Folketingets Retsudvalg
Christiansborg

Kgs. Lyngby, den 4. november 2004

**Nuværende sikkerhedsprincipper fremmer identitetstyveri**
Samfundet spilder i øjeblikket omfattende ressourcer og tid på at indføre sikkerhedsprincipper og -teknologier, der på forhånd må forventes at slå fejl. Det vil i stigende grad fremme kriminalitet baseret på identitetstyveri, hvor den kriminelle opnår sikkerhedsclearing til stadigt mere følsomme systemer og funktioner ved teknisk at udgive sig for en anden, som dermed også bliver offer.

Udover selve den kriminelle handling, så kan de uskyldige ofre for identitetstyveri komme i en helt umulig situation, hvor de reelt står med omvendt bevisbyrde. Aktuelt bevæger vi os imod såkaldt permanent identitetstab, hvor ofrene negativ-listes på basis af biometri og udelukkes fra normalt liv.

Specifikt vil jeg aktuelt opfordre Retsudvalget til at se på spørgsmålet om de nye pas med RFID og biometri uden for borgerens kontrol. Sagkyndige over hele verden siger fra[1], blandt andet fordi de nye pas gør det alt for nemt for kriminelle at tilgå data og begå identitetstyveri[2], men også fordi de unødvendige centrale registreringer skaber alvorlige risici for anden misbrug. Sikkerheden vil kun forværres, når falsk tryghed mindsker årvågenheden og der skabes permanent identitetstyveri.

Jeg foreslår ikke, at man skal bibeholde de nuværende pas og acceptere falskneri etc., men at der må skabes løsninger, som bygger på et grundprincip om borgerens egeninteresse i egen sikkerhed. Alternativet er, at sikkerhedsbevidste borgere helt må undvære pas og reelt stavnsbindes.

Overgangen til det Digitale Samfund har udviklet sig til en negativ spiral mellem en uholdbar sikkerhedspolitik fokuseret på stadig mere identifikation og tilsvarende mere avanceret kriminalitet. Begge dele skaber voksende sikkerhedsrisici og problemer demokratiet og økonomien. Det spil kun kan vindes ved at ændre spillets regler med fokus på den enkelte borger.

Jeg vil med den baggrund gerne opfordre Retsudvalget til generelt at fokusere i retning af de nødvendige ændringer af sikkerhedspolitikken for at give den enkelte borger mulighed for at beskytte sig imod identitetstyveri som den eneste langsigtede holdbare måde at øge sikkerheden for alle. Det har mange aspekter herunder Personlig Identity Management[3]. Argumentet for at det politiske bør blande sig er at markedet for Identity Management er drevet af gatekeepernes kommercielle magtinteresser snarere end samfundets sikkerhedsbehov, jf. slagsmålet mellem Digital Signatur og bankernes Net-Id. Den største udfordring er en politisk holdningsændring i retning af den enkelte borgers sikkerhed. For en uddybning henvises til omstående.

Venligst

Stephan Engberg
Open Business Innovation

[1] http://www.itsc.org.sg/events/cpitc_seminar_oct03/Tough_Problems_Facing_Biometric_Passports.pdf
[2] http://hasbrouck.org/blog/archives/2004_10_15.html
[3] Se f.eks. http://www.lawyersweekly.com.au/articles/23/0C020E23.asp?Type=56&Category=841

## Uddybning og baggrund

Udviklingen i retning af mere kriminalitet vil ske i takt med at kriminelle presses af det stigende fokus på identifikation til at begå identitetstyveri, dvs. hvor der er 2 ofre for kriminalitet, idet den kriminelle succesfuldt udgiver sig for at være en konkret eksisterende person med f.eks. sikkerhedsclearing til systemer, data eller fysiske døre. Identitetstyveri vokser overalt i verden[4] i mange forskellige former lige fra simpel misbrug af kreditkortnumre over fjernstyring af borgeres computere via indsmuglet spyware til de mere avancerede tiltag[5], hvor man f.eks. målrettet stjæler en identitet med falske fingeraftryk etc. for at kunne begå kriminalitet ved omgå adgangskontrol.

Samtidigt gør vi det stadigt nemmere at begå identitetstyveri fordi sikkerhed ikke tager udgangspunkt i individets mulighed for at beskytte sig selv, men fokuserer på at beskytte systemerne mod mennesker via global identifikation, som genbruges på tværs.

Dette selvom vi ved, at identifikation næsten per definition ikke kan blive perfekt. Man indfører dyre tekniske sikkerhedsmekanismer som man fejlagtigt opfatter som mere sikre, såsom f.eks. digitale pas, dankort, digitale signaturer osv. Vi løser altså ikke problemerne ved blot at gøre det sværere at kopiere eller forfalske f.eks. pas eller digitale signaturer – det ændrer blot misbruget.

