den vanligaste formen av certifikatstruktur som bygger på en publik nyckelstruktur (eng. *Public Key Infrastructure, PKI*), skapas tilltro till certifikaten genom en hierarkisk struktur. Överst i strukturen finns en betrodd part som signerar alla certifikat. Denna part benämns som certifikatutfärdare (eng. *Certificate Authority, CA*). Alla användare av certifikat inom en X.509-infrastruktur litar på sin CA (Figur 3).



Figur 3 Principbild över en PKI-struktur

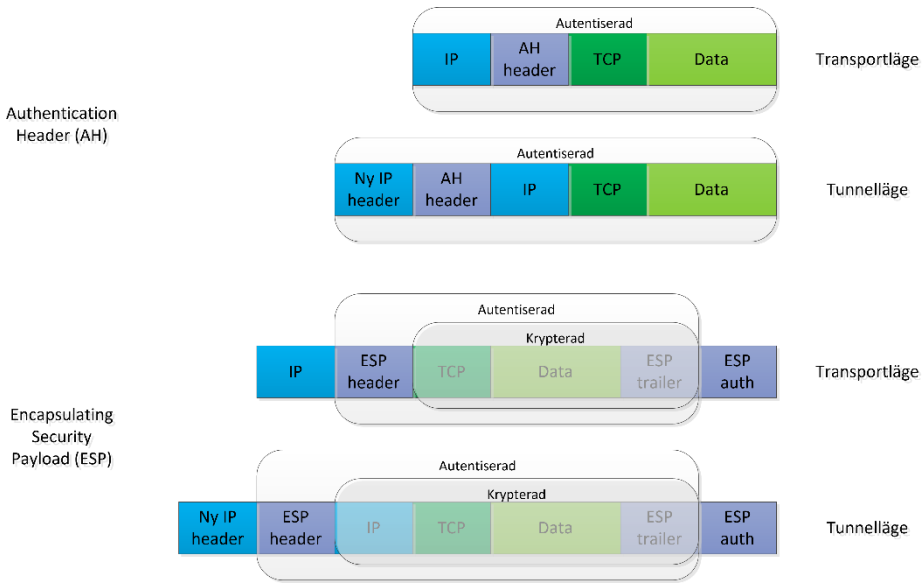
När ett certifikat skapas sätts även en giltighetstid för certifikatet. När giltighetstiden löpt ut upphör certifikatet att gälla även om den publika nyckel som certifikatet garanterar fortfarande kan fungera. En användare inskaffar ett nytt certifikat för samma eller en annan nyckel när tiden är på väg att löpa ut. Om certifikatägaren (Alice i Figur 3) skulle få andra förutsättningar än vad som anges i certifikatet, till exempel byta arbetsgivare, eller om hennes hemliga nyckel skulle komma på villovägar, kan certifikatet återkallas. Det innebär att certifikatet ogiltigförklaras och hamnar på en lista över återkallade certifikat (eng. *Certificate Revocation List, CRL*). Då ett certifikat, precis som den publika nyckel som certifikatet är kopplad till, ska kunna spridas godtyckligt, går det inte att ta bort ett ogiltigförklarat certifikat. Det innebär att den som vill kommunicera med Alice (Bob i Figur 3) måste dels kontrollera att signaturen i Alice certifikat är korrekt, dels om certifikatet är giltigt och inte har återkallats.

X.509 är *de facto*-standard för certifikat kopplat till personer och organisationer. Interna system inom en organisation har dock inte alltid certifikat som är signerade av en betrodd tredje part. För internt bruk kan en organisation använda självsignerade certifikat eller ha en intern CA.

Även om X.509 antyder att det bara ska finnas en CA och en hierarki så finns det flera företag och organisationer som har rollen som CA. För att användare från olika certifikatutfärdare ska kunna vara säkra på att certifikat de vill verifiera är korrekta har flera CA-organisationer även signerat varandra. På så sätt har en förtroendelänk skapats mellan olika certifikathierarkier.

3.3 Internet Protocol Security (IPsec)

IPsec är en förlängning av IP (Internet Protocol) och är utvecklat för att tillhandahålla kryptografisk säkerhet i nätverkslagret av OSI-modellen[1] eller internetlagret i TCP/IP-stacken[2]. IPsec består av två protokoll: *Authentication Header* (AH) och *Encapsulating Security Payload* (ESP), som kan användas i tunnel- respektive transportläge. AH garanterar anslutningslös integritet och ursprungsautentisering av data för IP-paket. Med AH kan även återspelningsattacker upptäckas genom implementation av ett unikt sekvensnummer för varje paket. På så sätt kan redan skickade paket detekteras. ESP förser kommunikationen med ursprungsautenticitet, riktighet och konfidentialitet (Figur 4). Även ESP innehåller sekvensnummer för att skydda mot återspelningsattacker. Den stora skillnaden mellan de två protokollen är att ESP, utöver de egenskaper som finns hos AH, även skyddar innehållet i varje paket mot röjande. Denna skillnad har lett till att AH idag används i mindre utsträckning än ESP på grund av protokollets redundanta egenskaper.



Figur 4 IPsecs protokoll i olika lägen

[1] Open Systems Interconnect (OSI) är en modell över hur datorer kommunicerar över nätverk. Modellen består av sju lager: fysiskt- (närmast nätverket), datalänk-, nätverk-, transport-, session-, presentation- och applikationslager.

[2] Transmission Control Protocol/Interent Protocol (TCP/IP) är en *de facto*-standard för hur datorer kommunicerar över nätverk. Stacken består av nätverks- (närmast nätverket), internet-, transport- och applikationslager.

