Svenskt signalskydd i dåtid, nutid och framtid

Inträdesanförande i KKrVa avd IV den 10 september 2014 av Pia Gruvö

Résumé

The article describes what communications security is and why the field of encryption has an exceptional position in most nations. It also gives an account of how the Swedish communications security has evolved from the cipher wheel of the early 1900's to today's advanced network crypto systems. The address gives an insight into the challenges with today's technology and complex systems along with the challenges that follow with the international collaborations that the Armed Forces are a part of. Finally, a few thoughts are presented on what the future of communications security may come to look like.

HÖSTEN 1987 ERHÖLL jag min magisterexamen i matematik med inriktning mot matematisk statistik i Lund. Jag skulle flytta till Stockholm och hittade två jobb lämpliga för en matematiker – aktuarie på Folksam och kryptolog på Totalförsvarets Signalskyddsavdelning, TSA, i Försvarsmaktens högkvarter. Båda dessa områden var okända för mig och (som tur var) fick jag svar att jag erhållit jobbet från TSA först. I februari 1988 påbörjade jag min anställning och befann mig plötsligt i en mycket intressant omgivning med kunniga människor och ett väldigt spännande ämnesområde. Signalskydd visade sig innehålla matematik, teknik, regelverk, design, politik, diplomati och mycket annat. Jag är fortfarande kvar på samma arbetsplats och det är fortfarande lika spännande.

Signalskydd är, enligt vår definition, åtgärder som syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder. Den tekniska lösningen kallas signalskyddssystem och indelas i

- system med kryptografiska funktioner för att skydda information som är hemlig med avseende på rikets säkerhet,
- system för skydd mot signalunderrättelsetjänst, störsändning eller falsk signalering med den samlande benämning trafikskydd.

Artikeln handlar om det förstnämnda, d v s signalskydd i form av kryptosystem och hur detta område har utvecklats genom åren fram till idag samt även innehålla några tankar om framtiden.

Jag gissar att det flesta numera är bekanta med begreppet krypto. Från att ha varit en teknik som endast användes inom det militära försvaret, i diplomatiska kretsar samt i underrättelsetjänsternas agentverksamhet så är det idag en teknik som vi alla använder vare sig vi är medvetna om det eller inte. Så fort vi betalar på nätet eller använder vår internetbank så använder vi oss av en krypterad förbindelse. Det grund-

läggande syftet är att någon som avlyssnar trafiken ska inte kunna läsa denna i så kallad klartext. Med hjälp av en kryptonyckel och en kryptoalgoritm omvandlas klartexten till kryptotext och endast den som har tillgång till aktuell kryptonyckel ska kunna läsa klartexten. Kryptoalgoritmen kan vara hemlig men systemets säkerhet ska, enligt Kerckhoffs princip från 1883,[1] endast bygga på att själva kryptonyckeln är hemlig.

En säker kryptoalgoritm innebär att det enda sättet att knäcka kryptot är att prova igenom alla tänkbara kryptonycklar. Därför är kryptonyckelns längd av största vikt och idag gäller nyckellängder på 192 ”bitar” eller mer vilket innebär 2^{192} nycklar att prova igenom. Detta är ett så stort tal så det är en omöjlig uppgift. En svaghet i algoritmen kan dock minska antalet nycklar att prova igenom. Det enda kryptosystemet som bevisligen inte går att forcera är s k engångskrypto. Varje bit klartext adderas modulärt till en bit av kryptonyckeln, som då blir lika lång som kryptotexten. Så länge som kryptonyckeln är slumpmässig och endast används en gång är kryptot icke forcerbart.

Traditionellt har symmetriska kryptoalgoritmer använts vilket innebär att sändare och mottagare har tillgång till samma hemliga kryptonyckel. Sedan 1980-talet har dock mer och mer asymmetriska algoritmer kommit till användning. Dessa bygger på en publik/öppen nyckel för kryptering och en privat/hemlig nyckel för dekryptering. Här är det andra nyckellängder som gäller såsom 2048 eller 4096 bitar. Alla bra sådana kryptoalgoritmer bygger dock på avancerad matematik som tämligen få matematiker till fullo behärskar.

Forcering av kryptosystem har haft stor betydelse för händelseförlopp i världshistorien i hundratals år och har det än idag. Kryptoområdet har i de flesta nationer en särställning och omgärdas av speciella regelverk. Det finns flera anledningar till detta:

- Ett dåligt konstruerat kryptosystem kan ge enorm skada utan att det märks. Detta skiljer krypto från andra IT-säkerhetsmekanismer. Om en ”hackare” har varit inne i ett IT-system finns det alltid spår till skillnad från avlyssning av krypterad information i nätverk som inte märks. Forcering av ett kryptosystem ger inga spår!
- Om man hittar en brist i ett system kan skadan redan vara skedd. Även om bristen åtgärdas så finns all trafik som har krypterats med det bristande systemet redan inspelad (om den är intressant för någon aktör).
- Nationer vill skydda sig själva men även signalspana på andra. Detta innebär att det inte ligger i nationers intresse att exportera bra system eftersom det skulle kunna försvåra den egna signalspaningen. Således är inte alltid förtroendet för andra nationers kryptosystem speciellt högt.
- Man kan inte ”granska in” säkerhet i dagens komplexa system, d v s systemen innehåller så mycket kod att en skicklig, illvillig leverantör skulle med stor sannolikhet kunna lägga in en s k ”bakdörr” i systemet utan att granskaren märker det. Detta innebär att det måste finnas ett förtroende för leverantören av kryptosystemet.

