2019-02-18

Till: Myndigheten för Samhällsskydd och beredskap
Avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet
Email: metodstodet@informationssakerhet.se

Från: Föreningen SNUS
Email: board@snus.se

Föreningen SNUS har tagit del av ***Vägledning för grundläggande kryptering***[1] version 0.94 och har följande synpunkter.

Generella kommentarer

Föreningen SNUS frågar sig varför vägledningen har skapats. Den verkar vara en sammanfattning av vad andra har sagt, och den missar tyvärr många detaljer som man bör känna till innan man tar beslut om vad som ska gälla. Innehållet i vägledningen är inte tillräckligt komplett för att kunna vara ett underlag för kravställning på en lösning, utan dokumenten som vägledningen refererar till måste studeras. Vägledningen skulle vara mera användbar om det för varje teknologi stannar vid att referera till ett auktoritativt dokument som innehåller den information som krävs. Vägledningen har också väldigt olika detaljnivå i olika avsnitt, med exempel på konfigurationsdetaljer i vissa avsnitt och avsaknad av konkreta råd i andra.

Det är dessutom otydligt hur vägledningen skall tolkas ihop med Försvarsmaktens (MUST, SÄKK, SÄKT, TSA) ensamrätt att godkänna säkra kryptografiska funktioner, och hur dokument från dessa organisationer skall hanteras parallellt med vägledningen.

Det är inte bra om det i vägledningen erbjuds ofullständiga anvisningar som läses istället för dokument med auktoritativ information.

Oklar målgrupp

Tyvärr är målgruppen för vägledningen oklar. Beskrivningen i inledning är otydlig. Vägledningen är för avancerad för små myndigheter och verksamheter, som i praktiken inte kan ställa så detaljerade krav och göra så detaljerade analyser som krävs. Samtidigt är den för tunn för dem som har resurser att kunna påverka och agera, eller är den som slutligen ska göra en kravställning eller införa en krypteringslösning.

[1] Myndigheten för Samhällsskydd och Beredskap, Avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet, 2019-01-21, version 0.94, https://www.msb.se/Upload/Forebyggande/Informationssakerhet/V%c3%a4gledning%20grundl%c3%a4ggande%20kryptering%20f%c3%b6r%20kommentarer.pdf

Protokoll för VPN-tunnlar

Föreningen SNUS noterar att dokumentet rekommenderar IPsec men varken WireGuard, OpenVPN eller någon annan teknologi.

Enligt vår mening är WireGuard de facto state-of-the-art för säkra VPN-tunnlar, men uppenbarligen inte allmänt känd ännu. En vägledning av denna typ bör upplysa om de olika teknologier som finns på marknaden och tydligare förklara fördelar och eventuella risker med att använda dem. OpenVPN har funnits i många år, och WireGuard är i och för sig tämligen ny, men den som privata marknaden idag väljer.

För att summera, idag har vi OpenVPN och IPSEC och inte bara IPSEC. Nu etableras WireGuard och dokumentet ger ingen bra vägledning i frågan om tunnelteknologier generellt eller vad de kan användas till och hur.

Vi vill tipsa om en bra presentation om IPSEC av Steven M. Bellovin, ***The Evolution of IPsec***[2], liksom en utvärdering av IPSEC av Niels Ferguson och Bruce Schneier, ***A Cryptographic Evaluation of IPsec***[3].

Konfiguration av VPN-tunnlar

Det är naturligtvis bra med VPN-tunnlar och vpn, men varje protokoll innanför tunneln bör också vara krypterat, för tyvärr så läcker vpn ibland. Eller så är tunneln inte explicit utan tillåter s.k. split tunneling så att kontrollplanet läcker information som man trodde hölls under kontroll. Likaså kan ändpunkt innan och efter tunneln läcka information.

Utifrån vårt perspektiv och erfarenhet skall varje koppel på internet krypteras så man inte behöver oroa sig för felkonfigurering av VPN-tunneln och dessutom gör det felsökning enklare. Dvs, tunnel kan vara intressant i vissa fall, men alltför ofta används säkerheten i tunneln (när den väl är etablerad) som ett sätt att säkra tjänster som accessas via tunneln, vilket är en farlig slutsats att dra. Tjänsterna måste fortfarande skyddas.

Trafikanalys är ett ganska kraftfullt verktyg för att ta reda på vad folk håller på med. Om grafen över vilka noder som kontaktas är inspekterbar förloras rätt mycket i skyddsförmåga.

---

[2] Steven M. Bellovin, *The Evolution of IPv6*, https://www.cs.columbia.edu/~smb/talks/why-ipsec.pdf

[3] Niels Ferguson och Bruce Schneier, *A Cryptographic Evaluation of IPsec*, https://www.schneier.com/academic/paperfiles/paper-ipsec.pdf

Eller, som det heter:

Gärna textskydd, men först trafikskydd!

Motsvarande gäller för konfigureringar som split tunnel. Man kan tycka att det är väldigt bekvämt, särskilt när den som hanterar VPN och brandvägg på det skyddade området har skruvat upp reglerna för hårt. Användarna kan på ett enkelt sätt komma åt sina saker på sitt lokala (hemma-) nät samtidigt som de kan nå saker genom tunneln, och det är en stor produktivitetshöjare.

Men detta är, ärligt talat, inte bra. Det läcker metadata och skapar osäkerhet om vad användarna kan hålla på med utan att avslöja för mycket.

Dokumentet bör därför inte bara tala om tunnelprotokoll utan hur de konfigureras.