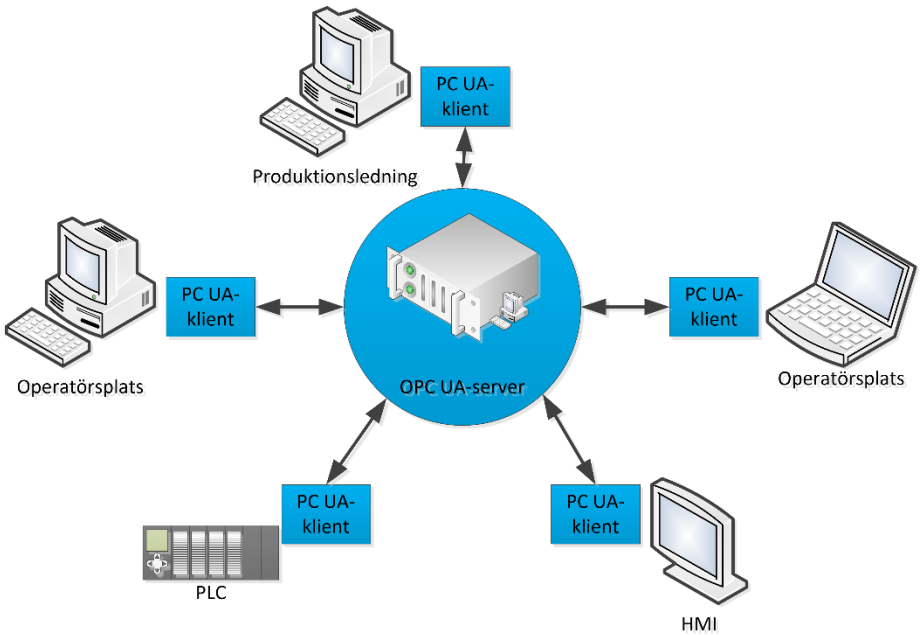
I transportläge är det bara innehållet i paketen som autentiseras och, för ESP krypteras. Vid användande av AH i transportläge så kan inte IP-adresser ändras genom NAT (Network Address Translation) eftersom det omedelbart medför att hashsumman för paketet inte längre stämmer. Behovet av att kunna ändra IP-adresser uppkommer när flera enheter med privata IP-adresser delar på en publik IP-adress. För att hantera detta, exempelvis för IP-telefoni, kan NAT Traversal (NAT-T) användas med AH i transportläge. I tunnelläge krypteras hela IP-paketet, där det krypterade paketet sedan inkapslas i ett nytt IP-paket med en ny IP-header. Tunnelläget används främst för VPN-kommunikation mellan två nätverk.

IPsec kan användas för IPv4 och är tvingande för IPv6 vilket kan komma att bli en nödvändighet då tillgängliga IPv4 adresser är i färd med att ta slut i takt med att allt fler enheter kräver en egen IP-adress (Danielsson, 2015).

Den stora fördelen med IPsec är att det kan appliceras på vilket annat underliggande industriellt protokoll som helst när ESP-protokollet används, eftersom detta protokoll tar meddelandet som ska skickas, paketerar om det genom att lägga paketet i sin helhet i ett nytt IP-paket och skickar iväg det. Detta innebär att ingen konvertering av det industriella protokollet måste utföras innan paketet kan skickas, vilket i sin tur innebär att dyrbar tid sparas.

3.4 OPC UA

Open Platform Communications (OPC) har en relativt lång historia inom industriella informations- och styrsystem. Ursprungligen fanns det en stark koppling till Microsoft och då under namnet OLE for Process Control, men har idag utvecklats till en fristående arkitektur. Den moderna versionen av OPC kallas för OPC Unified Architecture (OPC UA) och är en öppen protokoll-arkitektur för datainsamling och kontroll (Figur 5). Till skillnad från majoriteten av industriella protokoll så innehåller denna arkitektur funktionalitet för informationssäkerhet och inte enbart driftsäkerhet (Eidenskog & Lindahl 2017).

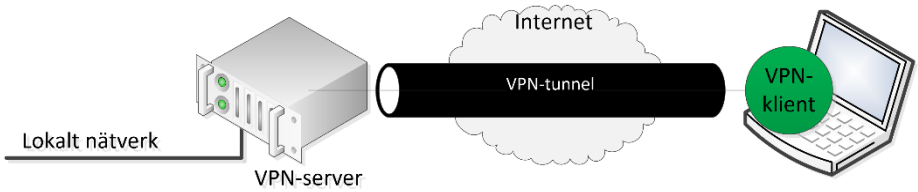


Figur 5 Principbild över OPC UA

De inbyggda säkerhetsfunktionerna omfattar autentisering, kryptering och riktighet via signaturer. Sessionskryptering uppnås genom användning av AES 128 eller 256, det vill säga en symmetrisk krypteringsalgoritm med 128 respektive 256 bitars nyckellängd. Vidare signeras meddelanden för att garantera att meddelanden inte har ändrats under färd. Arkitekturen innehåller funktionalitet för granskning (eng. *audit*) där all aktivitet från både system och användare loggas i spårbarhetssyfte. Det finns även åtkomstkontroller för användare där applikationer kan kräva att användare autentiserar sig med inloggningsuppgifter.

3.5 Fjärranslutning

Virtual Private Network (VPN) är en krypterad förbindelse som etableras genom en fjärranslutningsklient. En sådan klient är i enkla termer en datoranvändare som ansluter till ett privat nätverk från ett externt nätverk. Anslutningen sker till en VPN-server som ger tillgång till resurser på det privata nätverket. Klienten autentiserar sig mot VPN-servern och vice versa.



Figur 6 Principbild över VPN

VPN används ofta inom industriella informations- och styrsystem, bland annat för att tekniker ska kunna ha nödvändig tillgång till enheter för uppdatering, kontroll och statuscheck. Även kontrakterade leverantörer kan behöva tillgång till fjärranslutning.

Det finns flera protokoll för att upprätta en säker kommunikation via VPN, bland annat tidigare nämnda IPsec men även Secure Socket Layer (SSL) och Transport Layer Security (TLS). I IPsec används ESP och tunnelläge för att kryptera hela IP-paket för att på så sätt skydda kommunikationen mot avlyssning och manipulering. Ett SSL/TLS-VPN kräver ingen ytterligare installation av mjukvara utan kryptering sker direkt i en webbläsare. Användaren ansluter och autentiserar sig till en VPN-server som finns lokalt på det nätverk användaren vill ha tillgång till.

En fjärranslutning via VPN löser inte ensamt alla säkerhetsproblem. VPN skyddar data under dess transport, men ändpunkterna kan fortfarande vara sårbara. Om en angripare kan ta kontroll över en av dessa ändpunkter kan även säkert överförd information röjas. En angripare som lyckats installera skadlig kod i en ändpunkt kan sprida denna till andra ändpunkter via VPN-kanalen.

Det är vanligt förekommande att inloggningsuppgifter för dessa anslutningar är statiska, vilket i sig är en sårbarhet och gör arbetet enklare för en angripare. Det har även visat sig att angrepp via fjärranslutning står för mer än 25 % av alla kända källor för penetration av industriella nätverk (Kaspersky 2014)

Användning av VPN bör därför kombineras med flerfaktorautentisering, för att skydda det privata nätverket från angripare. Verksamheten kan skyddas ytterligare genom att använda vitlistning (eng. *whitelisting*), vilken endast tillåter trafik mellan betrodda IP- eller MAC-adresser. Det går även att ange specifika tider på dygnet då VPN-anslutningar ska tillåtas, då det i normalfallet bör vara inom tidsramen för en vanlig arbetsdag. Vidare så bör även tidsspannet för en normal VPN-anslutning undersökas för att upptäcka avvikelser och möjliga intrång.