Dåtid

Före 60-talet

Krypteringskonsten sägs vara runt 3 000 år gammal och det äldsta kända kryptosystemet är från 500-talet före Kristus, benämnt

Lakedemoniernas Skytale. En smal remsa pergament virades runt en trästav och sedan skrevs meddelandet bokstav för bokstav i stavens längdriktning på den omvirade pappersremsan. Remsan lossades sedan och sändes med en budbärare. Bokstäverna på remsan stod ju nu i en helt annan ordning och kunde inte läsas av en obehörig. Mottagaren hade en likadan trästav och kunde således upprepa proceduren och läsa meddelandet. I Sverige använde sig vikingarna av s k lönnrunor där det mest bekanta exemplet är inskriptionen på vissa delar av Rökstenen från 800-talet.

Världens första kryptomaskin var svensk.[2] Den presenterades 1786 i ett brev från friherren och hovjägmästaren Fredrik Gripenstierna till Gustaf III. Gripenstiernas morfar var Christofer Polhem, och i brevet skriver han att uppfinningen har sitt stöd i grunder han inhämtat från sin morfar i sin ungdom. Vad man vet tillverkades den endast i ett exemplar och en kryptomaskin måste förstås finnas i minst två exemplar för att komma till användning. Maskinen och även ritningarna till den är dock försvunna.

Den svenska kryptoapparatutvecklingen i modern tid börjar med bröderna Arvid och Ivar Damm.[3] Arvid var textilingenjör och Ivar var matematiklektor och de hyste båda ett brinnande intresse för kryptologi. År 1915 startade Arvid ett aktiebolag och fick de kommande åren fram flera prototyper till kryptoapparater. Dock stannade det vid prototyper, maskinerna fungerade inte felfritt och var svåra att sälja. Pengarna i företaget tog slut, men två personer vid namn K W Hagelin och Emanuel Nobel bestämde sig för att satsa pengar i Damms företag. Boris Hagelin som var son till K W Hagelin sattes in för att kontrollera företaget. Så småningom började han sköta företaget i Stockholm och produktifiera Damms uppfinningar. Ett antal apparater såldes till det svenska försvaret samt till Frankrike.

Vid krigsutbrottet 1939 var det denna maskin, som benämndes Chiffreringsapparat M/29, som fanns i drift för kryptosamband mellan högre staber. Mellan lägre staber användes koder och täcktabeller. På 30-talet fortsatte Boris Hagelin att vidareutveckla konstruktionen till mindre maskiner som byggde på en teknik med nyckelhjul, så kallade hjulverksmaskiner. C36 blev en klassiker och storsäljare som såldes till svenska och amerikanska försvaret m fl. Totalt tillverkades 140 000 maskiner. Boris Hagelin flyttade på 1950-talet till Zug i Schweiz och startade Crypto AG.

Det svenska försvaret fortsatte att använda Hagelins maskiner, och på 1950-talet fanns det endast ett maskinkrypto i drift som kallades MGB (Maskinkrypto Gemensamt Typ B) och var just en Hagelinmaskin.

Kort om organisation

1953 tillsattes en utredning angående vissa frågor rörande riksförsvarets sambandstjänst och 1957 överlämnades betänkandet ”Totalförsvarets kryptotjänst”. Statsmakterna beslöt 1959 att inrätta Statens Signalskyddsnämnd vars verkställande organ skulle vara Byrå K vid FRA. 1965 tillsattes ännu en utredning om ledningen av totalförsvarets signalskydd. Resultatet blev att ansvaret flyttades till Överbefälhavaren, där Totalförsvarets Signalskyddavdelning, TSA, organiserades i försvarsstaben 1968. Det fastställdes också att anskaffning av signalskyddsmateriel skulle flyttas till Försvarets Materielverk, FMV. Sedan dess har ansvaret legat i Försvarsmakten med enda skillnaden att TSA 1989 flyttades från sambandstjänsten till säkerhetstjänsten.

Numera ligger ansvaret för signalskyddet hos Chefen för Militära underrättelse- och säkerhetstjänsten där det operativa ansvaret utövas av Avdelningen för krypto och IT-säkerhet vid Säkerhetskontoret.

60- och 70-tal

På 60-talet och 70-talet byggde hela det skriftliga telekommunikationssystemet på fjärrskrift. För detta ändamål utvecklades fjärrskriftkryptot MGD som blev det mest använda fredssystemet för totalförsvaret. Under 1960-talet ägnades också mycket resurser åt att hitta en mer lätthanterlig ersättare till MGB. Detta resulterade i att systemet MGC köptes av det svenska företaget Transvertex AB. Nytt var att kryptonyckeln utgjordes av hålkort som kom att bli det gängse nyckelmediet för en lång tid framöver. Det behövdes dock ett off line-krypto med större kapacitet och som även kunde ge kryptotext för andra kommunikationsmedia än fjärrskrift. Detta behov löstes 1975 med att kryptosystem MGF togs i drift – försvarets första elektroniska krypteringsapparat.

