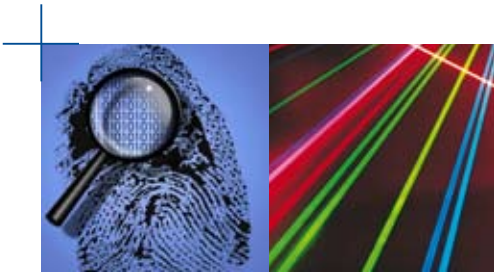
Forskningsrådet

IKT-sikkerhet: Det kontinuerlige kappløpet

Sluttrapport

Program
IKT sikkerhet og sårbarhet – IKT SoS



Om programmet

Forskningsprogrammet IKT sikkerhet og sårbarhet (IKT SoS) hadde som målsetning å frembringe og gjøre tilgjengelig ny viten og kunnskap som kan bidra til å øke sikkerheten og redusere sårbarheten ved bruken av dagens og morgendagens IKT-systemer. IKT SoS har støttet forskning som hadde til hensikt å studere, analysere og utvikle løsninger for bedret informasjonssikkerhet, slik at informasjon og informasjonsflyt ved bruk av IKT-systemer i organisasjoner kan gis en riktig beskyttelse mot uønskede hendelser, og at brukeres behov for sikkerhetsløsninger kan sikres gjennom tilstrekkelig tilgang til spisskompetanse for å kunne få utviklet dette.

Innhold

IKT-sikkerhet er et kontinuerlig kappløp

Informasjons- og kommunikasjonsteknologien (IKT) har gjennomgått en enorm utvikling de siste 20 årene og er på vei inn i stadig flere anvendelser. – Da blir vi mer sårbare for svikt i teknologien. Derfor må sikkerhetsløsningene utvikles i et kontinuerlig kappløp med utviklingen av nye produkter og tjenester, påpeker programstyreleder Leif Nilsen.

Forskningsprogrammet IKT SoS ble startet i 2003 og skulle dekke et fagområde som var i rivende utvikling mens forskningen pågikk. – Vi er inne i et slags kappløp hvor den teknologiske utviklingen skjer veldig fort, og da burde man egentlig utvikle sikkerhetsløsninger i samme takt. Men dessverre har sikkerheten en tendens til å bli en salderingspost preget av litt tilfeldige «lapper» i etterkant av systemutviklingen. Først når sikkerhet designes inn som en integrert del av systemarkitekturen, kan vi oppnå gode og helhetlige sikkerhetsløsninger. Både praktisk sikkerhetsarbeid og videre forskning må betraktes som en kontinuerlig prosess, sier Leif Nilsen, som har ledet programstyret i IKT SoS fra starten og frem til avslutningen i 2008.

– Vi har gjort veldig mye i løpet av programperioden, men ingen må finne på å tro at bevilgningene til denne forskningen kan avvikles fordi alle problemer er løst, tilføyer han.

Nilsen er spesialist i sikkerhetsfirmaet Thales Norway AS, som er en stor leverandør av sikkerhetsløsninger og krypteringsutstyr til det norske forsvaret og Nato. Han er også førsteamanuensis og foreleser i kryptologi ved Universitetsstudiene på Kjeller (UNIK).

Systemene skal tåle angrep

Mange har opplevd problemer med for eksempel internettforbindelser som svikter, tekstmeldinger som forsvinner, eller GPS-baserte navigasjonssystemer som gir feil informasjon.

– Slike problemer handler om brukernes opplevde kvalitet på de aktuelle tjenestene, og skyldes ofte tilfeldige tekniske eller menneskelige feil. Vi som jobber med sikkerhet må også ta hensyn til at konfidensialitet, integritet og tilgjengelighet blir bevart selv om systemene utsettes for bevisste angrep og sabotasje. I dag vet vi mye om systemarkitektur og grunnleggende teknologi, men det er ikke nok kunnskap om hvordan man designer og bygger sikre og gode systemer.

– Det er også et stort problem at IKT-baserte systemer blir stadig mer komplekse. Kompleksiteten er en veldig utfordring for sikkerheten, fordi det finnes så mange kombinasjoner og mulige ulike tilstander at ingen kan ha den fulle oversikten over hva som skjer når kjente funksjoner plutselig blir satt inn i nye sammenhenger. Da har det lett for å oppstå sikkerhetshull som kan utnyttes av folk med onde hensikter, påpeker Nilsen.