Förutom VPN är det även vanligt att använda sig av andra former av fjärranslutningar, främst Secure Shell (SSH) eller Remote Desktop Protocol (RDP). RDP är ett nätverksprotokoll som utvecklats av Microsoft och som finns tillgängligt för de flesta versioner av Windows, men även för andra

operativsystem såsom Linux, Android och iOS. Protokollet används för fjärrstyrning av andra enheter i samma lokala nätverk och förser användaren med ett grafiskt gränssnitt av målenheten. Det går även att köra RDP över Internet, men då krävs ytterligare VPN funktionalitet. SSH är ett nätverksprotokoll som används för fjärranslutningar över osäkra nätverk, exempelvis internet. RDP har sin svaghet i bristande autentisering av ändpunkter och är således sårbar för man-i-mitten-angrepp (eng. *Man-in-the-middle attack*). SSH inkluderar däremot möjligheter för multifaktorautentisering och kryptering genom PKI. Trots detta har SSH visat sig vara sårbart då både National Security Agency (NSA) och Central Intelligence Agency (CIA) lyckats snappa upp och dekryptera SSH-sessioner (Spiegel 2014; WikiLeaks 2017).

3.6 Nätverkskryptering

Processen för att kryptera nätverkskommunikation liknar till stor del processen för att kryptera fjärranslutningskommunikation. På en grundläggande nivå är målet detsamma för dessa typer av kommunikation – kryptering av kommunikationen mellan enheter över ett nätverk. Både IPsec- och OPC UA-arkitekturerna stödjer nätverkskryptering. För IPsec beror valet av protokoll och läge på vad som är viktigt att skydda gällande kommunikationen i nätverket; om data är konfidentiell eller om det är riktighet och ursprung som är centralt. För det sistnämnda lämpar det sig väl att använda AH i transportläge och för konfidentialitet är ESP i transportläge det bättre alternativet. Det ska dock nämnas att även ESP går bra att använda för riktighet och ursprungsautenticitet men att detta kan addera onödig fördröjning i kommunikationen om små paket ska krypteras och dekrypteras. För OPC UA används AES 128 eller 256 för sessionskryptering över nätverket, vilket innebär att all kommunikation i sessionen är krypterad.

Flera komponenter inom industriella informations- och styrsystem har inte nödvändig processorkraft för att på rimlig tid köra de matematiska operationer som kryptering och dekryptering innebär. En lösning på detta problem kan vara att implementera kryptografiska integrerade kretsar (IK) i varje enhet som inte klarar av att köra dessa funktioner själva. Detta är dock inte alltid rimligt, varken ekonomiskt eller tidsmässigt, då en verksamhet kan ha väldigt många små sensorer och dylikt som saknar nödvändig processorkraft. Ett alternativ till inbyggda kretsar är att införa ett krypto i en hårdvara i anslutning till styrsystemskomponenten. Detta medför också en kostnad, men inte lika stor som att implementera en kryptografisk IK för varje enhet i nätverket.

Trådlösa nätverk såsom Wi-Fi, är mycket lämpliga att skydda då de inte nödvändigtvis enbart är nåbara inom nätverksägarens faciliteter. Hur långt ifrån en anläggning som ett trådlöst nätverk kan avlyssnas beror på angriparens

utrustning. Nätverkskryptering skyddar både trafiken i det trådlösa nätverket och obehörigt nyttjande av nätverket.

3.7 Lagringskryptering

De data som lagras på hårddiskar och annan lagringsmedia bör i regel vara krypterade för att vara skyddade och därmed minimera konsekvenserna av ett framgångsrikt angrepp på nätverket, stöld eller förlust av hårdvara (NIST 2007; NIST 2013a; Verizon 2018). Verizon (2018) skriver i sin årliga undersökningsrapport för dataintrång att 47 % av alla rapporterade intrång var ett resultat av industrispionage där målet är att komma åt immateriella rättigheter. Detta var dock för tillverkningssektorn, vilket bara utgör en del av de olika sektorer som använder sig av industriella informations- och styrsystem. Vidare är denna rapport inte komplett med alla incidenter som skett under året utan är baserat på företags egna rapporter. Trots det är denna siffra betydande och belyser behovet av hårddiskkryptering, speciellt där data av större värde finns.

4 Utmaningar med kryptering

Kryptografiska funktioner skapar nya utmaningar som en organisation måste hantera för att framgångsrikt implementera och använda dessa funktioner. Detta kapitel presenterar några av de mest framstående utmaningar som en organisations ställs inför gällande kryptering.

4.1 Nyckelhantering

Effektiviteten i kryptografiska lösningar påverkas till stor del av nyckelhanteringen. Förlorade eller avslöjade nycklar har stor påverkan på symmetriska funktioner eftersom en röjd nyckel kan kräva att alla nycklar i nätverket måste bytas. Detta kan snabbt bli en belastning för verksamheter där ett stort antal enheter delar samma symmetriska nyckel. Ur ett konfidentialitetsperspektiv behöver även nycklar bytas ut regelbundet, för att undvika att mycket information blir tillgänglig om en nyckel röjs. En organisation som använder kryptografiska lösningar måste även effektivt kunna generera nya nycklar, distribuera, använda och lagra dessa på ett säkert sätt. Detta gäller även för asymmetrisk kryptering, dock med ökad komplexitet då varje enhet har två nycklar, som dessutom är relaterade till varandra.

Nyckelhantering kan utföras på flera olika sätt, men de flesta metoder (NIST 2012a; NIST 2013b; NIST 2016; OWASP 2018) för detta innehåller följande steg (med varierande namn): generering, distribution, lagring, säkerhetskopiering, revokering samt destruktion.