Under 1970-talet ökade behovet av system för olika kommunikationsprotokoll och projekt EDIT (Elektroniskt Digitalt Textskydd) startades. Det fanns fortfarande behov av fjärrskrift men även av asynkrona data upp till 9 600 bit/s i halvduplex samt synkrona data upp till 9 600 bit/s i full duplex. Flera terminalbaserade informationssystem som byggde på protokollet ISO 1745 planerades. Omkring 1980 utkristalliserades två krav på kryptosystem från EDIT-projektet: dels ett krypto för MILTEX (ersättare till försvarets fjärrskrift), dels ett för synkront data i duplextrafik. Systemen kom att kallas MGG och MGH. Nytt med systemen var att vissa hemliga delar av kryptoalgoritmen lagrades på ett särskilt hålkort, ett s k systemhålkortet.

Kryptosystem MGC.

80-tal

I början av 80-talet började det komma fram vokodrar för digitalisering av tal med tillräckligt god talkvalité. Sådana köptes in (Telefonkrypto 750/S) och kopplades till MGH. Dessa användes i försvarsmaktens incidentberedskap bl a mellan vakthavande befäl vid staber och förband. Även de första digitala faxarna hade kommit ut på marknaden och företaget Panasonic kunde leverera en specialbeställd variant med ett digitalt gränssnitt som kunde kopplas till MGH. Ungefär samtidigt kom behovet av taktiskt talkrypto för användning med radiostationer för VHF-bandet (radiofrekvenser mellan 30 MHz-300 MHz). Utveckling startades under namnet P810 och studieutrustningar från tre firmor inköptes. Intresset var stort även från totalförsvarets civila del, särskilt polisen. Då det var dags för inköp svalnade plötsligt intresset från alla tidigare intressenter. Projektet skulle avvecklas, men då dök flygvapnet upp som en ny intressent och beställde systemet som kom att kallas MFA (Maskinkrypto Flygvapnet Typ A).

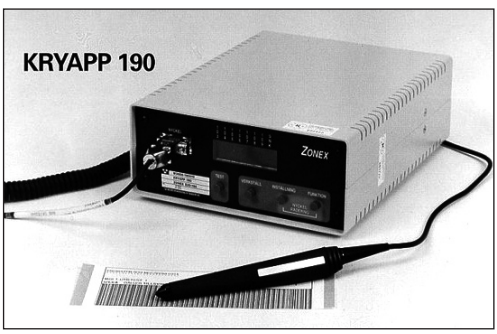
Samtidigt som systemet började levereras började de omskrivna ubåtsincidenterna, varvid även marinen kom att använda systemet, då benämnt MMA (Maskinkrypto Marinen Typ A).

Kryptosystem MGL.

I mitten av 80-talet ökade behovet återigen av nya system. MGC och MGF skulle ersättas med en liten terminal med kryptering som huvudfunktion. Inmatning av klartext skulle ske via ett tangentbord och utmatning av kryptotexten på display eller via en liten skrivare. Upphandlingen vanns av finska Nokia och ”på köpet” fick vi inbyggda modem för överföring via både telefon och radio. Systemet driftsattes i början på 90-talet under namnet MGK och är fortfarande i drift.

Behovet av talkrypto ökade och anskaffning av någon större mängd Telefonkrypto 750/s var inte möjlig, då det fanns krav på både billigare och mindre enheter. Studier av möjligheten att utnyttja modern kommunikationsteknik startades. USA hade lyckats med att miniatyrisera komponenter så att en kryptotelefon blev bara lite större än en vanlig telefon. Dock använde man låg datahastighet vilket medförde otillräcklig talkvalitet. Vår inriktning var att använda rön från mobiltelefonin för taldigitalisering kombinerat med erfarenhet från modemteknikutvecklingen. Datahastigheten skulle bli 9 600 bit/s, vilket till en början ansågs omöjligt. I början på 90-talet driftsattes MGL inköpt från Ericsson, vilket då var den kryptotelefon med bäst talkvalité i världen. Nytt med systemet var också att kryptonycklar på hålkort ersattes med streckkodsnycklar som därmed blev det nya nyckelmediet. Systemet är fortfarande i drift och anses vara det mest användarvänliga system vi har.

Likaså fanns ett starkt behov av utökad användning av krypterad fax. En krypteringsapparat köptes i ett stort antal exemplar av företaget Zonex AB och kallades MGM. Systemet är fortfarande i drift och är tillsammans med MGL det system som används inom krisberedskap i stora delar av totalförsvaret.



Kryptosystem MGM.

Vidareutveckling av befintliga datakrypton fortsatte och MGI och MGO togs i drift.