Konkret har vi f.eks. netop ved en sikkerhedskonference i Canada påvist[6], hvordan man relativt nemt kan stjæle identiteter ved brug af trådløst baserede Id kort - specielt hvis de er baseret på de såkaldte radiobrikker (RFID), men også hvis de baseres på de nuværende design af Smartcards.

På samme konference viste vi også, hvordan man formentlig vil kunne bruge de samme metoder til f.eks. at maskere en ikke-sikkerhedsclearet container som en allerede sikkerhedsclearet. I fremtiden vil vi se de samme problemer eskalere i forbindelse med det såkaldte Pervasive Computing – jf. høringen i regi af Rådet for IT-Sikkerhed under betegnelsen "IT-i-Alting – Sikkerhed i Ingenting".

Centeret i Canada havde netop investeret en million USD i såkaldt stærkt sikrede rum med fysisk sikkerhed og stærk adgangskontrol med biometri etc. til brug for f.eks. nationalt sikkerhedsclearede krisekonferencer, hvorefter flere deltagere kunne konstatere at det ville være relativt enkelt at bryde adgangskontrollen uden at begå fysisk indbrud – systemet ville TRO at det var en sikkerhedsclearet person, der kom ind i bygningen, selvom det fysiske adgangskort aldrig forlod ofret.

Brug af biometri (f.eks. fingeraftryk, ansigtsgenkendelse etc.) uden for individets kontrol vil sandsynligvis kraftigt forværre problemet, dels fordi biometri absolut ikke er så sikkert som påstået og dermed relativt nemt kan "stjæles", og dels fordi identitetstyveri baseret på biometri har nogle meget alvorlige konsekvenser for ofret, idet vedkommende pludselig vil opleve at vedkommendes biometri pludselig fremgår af negativlister, hvor det vil blive grænsende til umuligt at komme af igen. Danske borgere risikerer derfor helt uacceptabelt at blive udelukket fra deres eget liv for altid.

For et helt oplagt problem kan man pege på det umulige i fremtidige vidnebeskyttelsesprogrammer og "under cover" politi arbejde, fordi man ikke kan skifte identitet, selv hvis det er ønskeligt.

---

[4] F.eks. US FTC estimerer 27,3 millioner ofre for Id Theft de sidste 5 år - http://www.bizreport.com/news/8284/

[5] Se Gartner Groups aktuelle udmelding om problemet med Identitetstyveri og et par relativt simple eksempler - http://www.comon.dk/index.php/news/show/id=19854

[6] Kun delvist online tilgængeligt for ikke at publicere "opskrifter" - det online tilgængelige findes her: http://www.obivision.com/Papers/PST2004_RFID_ed.pdf

MERE af samme form for sikkerhed fokuseret på global og central identifikation vil blot forværre situationen. Som destruktiv konsekvens vil det samtidig skabe stadigt mere omfattende central kontrol, registrering og overvågning, der igen aflejre kilder til nye sikkerhedsbrud. I Danmark er vi i højere grad end andre steder i gang med at maksimere sikkerhedsrisici i f.eks. Digital Forvaltning og Infrastrukturen generelt. Her ser vi en udvikling i retning af stadigt større koncentration af risiko i få knudepunkter såsom f.eks. portaler såsom Sundhedsportalen og identity brokers såsom Net-Id, som gør alvorlige sikkerhedsbrud uundgåelige og samtidig medfører, at der sker sammenstilling af stadigt mere følsomme data uden for virksomhederne og borgeres kontrol.

Disse problemer rammer meget bredt i forhold til igangværende tendenser. Rejsekort, adgangskontrol, dankort, id kort men først og fremmest pas, hvor man internationalt og i Danmark har haft travlt med at indføre sikkerhedsmodeller, der reelt skaber flere sikkerhedsrisici end de fjerner. Som f.eks. Ekstrabladet viste med deres demonstration af Identitetstyveri i foråret, så er sikkerheden i det danske samfund gradvist svækket i takt med at systemerne kobles og borgerne mister kontrollen.

Vi begår kort sagt basale fejl i vores forståelse af sikkerhed med den konsekvens, at vi er i gang med at gøre overvågningssamfundet deterministisk uden det vil skabe mere sikkerhed. Det skaber destruktive konsekvenser for samfundsøkonomien, idet gatekeepere etablerer positioner, der forhindrer konkurrence, fri kommunikation og nedbryder tilliden.

Den helt afgørende beslutning ligger i overgangen fra softkey digitale signaturer til hardware-baserede. Det er kendt, at de nuværende OCES signaturer og Net-Id kan fjernstyres med standard spyware. Alligevel gør man systemet stadigt mere sårbart idet OCES signaturen genbruges til authentikering på tværs i stedet for kun at reservere den til identifikation. Med de nuværende hardwarebaserede modeller vil vi skalere risikoen og samtidig vende bevisbyrden.