Generering avser hur nycklar skapas, exempelvis vilken algoritm och nyckellängd som ska användas. Det är viktigt att organisationen förstår syftet med användandet av den kryptografiska funktionen. Exempelvis, om syftet är att skydda konfidentialitet för data i rörelse, så bör en algoritmuppsättning som stödjer skyddandet av just data i rörelse väljas. Först när en förståelse finns för syftet är det möjligt att gå vidare med att faktiskt bestämma vilket protokoll eller vilken algoritm som bör användas för att uppnå syftet. Detta skulle i det tidigare exemplet troligtvis innebära en algoritmuppsättning för att stödja användandet av både symmetriska och asymmetriska krypteringsnycklar för respektive algoritmer. Avseende själva genereringen av nycklar så bör alla värden som behövs för detta skapas inom den nyckelgenererande modulen. På så sätt har inga slumptal, initieringsvärden eller andra attribut som används för att skapa nyckeln sitt ursprung utanför den nyckelgenererande modulen.

För att enheterna i ett nätverk ska kunna ta del av och använda de genererade nycklarna krävs det att de på något sätt får tillgång till dem från det centrala nyckelhanteringssystemet. Ett centralt skapat nyckelpar får endast distribueras till den tänkta ägaren av nyckelparet och får endast vara känt av den skapande

entiteten samt ägaren. Asymmetriska nyckelpar och symmetriska hemliga nycklar kan distribueras på samma sätt. Detta bör antingen göras manuellt eller via ett säkert kommunikationsprotokoll, såsom IPsec. Med *manuellt* avses en fysisk överföring av ett digitalt medium, exempelvis ett USB-minne, vilket innebär att nyckeln överförs till detta medium och sedan transporteras av mänsklig hand till enheten som är den tänkta ägaren. Symmetriska nycklar kan även delas som sessionsnycklar genom användande av ett redan etablerat asymmetriskt nyckelpar. Nycklar som genereras lokalt på en enhet för kryptering av lagringsmedia bör inte distribueras, med undantag för en backup-entitet eller auktoriserade entiteter som behöver tillgång till lagringsinnehållet.

Utöver säker generering och distribuering är det även viktigt att nycklar skyddas i lagringsmedia för att förhindra röjande. Nycklar måste lagras på ett säkert sätt hos både det centrala nyckelhanteringssystemet och hos de enheter dit nycklarna är distribuerade, i både beständiga och flyktiga minnen. Det är här viktigt att tänka på att nycklar aldrig bör lagras i klartext, att riktigheten hos nycklarna måste skyddas, samt att nycklarna och all form av användande av dessa utförs i ett kryptografiskt valv. Kod på applikationsnivå bör aldrig tillåtas att läsa eller använda kryptografiska nycklar.

Data som krypterats med en nyckel som gått förlorad kan aldrig återfås (i rimlig tid). Det är därför lämpligt att överväga säkerhetskopiering av nycklar hos en betrodd tredje part. Detta bör speciellt övervägas för krypterad data som är tänkt att lagras under lång tid. Däremot bör säkerhetskopiering av en tredje entitet aldrig utföras på nycklar som används för digitala signaturer.

När en nyckel når slutet av sin giltighetstid bör alla instanser av den nyckeln och dess metadata förstöras för att minimera risken att obehöriga får tillgång till nyckeln eller delar av den i ett försök att återskapa information som krypterats med nyckeln i fråga. Nycklar måste förstöras på ett sådant sätt att inga spår av nyckeln eller dess beståndsdelar går att återskapa. Det räcker sällan att bara radera nyckeln från minnet. Det krävs även att de delar i minnet där nyckeln lagrats skrivs över (ibland flera gånger). Detta görs vanligen genom att skriva över dessa minnesplatser med orelaterad information som exempelvis en sträng av slumpmässiga bitar.

Det är ibland nödvändigt att återkalla en nyckel från en användare innan nyckelns livslängd är över. Detta kan exempelvis bero på att nyckeln är röjd eller att en användare har lämnat organisationen. Återkallandet kan uppnås genom att det centrala nyckelhanteringssystemet skickar notifikationer till berörda användare, alltså de användare vars nycklar återkallats. Ett återkallande kan även initieras av användare genom en begäran av återkallande (eng. *revocation request*). Om en nyckel har använts för kommunikation mellan två enheter så bör båda användarna notifieras om att nyckeln inte längre ska användas. För situationer där en användare har lämnat organisationen och fått sin nyckel återkallad, är det viktigt att överväga om signeringar som utförts innan

återkallandet fortfarande bör gälla. Om en privat nyckel i ett nyckelpar visar sig vara röjd bör det (efter återkallande av både privat och publik nyckel) istället övervägas om någon signerad information alls bör gälla. För certifikat uppnås återkallande eller dissociation generellt genom så kallade revokeringslistor där återkallade certifikat adderas till listan.

Sammantaget kan sägas att det inte bara är viktigt att skapa säkra nycklar, utan att nycklar även kräver skydd och omhändertagande under hela sin livslängd för att inte riskera att underminera den tänkta säkerheten med användandet. För att hantera alla dessa faktorer används ofta ett komplett nyckelhanteringssystem eller ett kryptografiskt nyckelhanteringssystem. Vid en sådan implementation behöver organisationen och verksamheten i fråga definiera, utveckla och förstå hur detta system är tänkt att fungera. Brister i någon av dessa delar kan underminera hela konceptet med nycklar och kryptografiska funktioner.

4.2 Implementation och kvalitetssäkring

Tilltron till kryptografiska lösningar bygger på hur väl kryptografiska lösningar är implementerade och hur de interagerar med övriga system. Felaktiga implementationer riskerar ge en falsk säkerhet samtidigt som antagonister har möjlighet att utnyttja svagheter i systemet. (Saltzer & Shroeder 1975).

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 det att programmet är funktionellt korrekt (Ferguson, Schneier & Kohno, 2011).

Logiska fel i implementationen av kryptografiska funktioner är ett annat problem som måste beaktas. I denna mening innebär logiska fel att organisationen i sig. eller de leverantörer som förser systemet med ny funktionalitet i form av en kryptografisk funktion, inte helt har förstått hur systemet egentligen fungerar. Detta kan leda till oförutsedd funktionalitet där enheter gör eller kan göra saker som de egentligen inte borde kunna. Det kan också leda till att systemet eller delar av systemet inte fungerar som det ska, exempelvis om en kommunikationslinje blockerats mellan två enheter som behöver kommunicera.

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).

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 medföra stora konsekvenser för hela systemets säkerhet. Enligt Kaspersky (2014) var så mycket som 23 % av alla incidenter i industriella informations- och styrsystem ett resultat av mjukvarufel. Vidare är det inte alltid lämpligt eller ens möjligt att implementera kryptografiska funktioner i ett industriellt informations- och styrsystem. Framförallt gäller detta tidskritiska system som kräver att information kan visas i realtid. Alla delsystem inom nätverket kan inte nödvändigtvis hantera kryptografiska funktioner, på grund av låg processorkraft.