Økt fare for digitale innbrudd

I april og mai 2007 ble mange offentlige nettsteder i Estland og Litauen utsatt for dedikerte angrep som stengte mange av sidene, og mange av angrepene ble sporet til Russland. I august 2008 ble de georgiske myndighetenes nettsider sabotert på en liknende måte av «crackere», parallelt med at den russiske hæren rykket inn i Georgia.

– Dette viser at dedikerte angrep som slår ut informasjonssystemer er en reell trussel. I disse tilfellene var det mest of-

Fra venstre: Programkoordinator Bjørn E. Braathen, Norges forskningsråd; programstyre-medlemmene professor Einar Snekkenes, Høgskolen i Gjøvik; sikkerhetssjef Anne Reinsnes, Telenor ASA; spesialist Leif Nilsen, Thales Norway AS og sikkerhetsrådgiver Eva Skipenes, Nasjonalt Senter for telemedisin. (Foto: Bjarne Røsjø)

fentlige nettsider som ble rammet, men også næringslivet kan bli utsatt for slike angrep. I næringslivet står man overfor et tilleggsproblem, fordi mange styrings- og administrasjonssystemer er tilgjengelige via internett. Tidligere var det slik at for eksempel styringssystemene i prosessindustrien ble styrt via lukkede nettverk som bare kunne styres fra en skjerm på et kontor i den aktuelle bedriften, men nå er systemene i ferd med å smelte sammen med administrasjonssystemene. Det innebærer at det etableres veier fra internett inn til styringssystemene, og da blir det i alle fall teoretisk mulig at utenforstående kan bryte seg inn og styre for eksempel kraftproduksjonen fra et vannverk eller oljeproduksjonen fra en plattform i Nordsjøen. Det er – for all del – en ønsket utvikling at operatørene i oljebransjen skal kunne sitte på land og styre produksjonen i Nordsjøen istedenfor å måtte reise ut til en plattform, men da blir det altså veldig viktig å lage sikkerhetssystemer som er gode nok til å holde uvedkommende borte, påpeker Nilsen.

– Jeg er sikker på at oljeselskapene og de store industribedriftene gjør mye for å beskytte systemene sine, men slike sammenkoplinger lager nye sårbarheter og sikkerhetsutfordringer. Samtidig vet vi at mange mindre bedrifter ikke er godt nok sikret mot digitale innbrudd, tilføyer han.

Utdanning er svaret

Det finnes først og fremst ett svar på alle utfordringene, og det er kompetanseutvikling. – Dette forskningsprogrammets viktigste bidrag til økt sikkerhet er at vi har vært med på å utdanne doktorander som senere kan gå ut og være med på utviklingen av bedre sikkerhetssystemer i alle organisasjoner som driver med IKT. Det er også et håp om at disse kandidatene kan bidra til at sikkerhetskunnskap blir en integrert del av den generelle IKT-utdannelsen på alle nivå. Utdanning og kompetansebygging er derfor et godt svar på sikkerhetsutfordringene vi står overfor, sier Nilsen.

Operativt og konkret

Forskningsprogrammet IKT SoS har lagt mer vekt på operative og konkrete problemstillinger enn på teoretisk grunnforskning, i tråd med de signalene som fulgte den opprinnelige bevilgningen fra Nærings- og handelsdepartementet. – Vi har blant annet støttet prosjekter som har sett på organiseringen av sikkerhetsvirksomheten og metodene for rapportering innad i organisasjonene, forteller Nilsen.

En ting som er viktig å huske, er at sikkerhetsløsningene må utformes på en måte som er tilpasset menneskene som skal bruke dem. – Det hjelper for eksempel ikke at IT-avdelingen skifter passord en gang i måneden, hvis passordene er så innviklede at folk skriver dem på en lapp istedenfor å huske dem. Det er også ganske lett å ringe IT-avdelingen under falskt navn og be om nytt passord fordi man har glemt det i løpet av ferien. Her må det være gode rutiner, for en sikkerhetsløsning er aldri bedre enn det svakeste leddet, understreker Nilsen.

Programmet har vært finansiert av Nærings- og handelsdepartementet (NHD) og Fornyings- og administrasjonsdepartementet (FAD).