Elliptiska kurvor

Det är bekymmersamt att algoritmerna Curve25519 och Curve448 inte är med i vägledningen. BSI får in sina algoritmer, men de algoritmer som det öppna kryptosamfundet kommit fram till är bra finns inte med. Det gör att TLS 1.3 blir svårare att få med i rekommendationerna. I avsnittet om DNS saknas t.ex. ECDSA som rekommenderad algoritm.

TLS

Föreningen SNUS anser att TLS 1.3 ska tas med i en rekommendation som denna. Rekommendation 7.3.1.1 bör därför vara att TLS version 1.2 *eller senare* skall användas.

7.3.2.1 ger rekommendation att använda HSTS vilket är bra, men motiveringen att “mix-content” inte tillåts på grund av det är felaktig.

DNS

Rekommendationerna gällande DNS är inte heltäckande. Det står ingenting om validering av signerade svar som fås från DNSSEC eller hur DNS och DNSSEC bör konfigureras (varken på validerings- eller signerings-sidan). Det står inget om hur DS-poster bör hanteras, eller i övrigt hur DNS skall hållas säkert. Även om denna vägledning är om kryptoalgoritmer blir inte kedjan starkare än den svagaste länken. Samtidigt som t.ex. avsnittet om SSH är detaljerat (för en viss implementation av SSH) är avsnittet om DNS mycket tunt. Det ställs

t.ex. inga rekommendationer vad gäller val av domännamn, registrar, och vilken typ av säkerhet som skall finnas.

Röst/Videosamtal

Det står att "*TLS är designat för att tillhandahålla säker kommunikation över internet och har många olika användningsområden på internet. Några exempel är att skydda hemsidor, e-post, instant messaging, och röst/videosamtal.*"

Detta är inte korrekt. Röst/videosamtal skyddas inte med TLS. Signalering kan använda TLS eller DTLS men samtalet använder oftast SRTP, i bästa fall med DTLS key exchange.

Design av röst och video är bara ett exempel på hur knepiga överväganden som kan behöva göras. Är det verkligen värt besväret (och ev. kostnad) att användare kräver kryptering av media? I nästa ”länk” av samtalet går det kanske i en gammal parkabel i gatan, via tydliga skruvskallar i kopplingsskåpet där nyfikna grannar lätt kan koppla in sig. Men visst; det är ju inget hållbart försvar att det kan vara sämre på andra håll. Någon form av kostnadsnyttoanalys bör i alla fall göras, och detta beskrivs inte i vägledningen.

SRTP

Konfiguration och hantering av SRTP saknas.

Exempel:

En kommun upphandlar en SIP-trunk till växeln och får en standard-SIP-trunk från sin operatör. Socialkontoret genomför nu okrypterade telefonsamtal i ärenden som ska vara konfidentiella över en internetförbindelse.

Fjärradministration

Vägledningen innehåller rekommendationer för SSH men inte för protokoll som Remote Desktop Protocol (RDP). Just RDP är ett mycket vanligt förekommande protokoll för fjärradministration.

Ojämn teknisk nivå

I övrigt är vägledningen ojämn. SSH-avsnittet går in på specifika konfigurationer men missar helt att även klienten kan konfigureras bättre.TLS-avsnittet föreslår inte ens en sund konfiguration av en vanlig webbserver som t.ex. Apache eller Nginx.

Multi-faktor autentisering

Vägledningen säger inget om multi-faktor-autenticering. Avsaknad av detta och istället användning av lösenord är idag ett av de största problemen vi har. Hur ska man hantera det, vad ska man kräva, hur är det med U2F, WebAuthn etc?

Lösenord

Som nämnts i förbigående på andra ställen bör vägledningen utförligt beskriva hur lösenord skall hanteras i de fall det måste användas. Idag nämns vissa detaljer t.ex. i avsnittet om SSH, men dessa och fler rekommendationer är generella.

E-mail eller e-post

Vägledningen använder både termen “e-mail” och termen “e-post” utan att ange om den avser samma sak eller olika saker. Vägledningen bör ha en konsekvent terminologi.

S/MIME

Det bör noteras att S/MIME inte är generellt spritt, speciellt inte i den operationella delen av Internet och därför kan S/MIME inte alltid användas. Detta är ett organisationsberoende förutom beroende av klientimplementation.

PGP

Det bör noteras att PGP används på individnivå, speciellt i den operationella delen av Internet. Användning är dock på individnivå förutom att vara beroende av klientimplementation.

PGP är också basen för programdistribution i många operativsystem. Man bör överväga en rekommendation om liknande tillvägagångssätt med tydliga riktlinjer för hur förtroende för signeringsnycklar ska etableras och hur nycklar ska hanteras inom respektive organisation.

Säkerhetsskydd

Det är oklart när man refererar till den nya säkerhetsskyddslagen (som gäller från 1 april 2019) gällande säkerhetsnivåer. Det borde i ett dokument som detta tydligt framgå vilket skyddsvärde som ges med de olika föreslagna lösningarna.

Framtagande av detta papper

Personer som arbetat med detta remissvar inkluderar:

Andreas Ehn, Daniel Stenberg, Eric Krona, Fredrik Strömberg, Fredrik Söderblom, Harald Barth, Joachim Strömbergsson, Jonas Lejon, Magnus Danielsson, Mats Dufberg, Mats Lindhé, Michael Cardell Widerkrantz, Mikael Kullberg, Måns Nilsson, Niklas Gerdin, Olle E Johansson, Patrik Fältström, Patrik Wallström, Per Kangru, Robert Malmgren, Take Aanstoot, Tobias Norrbom och Torbjörn Eklöv

Patrik Fältström
Ordförande Föreningen SNUS