Intern säkerhetsövervakning av ett system är nödvändigt för att upptäcka och hantera incidenter. Krypterad datakommunikation försvårarar övervakningen genom att trafiken är oläsbar även för de som övervakar. Krypterad trafik internt medför också att lastbalansering och annan intern optimering omöjliggörs.

Som nämnt ett antal gånger i detta kapitel, påverkas kryptografiska funktioners effektivitet av kvaliteten på den kryptografiska algoritm som används. Algoritmer som med tiden visat sig vara osäkra bör till stor grad undvikas då dessa direkt medför en negativ förändring i säkerheten och förmågan hos den kryptografiska funktionen. Det finns även exempel på organisationer som tagit sig an att utveckla sina egna kryptografiska algoritmer. Detta är generellt inte att rekommendera, då det krävs mycket kunskap att utveckla kryptografiska lösningar. En leverantör tjänar inte heller på att försöka dölja vilken lösning som tagits fram. En grundregel inom kryptografiska lösningar är att de ska utsättas för så mycket granskning som möjligt. Styrkan i en kryptografisk funktion ska alltid ligga i nyckeln, inte kunskapen om vilken algoritm eller implementation som används. Det mest rekommenderade alternativet är att förhålla sig till beprövade och rekommenderade algoritmer och arkitekturer då dessa hela tiden testas och utvecklas för att försäkra sig om att säkerheten håller (Ferguson, Schneier & Kohno 2011).

5 Intervjuresultat: Industriperspektiv på kryptografiska funktioner

I detta kapitel redovisas resultat från genomförda intervjuer. Respondenter är valda ifrån tre branscher med olika skyddsbehov. Syftet med intervjuerna var att identifiera vilka behov av kryptografiska funktioner som finns gällande industriella informations- och styrsystem. Den intervjuguide som används och som resultatet är strukturerat efter, återfinns i Bilaga A Kommentarer från de olika respondenterna presenteras som [resp. X]. Denna anonymisering beror främst på att det inte är relevant för resultatet att presentera vilka organisationer som deltagit i intervjuerna och vem som sagt vad.

5.1 Hotbild

Vilka hot som industriella informations- och styrsystem kan utsättas för varierar mycket mellan branscher. Mycket av skillnaderna är naturliga, beroende på hur exponerat systemet är både fysiskt och logiskt. Geografiskt spridda system som är obevakade har en högre risk för att utsättas för fysiska hot [resp. 2] medan logiskt exponerade sårbarheter är mer utsatta för opportunistiska angrepp. I det sista fallet vet kanske inte ens angriparen vad det är för typ av system som angrips eller var det finns [resp. 1]. För verksamheter med en hög grad av logisk separation från omvärlden är fysiska hot en större risk [resp. 3].

Ett av de största hoten bedöms komma ifrån insiders, det vill säga anställda eller konsuler med hög kunskap om hur systemen fungerar [resp. 2]. Även om mycket information om systemen kan vara publik, särskilt för statliga aktörer, så har insidern ofta ytterligare kunskaper om och behörigheter i systemen [resp. 2].

De konsekvenser ett angrepp kan få beror givetvis också på vilken bransch som angrips och vad systemet gör. En annan aspekt för konsekvenser av ett angrepp är den lokala miljön som det angripna systemet verkar inom [resp. 1]. I en miljö med en hög fysisk hotbild kan ett hot gälla både de människor som systemen är till för, men även för de som fysiskt behöver vara på plats för att åtgärda fel.

Något som normalt inte brukar räknas till hotbilden är kunskap om hot och vidtagna åtgärder [resp. 1]. Bristande kunskap kan dock få stora konsekvenser för systemen, vilket medför ett verksamhetshot.

5.2 Trafik

Datatrafik som går utanför egna nätverk är krypterad, vanligtvis via VPN, men andra lösningar förekommer också [resp. 1, 2, 3]. Den interna trafiken över egna nätverk är oftast inte krypterad i syfte att kunna övervaka datatrafiken [resp. 3].

För leverantörer är situationen lite annorlunda då de under ett supportavtal vill skydda trafiken till och från den produkt som levererats. För att så långt som möjligt säkerhetsställa att den levererade produkten inte kommer att utgöra en attackyta krypteras trafiken mellan leverantören och fram till aktuellt system, exempelvis en PLC [resp. 1].

Lokal trådlös kommunikation används i viss utsträckning. En bransch beskriver möjlighet för trådlös kommunikation inom den egna verksamheten under kortare tid. Kommunikationens spridning begränsas av byggnadens omgivande fysiska arkitektur [resp. 3]. Samma respondent applicerar även segmentering av nätverk i så kallade informationsöar. Dessa öar kan fungera oberoende av varandra under en begränsad tid om kommunikationen mellan dem skulle brytas.

5.3 Tillgångar

Tolkningen av denna fråga verkar skilja sig något mellan de tillfrågade. Exempelvis uttrycker en respondent att de innehar multipla styrsystem, informationssystem med mera [resp. 2]; medan en annan respondent svarar att de innehar ett eget PKI för särskilt viktiga inloggningar i vissa system [resp. 3]. En respondent uttrycker alltså vilka system de innehar och en annan beskriver en arkitektur. En av respondenterna beskrev att leverantörer ibland måste vara på plats för att hantera delar av system eftersom organisationen i fråga inte har rätt att göra det själv, men tillåter samtidigt inte att hanteringen görs från distans [resp. 2].

Från leverantörshåll utrycks ett tredjepartsberoende i en begränsad valmöjlighet av hårdvara för sina produkter. Exempelvis finns det väldigt få tillverkare av chipsets för de produkter som utvecklas för industriella informations- och styrsystem. [resp. 1] ser även en begränsning och ett beroende i bristande dokumentation av delkomponenter och mjukvara. Exempelvis finns ingen publik dokumentation för en nyckelhanteringsmjukvara de använder, vilket leder till begränsad förmåga att nyttja mjukvaran effektivt

5.4 Egna kryptolösningar i era system?

Data inne i det egna nätverket krypteras inte eftersom det försvårar övervakning [resp. 2, 3]. Respondenterna ser även att autentisering av meddelanden och aktör är viktigare än konfidentialitet internt och använder därför, i viss utsträckning, kryptografiska hashfunktioner [resp. 2, 3]. Leverantörer å andra sidan lägger fokus på att deras enheter inte blir en attackyta för antagonister och använder, i detta fall, en VPN-box i direkt anslutning till de egna enheterna samt certifikat [resp. 1]. Från ett branschperspektiv upplevs leverantörerna och den interna inköpsorganisationen styra mycket av säkerhetstänkandet och att mycket av detta tänk sker ur ett Safety-perspektiv [resp. 2].