IKT sikkerhet og sårbarhet – IKT SoS

Forskningsprogrammet IKT sikkerhet og sårbarhet (IKT SoS) hadde som målsetning å frembringe og gjøre tilgjengelig ny viten og kunnskap som kan bidra til å øke sikkerheten og redusere sårbarheten ved bruken av dagens og morgendagens IKT-systemer. IKT SoS har støttet forskning som hadde til hensikt å studere, analysere og utvikle løsninger for bedret informasjonssikkerhet, slik at informasjon og informasjonsflyt ved bruk av IKT-systemer i organisasjoner kan gis en riktig beskyttelse mot uønskede hendelser, og at brukeres behov for sikkerhetsløsninger kan sikres gjennom tilstrekkelig tilgang til spisskompetanse for å kunne få utviklet dette.

Programmets målgrupper
Programmets målgrupper for gjennomføring av forskningsprosjekter var forskningsmiljøer ved universiteter, høgskoler og forskningsinstitutter som utfører brukerrettet forskning innenfor programmets fagområder. Forskningsmiljøene ble invitert til å samarbeide med bedrifter eller andre virksomheter som arbeider med informasjonssikkerhet. Både næringsliv, forvaltning, enkeltindivider og andre forskningsmiljøer er mulige brukere av resultater fra programmet.

Programmets støttemidler skulle bidra til å:
- Styrke den nasjonale kompetansen innenfor informasjonssikkerhet i dybde og bredde
- Bygge og videreutvikle faglige nettverk nasjonalt og internasjonalt og bidra til å koordinere norske aktiviteter for å oppnå bedre utnyttelse av forskningsmiljøenes arbeider
- Støtte nasjonale strategier innen IKT sikkerhet og sårbarhet
- Styrke norske forskningsmiljøer på et høyt faglig nivå slik at de kan bearbeide viktige spørsmål og utfordringer knyttet til sikkerhet i IKT-systemer
- Finne løsninger og bringe frem resultater som kan gi grunnlag for nasjonal industri og næringsutvikling innen sikkerhetsområdet og som kan hevde seg i et internasjonalt marked
- Finne metoder for å utvikle en sikkerhetskultur for trygg elektronisk forretningsdrift i norske virksomheter og ved annen bruk av IKT i samfunnet

Hovedtyngden av prosjektene skal fokusere på fagområder som forventes å være av betydning for framtidig norsk nærings- og samfunnsliv. Det skal legges vekt på tiltak for å formidle resultatene av programmet fra forskningsmiljø til brukere i nærings- og samfunnsliv. Programmet vil prioritere prosjekter der resultatet av FoU fra et informasjonssikkerhetssyn bidrar til å:
- Gjøre systemer og infrastruktur for elektronisk informasjonsutveksling robust og sikker
- Utvikle innbyggeres og virksomheters holdninger slik at det bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling
- Etablere nye tjenester og produkter der sikkerhetsteknologi muliggjør nye måter å arbeide på, nye forretningsmodeller eller høyere effektivitet og god brukervennlighet
- Utvikle, vedlikeholde og håndheve lover og forskrifter slik at de fremstår og kan anvendes på en enkel og oversiktlig måte
- Muliggjøre deteksjon og sporing av sikkerhetshendelser med pålitelige og effektive metoder
- Redusere kostnadene forbundet med etablering av riktig informasjonssikkerhet for målgruppen


Foto: Photodisc


Foto: Shutterstock

Foto: Shutterstock og Bjarne Røsjø

Det nasjonale IKT-sikkerhetsarbeidet trenger nytenking

Det er behov for nytenking rundt det offentliges rolle i det nasjonale IKT-sikkerhetsarbeidet. Det har kommet mange forslag til tiltak når det gjelder IKT og sikkerhet, men det som mangler mest er gode rammebetingelser for at tiltak kan utvikles og inngå i en helhetlig og kontinuerlig arbeidsprosess.

– Utgangspunktet for dette prosjektet var at IKT er blitt veldig viktig for vårt moderne samfunn, og vi vet at en svikt i sentrale systemer vil skape enorme problemer. Hva skal vi gjøre for å unngå at IKT-problemer fører til at strømmen går, trafikken stanser eller at penger ikke blir utbetalt? Vi har ikke noe godt svar på disse problemene i dag. Sikkerhetstenkningen bør inn i en kontinuerlig prosess på nasjonalt plan, sier forsker Håvard Fridheim ved Forsvarets forskningsinstitutt (FFI).

