KRYPTO – EN DEL AV CYBERFÖRSVARET

PIA GRUVÖ
CHEF AVDELNINGEN FÖR KRYPTO OCH IT-SÄKERHET VID MUST

FÖRSVARSMAKTEN

VAD ÄR SPECIELLT MED JUST KRYPTO?

- Historia
- Dålig produkt kan ge stor skada utan att det märks
- Hittar man en brist kan skadan redan vara skedd för all trafik som gått på systemet
- Signalspaning kontra signalskydd
- Det går inte att granska in säkerhet

Säkerhetsskyddsförordningen (1996:663)

13 § Myndigheter och andra som förordningen gäller för skall, innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, förvissa sig om att det för uppgifterna finns en fullgod informationssäkerhet.

Hemliga uppgifter får endast krypteras med kryptosystem som har godkänts av Försvarsmakten.

SIGNALSKYDD

Kryptosystem för skydd av rikets säkerhet benämns signalskyddssystem

→ Kryptoapparat

→ Kryptonycklar

→ Regelverk

Styrkan i signalskyddsystemet anges av signalskyddsgrad (SG)

→ ”Lägre” nivåer: Restricted (SG R)

→ ”Högre” nivåer: Secret, TopSecret (SG S, SG TS)

→ I många fall även ett intrångsskydd för ett IT-system, ex VPN-krypto

VÅR UTMANING

→ Att godkänna ett kryptosystem som ska skydda TopSecret-information i gigabit/sek 95 år framåt, samt skydda ett TopSecret-nätverk från intrång

→ Motståndare: främmande underrättelsetjänst med mycket stora resurser

→ Vi kravställer, granskar och godkänner

VAD INNEBÄR DETTA?

- → Algoritm och protokoll
- → Nyckelhantering
- → Röd-svart separering
- → Design
- → Hård- och mjukvara
- → RÖS-skydd
- → ”Tamper protection”
- → Utvecklingsprocesser
- → Assurans!

FÖRMÅGOR INOM SIGNALSKYDDET

- → Krypterad datakommunikation
  - → SG R
  - → SG TS / SG S
- → Meddelandekrypto
  - → SG R
  - → SG TS / SG S
- → Krypterat tal
  - → SG R
  - → SG S

INTERNATIONELLT

- → Utländska system – inom ett interoperabiltetssamarbetes ram

- → EU
  - → nationellt godkännande upp till och med EU Confidential
  - → andrapartsevaluering för EU Secret
  - → vi är godkända andrapartsevaluerare (AQUA)

- → NATO
  - → nationellt godkännande upp till och med NATO Confidential
  - → NATO Secret kräver granskning av NATO (SECAN)

SLUT

FÖRSVARSMAKTEN