Som ett exempel på behov av autentisering inom nätverk beskrevs ett sensorsystem där mottagarsystemet inte kan avgöra ifrån vilken sensor data kommer. Det handlade om en grupp av sensorer som inte kan identifiera sig gentemot mottagarsystemet, varvid systemoperatören endast kan få en grov uppfattning om vad sensordatan kan betyda. Autentisering av avsändare är en viktig aspekt av kommunikationen [resp.1].

5.5 Framtida förändringar avseende krypto

Det är tydligt att både operatörer och leverantörer vill se tydligare vägledning och riktlinjer i framtiden, då föreskrifter och krav från myndigheter upplevs vara föråldrade jämfört med den tekniska utvecklingen [resp. 1, 3]. Vidare ses kryptografiska funktioner inte heller som lämpade för vissa delar av dessa system i framtiden. Detta eftersom processorkraften hos en del enheter inte räcker till och att dessa kryptografiska funktioner introducerar en fördröjning som inte är acceptabel i systemet [resp. 1, 2,]. Det ses heller inte som nödvändigt att inkludera kryptografiska funktioner på datatrafiken i det industriella nätverket (OT). Autentisering ses istället som det viktigaste och mest kritiska att åtgärda [resp. 2,3]. Dock skulle kryptering av datatrafiken på kontorssidan vara intressant [resp. 2].

Från operatörsperspektiv upplevs att säkerhetsutveckling är kopplat till leverantörer och skiljer sig mellan olika leverantörer [resp. 2]. Samtidigt önskar mans från leverantörsperspektiv en övergång från certifierade produkter till producentansvar eftersom certifiering ofta är bristfällig samt skapar problem och ökad kostnad när andra leverantörer kommer in och måste hantera den otillräckliga produkten [resp. 1]. En respondent beskrev ett behov av kortare livscykler för systemen för att passa bättre med IT-livscykeln [resp. 2].

En av de tillfrågade operatörerna ser en ökad IP-baserad kommunikation som positivt medan den andra operatören såg säkerhetsmässiga fördelar med att låta viss trafik vara seriell [resp. 2, 3]. Detta kan bero på att dessa branscher skiljer sig stort i geografisk utspridning och att det då är enklare att övergå helt till IP-baserad kommunikation inom ett litet kontrollerat område. En annan skillnad mellan de tillfrågade operatörerna är frågan om molnbaserad data, där den ena operatören ser detta som något positivt och hos den andra operatören ser detta mer som en utmaning.

Avseende framtida angrepp förutspås en ökad frekvens av angrepp mot PLC:er, specifikt ses utpressningsmjukvara som ett stort potentiellt hot [resp. 1].

6 Diskussion

Den upplevda hotbilden hos respondenterna är fokuserad på en eller ett fåtal av de aktörer som finns listade i rapportens generella hotbild (avsnitt 2.1). Respondenterna har prioriterat sin hotbildsanalys efter de hot som upplevs som mest sannolika.

Operatörsrespondenterna ser kryptering av intern datatrafik som onödig och i många fall olämplig eftersom kryptering försvårar övervakning av den interna trafiken. I vissa fall går det dessutom inte att applicera kryptografiska funktioner då vissa enheter har begränsad processorkraft och därför inte kan utföra komplicerade kryptografiska beräkningar i rimlig tid. Därutöver innebär kryptering även generellt en fördröjning av kommunikationen, vilket i många fall inom detta område är oacceptabelt. Det kan även ses som överflödigt att kryptera styrsignaler och mätdata som utgör majoriteten av kommunikation i dessa nätverk då dessa för verksamheten inte innehåller särskilt signifikativ eller skyddsvärd information.

Det är dock möjligt att kryptera de interna nätverken, exempelvis genom introduktionen av ett säkert kommunikationsprotokoll. De två protokoll som beskrevs i avsnitt 3.3 (IPsec) och 3.4 (OPC UA) kan båda appliceras för detta ändamål. Dock, kräver OPC UA en omstrukturering av kommunikationsarkitekturen då det är tänkt att ersätta ett eller flera redan existerande protokoll. IPsec kräver däremot ingen omstrukturering då det kan appliceras som ett lager ovanpå existerande protokoll. Paketen som skickas kapslas då in i ett nytt krypterat IP-paket innan de sänds iväg. För större existerande anläggningar lämpar sig IPsec bättre då kostnaden, både ekonomiskt och tidsmässigt, att implementera OPC UA på alla enheter troligtvis blir mycket hög. För mindre eller nya anläggningar kan OPC UA vara ett bättre alternativ eftersom det är ett protokoll som ligger på industriell nivå och inte utgör ett extra lager som läggs ovanpå existerande protokoll.

Om en organisation innehar trådlösa interna nätverk utöver trådade interna nätverket, är det viktigt att dessa behandlas olika säkerhetsmässigt. Anledningen är att trådlösa nätverk i regel är mer lättåtkomliga än trådade nätverk. Trådade nätverk kräver fysisk åtkomst eller tillgång till en enhet på det interna nätverket för att en angripare ska kunna läsa eller ändra data. Med trådlöst behöver angriparen istället bara vara inom räckhåll för den trådlösa kommunikationen. Det även vanligt att trådlösa nätverk bristfälligt konfigurerade ur säkerhetssynpunkt i syfte att underlätta för användare och administratörer. Kryptering rekommenderas därför för dessa trådlösa nätverk för att skydda innehållet i trafiken. Utöver kryptering är det även viktigt att regelbundet övervaka och skanna nätverket för att upptäcka angrepp och sårbarheter, exempelvis i form av oregelbunden nätverkstrafik, obehöriga accesspunkter eller felkonfigurerade enheter (NIST 2012b).

Behovsmässigt får kryptering och konfidentialitet ge vika för riktighet och autentisering av meddelanden och aktörer. Autentisering ses generellt hos branscherna som den viktigaste och mest kritiska säkerhetsåtgärden i de interna nätverken. Det är kritiskt att försäkra sig om att innehållet i den kommunikation som skickas inte ändrats under färd och att säkerställa vem avsändaren är. Kryptografiska funktioner kan användas även för detta ändamål i exempelvis kryptografiska hashfunktioner eller digitala signaturer (certifikat). Tillämpning av dessa typer av funktioner kräver användandet av rekommenderade hashfunktioner (exempelvis SHA-2 256 eller SHA-3) eller de facto-standard certifikat (X.509) för att användandet av funktionerna ska höja säkerheten i kommunikationen.