FFI startet sitt første prosjekt i serien «Beskyttelse av samfunnet» (BAS) i 1994, og publiserte blant annet en rapport om IKT i 1999 med konkrete forslag til nasjonale tiltak og strategier.
– På den tiden hadde verken mobiltelefoni eller internettbruk tatt helt av, det var fortsatt slik at nesten alle brukte bare fasttelefon. I dag går utviklingen enda fortere enn for ti år siden, og hvis vi lagde en tiltaksliste nå ville den fort bli utdatert, påpeker Fridheim.

Et mer generelt nivå

I BAS5-prosjektet (2004–2007) har forskerne derfor løftet problemstillingene opp på et mer generelt nivå. Prosjektmedarbeiderne har utviklet en metodikk og en prosess for identifisering og prioritering av kritiske samfunnsfunksjoner og IKT-systemer. Det er også utviklet en prosess for risikoanalyser av samfunnskritisk IKT, i form av et rammeverk som understøtter valg av analysemetoder og en veileder for støtte til personer som skal gjennomføre risikoanalyser. Doktorgradsstipendiaten Janne Hagen er dessuten i ferd med å vurdere metodikker for effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer.

BAS5 har vært et samarbeidsprosjekt mellom flere forskningsinstitusjoner samt myndigheter og offentlige og private virksomheter, og for eksempel Kredittilsynet har allerede tatt inn informasjon fra prosjektet i sine veiledere.

Den viktigste anbefalingen

– Den viktigste anbefalingen fra FFI i forlengelsen av BAS5 er at det bør etableres nødvendige rammebetingelser for at det kan gjennomføres kontinuerlige og metodisk baserte arbeidsprosesser innen arbeidet med nasjonal IKT-sikkerhet, sier Fridheim.

Han påpeker at det blant annet er vanskelig å se en helt klar målsetting med sikkerhetsarbeidet i Norge i dag.

– Dette er en stor og tung problemstilling som blant annet henger sammen med at Norge har et sterkt sektorprinsipp i forvaltningen. Det ene departementet har ansvaret hvis det skjer noe innen kraftforsyningen, et annet departement har ansvaret hvis det skjer noe i teletjenestene, og så videre. Midt oppe i dette har vi IKT som griper inn i alle sektorer, og man har ikke gitt noe fullgodt svar på hvordan IKT-sikkerhet på tvers skal ivaretas. Dette er for øvrig ikke noe særnorsk fenomen, forklarer Fridheim.

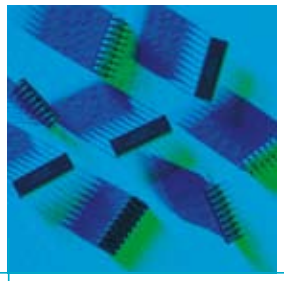


Foto: Bjarne Røsjø

Tidligere statsminister og fylkesmann Kåre Willoch har foreslått at det bør etableres et slags sikkerhetsdepartement som kan koordinere det nasjonale krise- og beredskapsarbeidet, og det synes Fridheim er en interessant tanke. – Men forslaget innebærer også en del utfordringer. Hvor skulle man for eksempel sette grensen for et slikt departement? Det ville jo få et veldig stort nedslagsfelt hvis det skulle gå inn i alle sektorer, innvender han.

FFI-rapporten peker derfor på et stort behov for nytenking. – Det offentlige hadde tidligere en sterk rolle i den nasjonale infrastrukturen, ikke minst fordi man eide store deler av den. Men i dag har det skjedd en deregulering som har medført at det isteden er private aktører som eier samfunnsviktig infrastruktur. Dessuten er jo de norske myndighetenes mulighet til å regulere for eksempel internett på globalt nivå ganske begrenset, for å si det mildt. Derfor er det nødvendig med en debatt om hva man ønsker å oppnå, mener Fridheim.

Prosjektet:

Prosjektleder:
Forsker Håvard Fridheim, Forsvarets forskningsinstitutt (FFI).

BAS5 – Critical Information Infrastructure Protection

Doktorgradsstipendiat:
Janne Hagen: Forsker ved FFI, stipendiat ved Universitetet i Oslos Institutt for informatikk og Norwegian Information Security laboratory (NISLAB) ved Høgskolen på Gjøvik

Viktige publiseringer:

- H. Fridheim, J. Hagen, «Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport», FFI/RAPPORT-2007/01204, 2007
- Senter for risikostyring og samfunnssikkerhet (SEROS), «Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT», SEROS-Rapport nr 91892, 2007.
- S. Henriksen, K. Sørli, L.Bogen, «Metode for identifisering og rangering av kritiske samfunnsfunksjoner», FFI/RAPPORT-2007/00784, 2007

Oljebransjen bør satse mer på informasjonssikkerhet

Den norske oljebransjen har hittil ikke vært tilstrekkelig opptatt av informasjonssikkerhet, men det blir nødt til å endre seg i nær fremtid. Bransjen er nemlig midt inne i et teknologisk paradigmeskifte som kan gjøre plattformer og andre installasjoner mer sårbare for virusangrep, hackere og andre digitale trusler.