Kryptoapparaterna var vid den här tiden helt konstruerade i mjukvara, d v s i apparaterna finns det dataprogram som sköter krypteringen och lagrar kryptonycklarna som är det hemligaste i systemet. En nackdel med detta är att om någon obehörig kommer åt en apparat med inläst nyckel så går det att läsa ut hela minnet ur enheten och möjligen hitta nyckeln. Detta var

en av anledningarna till att det dök upp en idé om att utveckla en särskild elektronisk krets för kryptering och dekryptering. Med den elektroniska kretsen skulle utvecklingen av kryptomateriel både snabbas upp och bli billigare samtidigt som systemens säkerhet skulle öka, utrustningarna skulle kunna bli mindre och antalet tänkbara leverantörer skulle kunna öka eftersom den del som var svårast att konstruera redan fanns. Tillsammans med Televerket upphandlades två versioner av en sådan kryptomodul som fick namnet KM3-MIL och KM3-C (civil). Sectra AB i Linköping vann upphandlingen i hård konkurrens.

90-tal

För att dra nytta av internet-världens trafikmetoder och kommunikationstjänster beslöt Högkvarteret i mitten på 90-talet att Försvarsmakten skulle utveckla ett eget IP-nät byggt på FTN, FM IP-nät. För att man skulle kunna förhindra intrång i nätet och försvåra trafikanalys fanns behov av kryptering i högre hastigheter, vilket ledde till att de första kryptoapparaterna med kryptomodulen KM3 utvecklades. Flerkanalskrypto MGP togs fram för kryptering av radiolänksträckor i Försvarets Telenät, FTN och parallellportskrypto MGU utvecklades för delsträckskryptering i FM IP-nät. Så småningom uppstod även behov av ett system för end-to-end-krypto (kryptering hela vägen mellan sändare och mottagare) i detta nät och i början 2000-talet driftsattes det första s k VPN-kryptot (Virtuellt Privat Nätverk), MGV.

Vid den här tiden utvecklades en ny idé som kom att kallas kryptokort. Detta var ett instickskort med kryptofunktionalitet i form av kryptomodulen för persondatorer. Syftet var att kunna merutnyttja datorer som användes för bearbetning av hemlig information till att även kunna kryptera. Till kryptokorten utvecklades ett filkryptoprogram med vilket användaren på ett enkelt sätt kunde kryptera sina filer. Den första versionen benämndes MGR. Samma kryptokort kom sedan till användning i ett flertal system såsom LuLIS för luftlägesinformation och StriC, flygvapnets stridsledningscentral.

Försvarsmakten var tidigt ute med aktiva kort (eller smarta kort) för inloggning. Redan 1996 driftsattes TAK – Totalförsvarets aktiva kort – och började användas i ett antal hemliga informationssystem. Korten kunde även användas till att lagra kryptonycklar och kommande system inriktades på att utvecklas mot denna typ av nyckelmedia. Till TAK utvecklades även en kortterminal med tangentbord samt programvaror för att kommunicera med korten.

I mitten av 90-talet började användningen av mobiltelefoni bli mer allmän och ett stort behov av kryptering för denna kommunikation uppstod. Krypto för analog kommunikation är förenat med tämligen stora svårigheter men med GSM kom en datakanal som var lämplig för krypterad kommunikation. Det första systemet blev MGWI som när det togs i drift 2001 var världens första krypterade mobiltelefonisystem. Antennen satt ”upp och ner” vilket många trodde hade med krypteringen att göra men det berodde främst på att leverantören i den första prototypen hade en antenn som kunde vikas ned vid samtal, likt en annan telefon som då fanns på marknaden, för att minska stoleken på dåtidens skrymmande telefoner. Vid prov och försök med prototypen visade det sig dock att antennen lätt kunde brytas loss från sitt fäste och leverantören tvingades till att hitta en ny lösning. Kretskortet var i princip redan färdigt och de placerade då antennen

på telefonens undersida för att undvika att göra om hela kretskortet.

Som en kuriositet kan nämnas att TV-programmet Plus med Sverker Olofsson som programledare visades upp denna telefon som ett lysande exempel på hur Försvarsmakten på ett föredömligt sätt hade tagit fram en telefon som gav minde strålning mot hjärnan då eventuella faror med strålning debatterades en hel del under denna tid – trots att detta inte var det egentliga skälet till att antennen pekade nedåt.

Kryptosystem MGWI.

Med fler uppdrag utomlands för Försvarsmakten ökade behovet av att använda våra system i andra länder, vilket av säkerhetsskäl inte är tillåtet. Även om systemets säkerhet inte bygger på att algoritmen hålls hemligt vill man ändå skydda den eftersom användning utomlands anses öka dess exponering. Därför började vi ta fram särskilda system som fick användas utomlands, dessa skiljde sig endast i kryptoalgoritmen från grundsystemet. För att särskilja systemen lades bokstaven U till i slutet systembeteckningen, t ex MGLU.