För leverantörer skiljer sig perspektivet något, då det för dem är viktigt att säkerställa att de egna produkterna inte blir en attackyta hos kunden. Därför vill leverantören gärna kryptera all kommunikation som går från det egna nätverket ända fram till produkterna hos kunder. Denna kommunikation blir ett mellanting mellan extern och intern kommunikation, men eftersom kommunikationen kommer utifrån kundens nätverk kan den i det avseendet ses som extern. Samtidigt går kommunikationen in i det interna nätverket hos kunden (beroende på vilket nätverk produkten tillhör), vilket leder till att kommunikationen kan klassas som intern, vilket i sin tur betyder att kunden ogärna vill att den ska vara krypterad då de vill kunna övervaka innebörden av kommunikationen. Det finns flera tänkbara kompromisser för att lösa denna motsättning, ett exempel är att kryptera fram till kundens interna nätverk, dekryptera kommunikationen och skicka den vidare till produkten. En annan kompromiss är att den krypterade leverantörskommunikationen manuellt måste släppas igenom brandväggen av kunden genom begäran från leverantör över telefon eller dylikt. En av branschrespondenterna uttryckte dock att de inte tillät leverantörer att utföra underhåll med fjärranslutning, istället var leverantören tvungen att vara på plats för att utföra underhållsarbete.

Till skillnad från intern kommunikation så ses kryptering av extern kommunikation som en nödvändighet av både operatörer och leverantörer. Resultatet av intervjuerna har dock inte visat vilken typ av kryptering som används för denna kommunikation, undantaget den intervjuade leverantören som använder en VPN-box och certifikat.

Kryptering av lagrad data har inte diskuterats under någon av de genomförda intervjuerna. Trots det rekommenderas det starkt att kryptera denna typ av data (NIST 2007: NIST 2013a: Verizon 2018). Eftersom data i denna form har lägre krav på tillgänglighet än data i rörelse, är den fördröjning som kryptering medför acceptabel. Denna typ av kryptering, vilken är särskilt lämplig för bärbara datorer, förhindrar att otillbörliga får tillgång till att läsa lagrad data och försvårar således även industrispionage.

Internetsökningar hos de största leverantörerna för industriella informations- och styrsystem har visat ett väldigt begränsat utbud av kryptografiska funktioner i de erbjudna lösningarna. Det är oklart om detta beror på bristande efterfrågan hos kunder eller om leverantörerna själva inte har kapacitet eller vilja att erbjuda kryptografiska lösningar. En operatörsrespondent ansåg att dennes inköps-organisation stod för mycket av säkerhetstänkandet för nya produkter och att dessa ofta var mer inriktade på *safety*-aspekter snarare än cybersäkerhet.

Det finns heller inga specifika krav i lagar eller föreskrifter om kryptografiska funktioner med avseende på industriella informations- och styrsystem, vilket också kan vara en bidragande faktor till det begränsade utbudet.

När det gäller framtiden är det tydligt att både operatörer och leverantörer vill ha tydligare vägledning och riktlinjer eftersom dagens föreskrifter och myndighets-krav ligger efter den tekniska utvecklingen.

De senaste årens utpressningsattacker har för en respondent fört med sig en tro om att dessa attacker inom en snar framtid även kommer riktas mot industriella informations- och styrsystem. Utpressningsattacker riktade mot PLC:er ses som ett särskilt hot.

7 Slutsats

Målet för denna studie var att undersöka behovet och nyttjandet av kryptografiska funktioner inom industriella informations- och styrsystem samt visa vilka kryptografiska funktioner som är lämpliga att använda i dessa typer av system.

All trafik som färdas externt från de interna nätverken över osäkra nätverk, såsom internet, bör i regel krypteras. I dessa fall ska konfidentialitet värderas högt, det vill säga att kommunikation inte kan läsas av obehöriga. Det är även möjligt att kryptera trafiken i de interna nätverken exempelvis genom implementation av ett av de två protokoll som beskrivits i avsnitt 3.3 (IPsec) respektive 3.4 (OPC UA). Respondenterna motsatte sig dock kryptering av trafiken i de interna nätverken till stor del på grund av att det avsevärt försvårar övervakning av kommunikationen i nätverken. Autentisering identifierades istället av respondenterna som den viktigaste säkerhetsaspekten för de interna nätverken. Kryptografiska funktioner kan användas även för detta ändamål exempelvis genom kryptografiska hashfunktioner eller digitala signaturer. Det är även nödvändigt att hantera trådlösa och trådade interna nätverk på olika sätt säkerhetsmässigt då de trådlösa nätverken är mer lättåtkomliga för en angripare och kräver således starkare skydd. Vidare rekommenderas kryptering av lagrad (vilande) data starkt. Den fördröjning som introduceras genom kryptering av denna typ av data är acceptabel på grund av lägre krav på tillgänglighet än för data i rörelse.

Det är oklart hur framtiden för kryptografiska funktioner i industriella informations- och styrsystem kan komma att utvecklas. I nuläget specificerar existerande lagar, förordningar, föreskrifter, standarder och rekommendationer vilken data och trafik som bör skyddas, men det finns få konkreta exempel på vilka funktioner som faktiskt ska användas i detta syfte. Det finns inga specifika krav på att kryptografiska funktioner ska användas för att hantera specifika situationer, bara att de kan användas. NIS-direktivets implementation kan komma att ändra detta, men det klargörs dock först när direktivet träder i kraft.

Sammantaget kan sägas att denna rapport visar att kryptering av extern kommunikation och vilande data bör appliceras. Kryptering av trafiken i interna nätverk är möjlig att genomföra, men skulle försvåra övervakning. Riktighet och autenticitet ses istället som kritiskt för de interna nätverken och kryptografiska funktioner kan även användas för detta ändamål.

Referenser

Butler, J.M. (2012). *Privileged Password Sharing: "root" of All Evil.* SANS.