Det er ikke holdbart at bygge informationssamfundet op omkring et verdensomspændende og alt omfattende kommunikationsnetværk baseret på sikkerhedsfilosofier, der stammer fra 1970erne. I dag er udfordringen hvordan man undgår alle de sikkerhedsproblemer, som skabes af Identifikation.

Som samfund er vi i færd med at tage nogle meget farlige beslutninger på vej ned af en sti, hvorfra der ikke er nogen vej tilbage. Hastværk vil vise sig at blive lastværk og virke ødelæggende ikke bare for sikkerheden, mens også for samfundsøkonomien, ofrenes tilværelse og tilliden til informationssamfundet som sådan.

For at citere Albert Einsteins vise ord
***Intellektuelle løser problemer, genier forebygger dem***
***Vi kan ikke løse problemer med den samme tænkning, som da vi skabte dem***

Kun rettidig omhu vil være i stand til at forebygge de selvskabte problemer, der opstår i takt med at systemerne kobles sammen og stadigt flere følsomme data lægges i samme kurv, samtidig med at stadigt flere har adgang via stadigt flere kommunikationskanaler. Hvor det fysiske net kobler og sammenstiller alt må vi indbygge logiske grænser. Det centrale er, at kontrollen med de kontekst-specifikke nøgler lander hos den enkelte borger[7] frem for en gatekeeper eller myndighed.

[7] http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/text_en.htm

**Open Business Innovation**

Open Business Innovation er en højteknologisk innovationsvirksomhed hjemmehørende i Kgs. Lyngby. Vi har gennem de seneste 5 år koncentreret os om, hvordan vi skaber sikkerhed for alle i en verden, hvor alt og alle kobles sammen i et og samme fysiske netværk. En virkelighed, som vi er tæt på at realisere uden fornøden forståelse for, hvad det vil kræve for en holdbar samfundsmodel.

Vi underviser på de højere læreanstalter og deltager aktivt i forskning og udvikling indenfor en lang række sikkerhedsrelaterede områder både i Danmark, i EU og internationalt. Undertegnede blev f.eks. af OECD anmodet om at repræsentere borgerne på det afsluttende Roundtable af OECDs sikkerhedskonference i Oslo november 2003 – "Global Forum on Information Systems and Network Security". I deccember 2002 var vi indlægsholder på workshoppen "Living with Security"[8] i forbindelse med IST-konferencen i Bellacenteret under Danmarks EU-formandskab. I sommeren 2003 var vi inviteret som paneldeltager på udbyder-siden af sikkerhedsteknologier sammen med IBM og Microsoft på EU's "Workshop on Privacy Enhancing Technologies". I foråret 2004 var vi inviteret indlægsholder på EU's "Smarttags Workshop" om fremtiden for de såkaldte RFID-teknologier som er grundbyggestenen i "It-i-Alting", som f.eks. VTU promoverer stærkt.

Af hensyn til forståelsen af ovenstående vil jeg henvise til Teknologirådet Publikation nr. 186[9], hvor dele af vores arbejde med at designe teknologiske løsninger og påvise, at man kan løse denne type problemer uden at gå kompromis med hverken borgernes rettigheder eller hensyn til at effektivisere og samtidig opretholde sikkerheden mod truslerne, som opstår i et digitalt Informationssamfund.

Det drejer sig om en grundlæggende forståelse af, at essensen af f.eks. et Borgerkort og Digital Signatur IKKE er identifikation, men at kunne arbejde med mange forskellige kontekst-specifikke nøgler, så borgeren selv kan styre sine adgange og egne data i en lokal kontekst, dvs. så man ikke lægger stadigt flere og mere skrøbelige æg i samme kurv. Teknisk og juridisk kan det forstås som ejerskab af egne data. Ideologisk og økonomisk er der ingen grund til at regulere lokale data.

Gør vi det rigtigt kan vi opnå BÅDE mere frihed, bedre services og samtidig mere sikkerhed end nogensinde før. Gør vi det forkert, kan det nemt vise sig at blive fatalt, fordi vi står på overgangen til en helt anden type samfund, hvor nye digitale grænser skal opbygges for at erstatte de gamle geografiske og tekniske grænser under nedbrydning. Bevidst eller ubevidst er vi ved at vælge.

Stephan J. Engberg
Open Business Innovation
Stengaards Alle 33D
2800 Kgs. Lyngby

*Making Privacy Default*
*... because the alternative is not an option*

[8] IST-konferencen i Bellacenteret: http://www.obivision.com/Papers/IST_Living_with_security_20021106.PDF
[9] Teknologirådet "Fra Råd til Tinge nr. 186 - IT-Privacy skal forbedres" - http://www.tekno.dk/pdf/nummer186.pdf