Ett signalskyddsystems styrka anges av dess signalskyddsgrad, SG. Fram till slutet av 90-talet byggde signalskyddsgraderna på tidsbegrepp, d v s man valde signalskyddsgrad efter hur länge informationen skulle kunna vara hemlig. SG 3 var under sex timmar, SG 2 mellan sex timmar och två år och SG 1 var mer än två år. Nu bytte man till de säkerhetsskyddsnivåer som används internationellt och kopplade signalskyddsgraden till vilken informationssäkerhetsklass som systemet får skydda. Nya signalskyddsgrader blev SG R (Restricted), SG C (Confidential), SG S (Secret) och SG TS (Top Secret).

Nutid

På 2000-talet fortsätter vidareutvecklingen av system på datakommunikationssidan, medan fax (MGM) och telefoni (MGL) kvarstår i samma form. Ett kryptomodem, MGZI, för att ersätta gamla utrustningar framför allt inom marinen utvecklas och ett krypto för radiokommunikation mellan två JAS-plan granskas och godkänns för SG R. Nya kryptomoduler med högre hastighet och fler driftfall utvecklas och nya versioner av kryptokort tas fram.

Ett nytt VPN-krypto utvecklas av Business Security (numera Advenica), MGB (här kan vi se att beteckningen återanvänds då antalet tecken i alfabetet är begränsat), som senare vidareutvecklas till MGEI som är det mest komplexa som hittills har utvecklats.

Kryptosystem MGEI.

Erfarenheter från krypterad mobiltelefoni gör att det är omöjligt att följa den

oerhört snabba mobiltelefoniutvecklingen. När ett system är utvecklat och klart är det i princip redan för gammalt avseende storlek, batteritid och funktionalitet. Därför utvecklas ett nytt koncept, mobilt krypto, som utgörs av en enhet som användaren talar i och där krypteringen sker för att sedan skickas via protokollet ”Bluetooth” till mobiltelefonen som genomför sändningen. Systemet finns även med en bordsadapter för fast telefoni. Konceptet är nytt i världen och en del andra länder följer efter. För att minska kostnaderna för Sverige påbörjas ett samarbete med Holland. Systemet benämns MGFI.

Kryptosystem MGFI.

Sverige är nu med i flera internationella insatser och samarbeten och lånar därmed ut kryptosystem till andra samarbetande länder. Detta leder till att systemen görs även i en s k I-version för internationellt bruk medan de tidigare U-varianterna fasas ut. För att man ska sälja eller låna ut ett system krävs ett avtal där det köpande/lånande landet förbinder sig att hantera utrustningen enligt ett överenskommet regelverk.

De nya signalskyddsgraderna ger ett ökat behov av produkter för SG R (Restricted). Denna typ av produkter kan utgöras av endast mjukvara och ett VPN-krypto utvecklas och får en mycket stor spridning i Försvarsmakten och vid civila myndigheter. Systemet får beteckningen PGAI, Programvarukrypto Gemensamt Typ A Internationellt. Fler och fler mjukvaror för olika ändamål utvecklas och används som komponenter i IT-system.

TAK.

TEID.

Ett stort projekt med nya aktiva kort startar och leder till kort i olika versioner, TAK (Totalförsvarets Aktiva Kort) för inloggning i hemliga system, TEID (Totalförsvarets Elektroniska ID-kort) för inloggning i öppna system, NBK (Nyckelbärarkort) för lagring av kryptonycklar, DBK (Databärarkort) för lagring av information såsom konfigurering samt CEK (Card for Encrypted Keys) för lagring av krypterade nycklar.

Idag har vi drygt fyrtio system i drift. De flesta är maskinkrypto med signalskyddsgrad Secret och ett fåtal är programvarukrypto med signalskyddsgrad Restricted. En del av systemen såsom telefon- och faxkrypto är egentligen alldeles för gamla och bör tas ur drift inom de kommande åren. Detta delvis av säkerhetsskäl men även p g a att kommunikationstekniken ändras och går mot IP (Internet Protocol). Alla har ju t ex inte ens en analog telefonanslutning längre på jobbet.

Att utveckla nya system idag är en stor utmaning. Kraven från användarna är höga, helst ska man kunna t ex surfa med mobilen och samtidigt kunna prata hemligt och helst på nivån Secret. Detta är i prin-

cip omöjligt. Ju mer funktionalitet vi bygger in i ett system desto mer komplext blir systemet och desto svårare blir granskning och verifiering. Således vill användarsidan bygga in funktioner, medan vi vill att kryptoapparaten ska vara så enkel som möjligt. Hotbilden är en annan idag då en kryptoapparat vanligen ska kunna kopplas in mot internet och det är förstås allmänt bekant vilken hotbild som finns där.

För att granska en produkt behövs kryptologer, hårdvaruexperter, mjukvaruexperter, penetrationstestare och fuzz-testare. När jag började på TSA kunde jag själv göra det jobbet. Att produkterna kopplas mot internet gör att systemen även utgör ett intrångsskydd för det nätverket som kryptoapparaten ska skydda. Detta innebär att, förutom att kryptera/dekryptera, ska apparaten också skydda emot att en hackare kan ta sig förbi den och in i nätverket. Kryptoapparaten måste alltså ”skydda sig själv” mot intrång, en tuff uppgift idag. Detta ställer höga krav på design, t ex ”röd-svart-separering” vilket innebär att så gott som all data som förflyttas från den hemliga sidan till den öppna sidan ska passera kryptochipet.