Cornell, D. (2007). Properties of Secure Hash Functions. *Denim Group* [blogg], 21 november. https://denimgroup.com/resources/blog/2007/11/properties-of-1/ [2018-02-25]

Danielsson, L. (2015). Nu är ip-adresserna slut på riktigt – åtminstone i Nordamerika. *Computer Sweden*, 25 september. https://computersweden.idg.se/2.2683/1.637961/ipv4 [2018-02-25]

Eidenskog, D. & Lindahl, B. (2017). *NCS3 - Industriella protokoll i Sverige - en översikt över protokoll inom industriella informations- och styrsystem i kritisk infrastruktur* (FOI-R--4438--SE). Stockholm: FOI.

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

International Society of Automation (ISA) (u.å.). *ISA99, Industrial Automation and Control Systems Security*. https://www.isa.org/isa99/ [2018-05-20]

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

Lagner, R. (2013). *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tries to Achieve.*

Macaskill, E. & Dance, G. (2013). NSA Files: Decoded. *The Guardian*, 1 november. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [2018-05-18]

Myndigheten för samhällsskydd och beredskap (MSB) (2014). *Vägledning till ökad säkerhet i industriella informations- och styrsystem*. Stockholm: MSB.

National Institute of Standards and Technology (NIST) (2007). *SP800-111 Guide to Storage Encryption Technologies for End User Devices* (SP800-111). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2012a). *SP800-133 Recommendation for Cryptographic Key Generation* (SP800-133). Gaithersburg: NIST.

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

National Institute of Standards and Technology (NIST) (2013a). *SP800-53 Security and Privacy Controls for Federal Information Systems and Organizations* (SP800-53r4). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2013b). *SP800-130 A Framework for Designing Cryptographic Key Management Systems* (SP800-130). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2015a). *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) (2015b). *SP800-82 Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)* (SP800-82r2). Gaithersburg: NIST.

National Institute of Standards and Technology (NIST) (2016). *SP800-57 Recommendation for Key Management, Part 1: General* (SP800-57, pt.1, rev.4). Gaithersburg: NIST.

NIS-utredningen (2017). *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36). Stockholm: Justitiedepartementet.

OWASP (2018) Key Management Cheat Sheet. *OWASP* [Wiki], 1 mars. https://www.owasp.org/index.php/Key_Management_Cheat_Sheet [2018-04-10]

Richter, M. (2017). To Pay or Not to Pay? Lessons from the Uber Cyber Attack. *Assurance Software* [blogg], 30 november. http://www.assurancesoftware.com/product-blog/to-pay-or-not-to-pay-lessons-from-the-uber-cyber-attack [2018-02-19]

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

Sanchez, G. (2015). *Case Study: Critical Controls that Sony Should Have Implemented.* SANS.

Swedish Standard Institute (SIS) (u.å.). *ISO 27 000 Informationssäkerhet.* https://www.sis.se/iso27000/ [2018-05-20]

Spiegel (2014). Inside the NSA's War on Internet Security. *Spiegel Online*, 28 december. http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [2018-02-19]

Stevens, M., Bursztein, E., Karpman, P., Albertini, A. & Markov, Y. (2017). The first collision for full SHA-1. I *Proceedings from Crypto 2017 - 37th Annual*

International Cryptology Conference. Santa Barbara (CA), USA 20–24 augusti, ss. 570-596. https://eprint.iacr.org/2017/190.pdf

Svenska Kraftnät (SvK) (2010). *Tekniska riktlinjer IT-säkerhet* (TR4-02). https://www.svk.se/siteassets/aktorsportalen/tekniska-riktlinjer/tr04/1tr-4-02-b.pdf

Svenska Kraftnät (SvK) (2015). *IT-säkerhetsarkitektur - En vägledning för elbranschen med typexempel och referenslösningar*. https://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-it-sakerhetsarkitektur-final.pdf

Verizon (2018). 2018 Data Breach Investigations Report, 11 uppl. https://www.verizonenterprise.com/verizon-insights-lab/dbir/

WikiLeaks (2017). WikiLeaks - Vault 7: BothanSpy. *WikiLeaks*, 6 juli. https://www.wikileaks.org/vault7/#BothanSpy [2018-02-19]

WP Engine (2015). *Unmasked: What 10 million passwords reveal about the people who choose them*. https://wpengine.com/unmasked/ [2018-02-23]

Bilaga A. Intervjufrågor

Syftet med studien är att öka kunskapen om möjligheterna att tillämpa kryptografiska funktioner inom industriella informations- och styrsystem.

Målet med studien är att ge en kunskapsöversikt över möjligheter och problem vad gäller kryptografiska funktioner av information inom användningsområdet industriella informations- och styrsystem.

Studien ska svara på vilka kryptografiska lösningar som är lämpliga för industriella informations- och styrsystem.

A.1. Om respondenten

- Namn
- Roll/befattning
- Organisationens uppgift

A.2. Tillgångar

- Vilka tillgångar är kritiska för er verksamhet? (Process, System, Information?)
- Finns några av de kritiska tillgångarna utanför era egna nätverk (ex. en molnlösning)? [Jmf. med ISA-95-arkitektur.]
- Finns några av de kritiska tillgångarna utanför era egna nätverk (3-partberoenden)?

A.3. Trafik

- Går någon datortrafik utanför era egna nätverk?
- Hur säkerställs att det är rätt sändare/mottagare?

A.4. Hotbild

- Vilka hot ser du mot ICS?

A.5. Egna lösningar alt. används kryptolösningar i era system?

- För sekretess?
    - Trafik
    - Egen trafik över externa kanaler?
    - Trafik från underleverantörer?
    - Intern trafik
        - Mellan affärs- och övervakningssystem (lager 4-3)? [Jmf. scada/dcs]
        - Mellan övervakning och kontrollsystem (lager 3-2)? [Jmf. scada/dcs]
    - System
    - Information
        - End-to-end
- För riktighet?
    - Kryptolösningar för riktighet?
    - Kryptolösningar för hashvärden?
    - Korrekthetskontroll utan kryptolösningar (sha/md, hash)
- För autentisering?
    - 2-faktorautentisering
    - Certifikat
    - Behörighetssystem
- Erfarenheter
    - Införande
    - Drift

A.6. Framtida förändringar avseende krypto

(Öppen frågeställning)

A.7. Om kryptering

- Behov/krav
    - Finns det behov av att skydda information/kommunikation inom ICS?
        - Nutid?
        - I framtiden?
    - Ställs det krav på skydd av information inom er bransch?
        - Svensk lag?
        - Branschreglering?
    - Finns det fall då kryptering är olämpligt även om behov finns?
    - Finns/används alternativa lösningar till kryptering?
- Aktuellt ämne?
    - Diskuteras kryptering, exempelvis av säljare eller myndigheter?

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