Oljebransjen har nedlagt mye arbeid i det sikkerhetsarbeidet som innebærer at operasjonene ikke skal skape trusler mot liv og helse. – Men oljeselskapene og leverandørindustrien har ikke vært like flinke til å fokusere på et annet aspekt, nemlig informasjonssikkerheten. Det finnes fortsatt ikke gode nok rutiner på dette området, forteller forsker Martin Gilje Jaatun. Han er faggruppeleder for informasjonssikkerhet ved SINTEF IKTs Avdeling for systemutvikling og sikkerhet. Informasjonssikkerhet kalles også datasikkerhet og handler om å beskytte datasystemer mot hackere, virus, ormer og andre typer angrep.

Fremtidens oljeproduksjon i Nordsjøen kommer til å bli styrt fra landbaserte kontrollrom som likner dette testrommet, som er utviklet av NTNU, SINTEF og IFE. (Foto: Center for Integrated Operations in the Petroleum Industry – IO Center)

IKT i oljebransjen har tradisjonelt blitt brukt til å styre lukkede prosesser uten kobling til omverdenen, og det fantes ingen beskyttelsesmekanismer av den typen som har vært nødvendig i den landbaserte og nettverksbaserte IKT-bransjen, som bruker mye internett og epost. Men nå er oljebransjens produksjonssystemer og administrasjonssystemer i ferd med å smelte sammen, fordi utviklingen går raskt i retning av det som kalles Integrerte Operasjoner (IO). IO går kort fortalt ut på økt IKT-støtte til operasjoner på oljeplattformer og andre installasjoner. Dette manifesterer seg i alt fra samhandling i sann tid mellom operasjonsrom på hav og land, til fjernstyring av prosesser på sokkelen av personell som sitter ved vanlige pc-er i nettverk på land. Dette skaper helt nye

Prosjektet:

Prosjektleder 2005-2006: Odd Helge Longva, SINTEF IKT

Prosjektleder 2006-2007: Martin Gilje Jaatun, SINTEF IKT

From Incident Response to Incident Response Management: Case studies from the oil and gas industri (IRMA)

Viktige publiseringer:

- M. B. Line, E. Albrechtsen, S. O. Johnsen, O. H. Longva, and S. Hillen, «Monitoring of Incident Response Management Performance,» Konferansepublikasjon, International Conference on IT-Incident Management & IT-Forensics (IMF 2006), Stuttgart, Germany 2006
- S. O. Johnsen, C. W. Hansen, M. B. Line, Y. Nordby, E. Rich, and Y. Qian, «CheckIT – A program to measure and improve information security and safety culture,» International Journal of Performability Engineering vol. 3(1 Part II), pp. 174-186, 2007.
- M. B. Line, E. Albrechtsen, M. G. Jaatun, I. A. Tøndel, S. O. Johnsen, O. H. Longva, I. W.: A Structured Approach to Incident Response Management in the Oil and Gas Industry. Konferansepublikasjon, 3rd International Workshop on Critical Information Infrastructures Security (CRITIS'08), October 13-15, 2008, Frascati (Rome), Italy

problemstillinger, fordi produksjonssystemene risikerer å bli eksponert for både virus og ormer og andre trusler som tidligere bare kunne ramme «vanlige» bedrifter.

Hendelser blir underrapportert

Forskere ved SINTEF IKT og SINTEF Teknologi og samfunn har dybdeintervjuet nøkkelpersoner i oljebransjen for å undersøke hvordan det står til med informasjonssikkerheten. De konstaterte at det har vært et økende antall såkalte sikkerhetshendelser ved produksjonssystemene de siste årene, men ingen av dem har så langt fått alvorlige konsekvenser.