För ett system som krypterar kvalificerat hemlig information, som är hemlig i femtio år, i hastigheter upp till flera gigabit per sekund, är kraven oerhört höga. Som tidigare nämnt skyddar ett sådant system dessutom hela nätverket mot intrång. Vi ska garantera att systemet inte har några brister, till skillnad från en hackare som ”bara” behöver hitta en brist. Vi ska inte hitta en ”nål i en höstack”, vi ska garantera att höstacken inte har några nålar. Dessutom får vi troligen aldrig reda på om vi har gjort att bra jobb eller inte. Vad ett lands signalspaning lyckas forcera brukar vara bland det hemligaste man har.

Vi kallar denna typ av produkter för högassuransprodukter. Ordet assurans står för tilltro till att en produkt gör vad den ska och ingenting annat. En organisation som vår kan dock inte hålla på med för många högassuransprodukter samtidigt, det är alltför komplext. Detta är anledningen till att en del äldre produkter inte kan bytas ut i den takt vi önskar.

Samtidigt finns idag en mängd produkter på marknaden som har en inbyggd krypteringsfunktion, t ex ”appar” för mobilen som krypterar talet och krypterande USB-minnen. En del av dem är säkert tillräckligt bra om inte hotbilden är främmande makts underrättelsetjänst, och för de flesta är trots allt inte den hotbilden aktuell. Tyvärr är dock en del produkter inte alls tillräckligt bra för att skydda mot någon med någorlunda kompetens inom området. Anledningen till detta kan jag bara spekulera om, men svårigheten att bygga säkra krypto och användarnas krav på enkelhet lär vara en stor del av problemet. Hur ska man då veta vad man ska köpa för produkt, även om det bara är pressen man ska skydda sig emot? Det korta svaret är att det vet man inte. Detta är en av anledningarna till att Försvarsmakten fått ett utökat uppdrag att även godkänna krypto för skyddsvärda uppgifter som inte rör rikets säkerhet, KSU. Detta ska kunna vara kommersiella produkter av god kvalité som ger ett skydd mot en medelduktig illvillig aktör men inte säkert skyddar mot den värsta hotbilden.

Ytterligare en skillnad idag mot förr är att systemen används av fler människor. Förr gick man till en sambandscentral där kryptörer hade som profession att använda kryptosystemen och var välutbildade på dessa. Idag ska gemene man helst kunna använda ett signalskyddsystem efter kort utbildning – detta ökar kraven på användarvänlighet och att det inte ska gå att göra fel.

Några jämförelser genom åren

Sammanfattningsvis kan vi göra jämförelser inom några områden:

Antal system i drift:

- 1959: Ett maskinkrypto.
- 1974: 4 maskinkrypto.
- 1989: 14 maskinkrypto.
- 1999: 22 maskinkrypto + aktiva kort och kortterminal.
- 2014: 44 maskinkrypto, 2 programvarukrypto, flera aktiva kort och kortterminaler, mjukvarukomponenter.

  Utvecklingstiden är ungefär samma i antalet år, dock är den totala tiden som läggs på utveckling av ett system långt större. På 80-talet kunde ett system utvecklas av en person som arbetade några år medan dagens komplexa VPN-system har ungefär 200 manårs utvecklingstid.

Teknik för krypteringsalgoritmer:

- 1959: Hjulverk.
- 1974: Hjulverk/elektronik.
- 1989: Processor.
- 1999: ASIC (Application Specific Integrated Circuit).
- 2014: programmerbar FPGA (Field-Programmable Gate Array).

Nyckelmedia:

- 1959: Blankett.
- 1974: Hålkort.
- 1989: Streckkod.
- 1999: Aktiva kort.
- 2014: Svarta (krypterade) nycklar.

Storlek på talkrypto:

- 1983: Telefonkryptosats 750/S till MGD – ca 80 x 40 x 40 cm.
- 1991: MGL – ca 22 x 20 x 5 cm.
- 1995: MGWI – 13 x 5 x 2.5 cm.
- 2009: MGFI – 11 x 6 x 2 cm.

Granskning:

- 1959: Mekanisk granskning.
- 1974: Begränsad verifiering.
- 1989: Kryptoverifiering av en person.
- 1999: Kryptoverifiering och lite källkodgranskning.
- 2009: Mycket kryptoverifiering, hårdvarugranskning, källkodsgranskning och testning.

Internationellt

Sverige har traditionellt utvecklat signalskyddsverksamheten på egen hand, utan så mycket internationell samverkan. De länder som är med i Nato har ofta regelverk som är mycket influerade av det gemensamma Nato-regelverket. När vi nu blir mer internationella har det ändå visat sig att det är förvånansvärt lite som skiljer oss från övriga länder som är duktiga på kryptoområdet, och Sverige har ett mycket högt anseende utomlands som kryptonation. Våra streckkodsnycklar är vi ensamma om och vi lägger större vikt på utbildning än många andra, i övrigt är regelverken i princip de samma. Vad gäller algoritmer så har vi sedan länge deltagit i en del internationella konferenser och har på så sätt utvecklats i takt med övriga världen. Där skiljer vi oss möjligen genom en lite mer skeptisk inställning till så kallade asymmetriska metoder. I övrigt är vår kravställning och våra granskningsmetoder mycket lika de som våra mer närstående nationer har. Inom många områden lig-

ger vi på framkant, vilket är imponerande av en liten nation som vår.

Interoperabilitet

Internationaliseringen innebär bland annat att en försvarsmakt måste vara interoperabel och en följd av detta är givetvis att de länder som ingår i ett samarbete måste ha samma kryptosystem för att utbyta information. Grundfilosofin är att båda parter har samma intresse av att skydda den gemensamma informationen så den part som tillhandahåller kryptot kommer att använda ett krypto som denne har fullt förtroende för. Vi kan låna ut eller sälja våra system eller så köper/lånar vi av andra länder. Idag köper Försvarsmakten mycket kryptosystem från USA, framförallt för användning i taktiska datalänkar. Dessa system är dock endast godkända för att kryptera information som är delgivningsbar till de länder som har tillgång till kryptonyckeln. För ett samarbete måste det landet som tillhandahåller kryptosystem även tillhandahålla kryptonycklar till de ingående parterna. All trafik som sänds med systemet kan då läsas av alla som har tillgång till nyckeln. Den information man inte vill dela med andra ska givetvis därför inte sändas på systemet. Detta blir problematiskt när man bygger upp system med endast utländska krypton. En annan aspekt är att man även blir beroende av tillgången på kryptonycklar, utan nycklar ingen trafik. I normalfallet får/kan man inte heller tillverka egna nycklar.

Nato och EU

Sverige hanterar en hel del säkerhetsskyddsklassificerad (hemlig) Nato-information och har i ett avtal förbundit sig att följa Natos regelverk kring detta. När det gäller IT-system säger avtalet i princip att vi kan använda vårt eget regelverk för hantering av hemlig information på motsvarande nivå. Det finns dock ett undantag och det är kryptosystem. För Natoländer gäller att kryptosystem upp till och med nivån Hemlig/Confidential ska vara godkända av en medlemsstats nationella kryptogodkännande organisation. Vi som icke Natoland har ansökt om att få göra motsvarande och fått detta beviljat. För nivån Hemlig/Secret måste dock systemet vara godkänt av Natos säkerhetsorganisation. Detta innebär att deras organisation SECAN (Military Committee Communications Security and Evaluation Agency) genomför ytterligare en granskning av kryptosystemet. Av denna anledning har vi inga system godkända för att skydda information klassas NATO Secret och i dagsläget finns det inga sådana system framtagna av länder som inte ingår i Nato.

Nationen Sverige har även i avtal förbundit sig att följa Europeiska Unionens råds beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade (hemliga) EU-uppgifter och även här har krypto en särställning. Av regelverket framgår att kryptoprodukter för skydd av sådana uppgifter ska vara godkända av en medlemsstats nationella kryptogodkännande organisation samt genomgått en andra granskning, en s k andrapartsevaluering, av en AQUA (Appropriately Qualified Authority) innan produkten godkänns av rådet. I praktiken gäller detta ännu så länge endast för nivån EU Secret.

Anledningen till dessa krav är att medlemsstaterna har en varierande förmåga att tillverka säkra kryptosystem. Genom att man låter SECAN respektive ett AQUA-land granska kryptosystemet innan godkännande av EU-rådet, elimineras förhoppningsvis risken att ett dåligt krypto används.

En AQUA utnämns av rådet på grundval av kriterier som rådet fastställt och innebär att organisationen har teknisk kompetens och goda processer inom kryptoområdet som gör den lämplig att genomföra kryptoevalueringar. Vi ansökte om att bli AQUA 2008, och i november 2011 togs beslutet att Sverige som sjätte land godkändes att bli en AQUA. Genom att påvisa att vi har förmågan att genomföra andrapartsevalueringar fick vi detta förtroende och mandat. Under processen fick vi en kryptoprodukt andrapartsevaluerad av en annan AQUA-nation till nivån EU SECRET. Idag har vi flera produkter på rådets lista.

De olika regelverken ställer till en hel del praktiska problem när man vill kunna hantera hemlig svensk, Nato- och EU-information i samma IT-system på nivån Hemlig/Secret. Kryptosystemet behöver då ett nationellt godkännande, ett Nato-godkännande och ett EU-godkännande. Därför pågår diskussioner mellan EU och Nato om att ett EU-godkänt krypto ska få användas för skydd av Nato-information som är delgivningsbar till EU och vice versa. Förhoppningen är att vi sedan ska kunna teckna ett motsvarande bilateralt avtal med Nato och på så sätt kunna använda egna system som blivit EU-godkända.

Framtid

Att sia om framtiden är givetvis oerhört svårt men några tankar ska jag ändå försöka mig på.

Det blir svårare och svårare att knäcka kryptosystem genom avlyssning. Det finns idag publika algoritmer som AES (Advanced Encryption Standard) som med en god nyckelhantering ger ett bra skydd. På internet går man mot flera lager av kryptering vilket ytterligare försvårar forcering. Det är enkelt att konfigurera dagens nätverkskomponenter så att trafiken krypteras. För att ens hitta intressanta kryptotexter måste man i många fall först knäcka ett annat krypto som är tämligen avancerat. Detta kan vara en av anledningarna till de metoder från amerikanska NSA (National Security Agency) som läckta uppgifter från den tidigare NSA-anställda Edward Snowden gör gällande. Genom att t ex placera så kallade bakdörrar i hårdvara från kommersiella leverantörer kan man få tillgång till kryptonycklarna och slipper lägga tid och kraft på att försöka forcera kryptot. Jag tror att motsvarande operationer pågår även i andra länder och kommer att fortsätta. Tilltron till leverantören är som tidigare nämnts av yttersta vikt och kommer att fortsätta vara så.

I USA har NSA påbörjat en utveckling kallad ”Commercial Solutions for Classified”. Detta är en process som syftar till användning av kommersiella produkter för skydd av hemlig information. Tanken är just att man ska använda två lager kryptering från olika leverantörer och sätta tilltro till att två olika produkter inte ska ha samma brister. Med tanke på den stora mängden nätverk och den stora mängden användare som USA har så kan jag väl förstå deras vilja att få fram billigare lösningar. Nu är det inte så att amerikanarna köper in vilken kommersiell produkt som helst utan processen innefattar en hel del krav på säkerhet, evaluering och testning samt att NSA själva genomför viss granskning. Leverantören ska även signera en överenskommelse med NSA där denne bland annat åtar sig att omgående korrigera eventuella brister i produkten.

Resonemanget bygger återigen på förtroendet för leverantörerna och här kan ett litet land som Sverige få problem då de flesta stora leverantörer är amerikanska och våra egna är tämligen få. Själva den tekniska principen med två lager kryptering anser jag dock ge en god design i vissa typer

av produkter för de lägre signalskyddsgraderna.

Min uppfattning är att vi kommer att fortsätta utveckla svenska signalskyddsystem. Dock kommer vi att behöva begränsa produktfloran till ett antal produkter som vidareutvecklas över tiden. Vi kan omöjligen ha över fyrtio system i drift framöver. Redan nu har ett arbete påbörjats som identifierar vilka förmågor vi behöver inom tal, meddelande- och datakommunikation för olika signalskyddsgrader. De system som utvecklas ska ha som syfte att kryptera/dekryptera och så mycket annan funktionalitet som möjlig måste läggas utanför kryptosystemet. De förmågor vi väljer måste underhållas på ett helt annat sätt än tidigare. Förr kunde vi driftsätta ett system som fick stå omodifierat på användarnas skrivbord i tjugo år, så kan vi inte längre göra. Snarare är det så att när ett nytt system är driftsatt så gör teknikutvecklingen att vi tämligen omgående måste börja fundera på nästa generation av systemet.

Antalet enheter kommer däremot att öka. Säkerhetsskyddslagen är under utredning och det är möjligt att begreppet rikets säkerhet vidgas till att även omfatta t ex kritisk infrastruktur. Om så blir fallet kommer behovet av krypto som skyddar mot främmande makts underrättelsetjänst att öka – och då är det signalskydd som behövs. Kraven på användarvänlighet och enkel nyckelhantering kommer därmed att bli ännu större.

Samtidigt är det kostsamt att utvecklas signalskyddssystem. Detta leder till behov av samarbete med partner som vi litar på. Idag har vi ett samarbete med vår holländska motsvarighet, och min uppfattning är att dessa samarbetsformer kommer att öka i framtiden för att spara på kostnader och resurser.

Jag anser att det är oerhört viktigt att Sverige har en inhemsk kryptoindustri. Skälen till detta har flera gånger påtalats här. Svensk kryptoindustri är duktig men har svårt att överleva med endast Försvarsmakten/FMV och övriga myndigheter som kunder. EU-godkännande av svenska produkter öppnar dock upp marknaden för att sälja dessa produkter inom EU. Vi måste då stötta industrin med att teckna signalskyddsöverenskommelser med de köpande länderna vilket vi gör på uppdrag av Försvarsexportmyndigheten. Denna uppgift lär öka i framtiden.

Slutligen skulle jag vilja framhålla att det under hela historien har varit en kamp mellan de som skapar kryptosystem och de som forcerar dem. I alla tider har de som skapar trott att de ligger före de som forcerar och än så länge har de som forcerar kommit ifatt. Detta är av vikt att tänka på när man från olika håll tycker att vi granskare är väl paranoida. Skulle vi verkligen vara de första ”kryptokonstruktörerna” som har lyckats? Och får vi någonsin veta detta?

Författaren är chef för Avdelningen för krypto och IT-säkerhet vid MUST och ledamot av KKrVA.

Noter

1. Kerckhoffs, Auguste: ”La cryptographie militaire”, *Journal des sciences militaires*, vol IX, s 5-83, januari 1883, s 161-191, februari 1883.
2. Beckman, Bengt: *Svenska kryptobedrifter*, Albert Bonniers Förlag, 1996, s 21-22.
3. Ibid, s 29-40.