– Vi tror det er mye underrapportering på dette området. Oljebransjen har gode systemer for å rapportere hendelser som kan true liv og helse, men de samme systemene kan vanskelig brukes for å rapportere for eksempel virusangrep eller andre hendelser som kan true informasjonssikkerheten. Dataprogrammene som brukes har for eksempel ikke kategorier eller felter som passer til formålet. Det har også forekommet at operatører har vært usikre på om de egentlig var utsatt for en hendelse, eller om de kanskje gjorde en feil som kunne rettes ved å slå pc-en av og på igjen. En tredje årsak til underrapportering kan være at folk er usikre på hva slags konsekvenser en rapportering kan få for dem selv, forteller Jaatun.

Det konkluderes derfor med at oljebransjen bør fokusere sterkere på informasjonssikkerhet i fremtiden.

– Vi tror det bør gjøres en økt innsats for å utvikle indikatorer som proaktivt kan måle sikkerheten ved de ulike installasjonene. Hvis bransjen utvikler en falsk følelse av sikkerhet fordi det hittil ikke har vært mange hendelser, risikerer den å bli utsatt for en flodbølge av angrep i fremtiden, heter det i en rapport fra IRMA-prosjektet.

Plattformsjefene passer på

– Under dybdeintervjuene har vi fått høre om flere mindre hendelser som kunne ha utviklet seg til noe dramatisk. Skrekkscenariet er at en hacker bryter seg inn og overtar styringen av en hel oljeplattform, men noe slikt har ennå ikke skjedd så langt vi vet. Men det vi har hørt om, er at datautstyr i et prosessmiljø er blitt ustabilt på grunn av en virusinfeksjon. Slike angrep har foreløpig ikke fått store konsekvenser, og i dagens situasjon har man faktisk en ekstra sikkerhet fordi det fortsatt finnes folk på plattformene. Plattformsjefene har muligheten til å overstyre alt som skjer der ute. Men om noen år, hvis IO fører til at bemanningen på plattformene reduseres til et minimum, kan dette bli et større problem, utdyper Jaatun.

Mye velvilje

SINTEF-forskerne har med andre ord funnet mye å sette fingeren på i oljebransjen, men Jaatun understreker at de også har møtt mange interesserte og velvillige nøkkelpersoner. – Vi har imidlertid følt på kroppen at informasjonssikkerhet ikke alltid står høyest på agendaen. Vi hadde et tett samarbeid med Hydro og så fram til å utprøve

Gode metoder gir bedre sikkerhet

IRMA-metoden hos Statoil, men under fusjonsprosessen som førte fram til etableringen av StatoilHydro ble dette arbeidet – forståelig nok – i praksis lagt på is. Nå er prosjektet vårt slutt, og SINTEF er avhengig av ferske prosjektmidler for å videreføre arbeidet, sier Jaatun.

– Men, for all del: For oss som enkeltforskere har samarbeidet med Hydro, Oljeindustriens Landsforbund og Petroleumstilsynet vært veldig verdifullt. Det har gitt oss et nytt innblikk i bransjen, som har gjort det mulig å si noe om tilstanden. Hvis vi fikk muligheten, vil vi i fremtiden gjerne gå nærmere inn på hvordan man skal kunne måle informasjonssikkerheten. Det er også viktig å studere det vi kaller nesten-hendelser nærmere, med tanke på å kunne lære noe også av de hendelsene som ikke fikk konsekvenser. Dessuten ser vi at sammenhengene mellom sikkerhet for liv og helse (safety på engelsk) og informasjonssikkerhet (security) er et uutforsket område. Her er det mye å ta tak i, konstaterer de to.

– Oljebransjen selv snakker om at overgangen til Integrerte Operasjoner skal kunne skape gevinster i størrelsesorden hundrevis av milliarder. Dette er altså prosesser av enorm viktighet for både bransjen og hele landet. En god informasjonssikkerhet, innbefattet gode metoder og teknikker for registrering og håndtering av uønskede hendelser, er helt nødvendig for å muliggjøre denne viktige overgangen, sier Jaatun til slutt.

Hendelseshåndtering i oljebransjen har mange paralleller til brannslukking: Det er om å gjøre å ha et brannvesen som er godt forberedt, og som vet hva de skal gjøre når det skjer noe. I IRMA-prosjektet er det utviklet en metode som kan brukes både til å håndtere uønskede hendelser, og til å lære av dem etterpå.

– IRMA-metoden i et nøtteskall består av tre faser. Først må man forberede seg på uønskede hendelser, deretter må man oppdage hendelsen og gjenopprette en normal drift, og deretter skal man trekke lærdommer av hendelsen. Det kan være vanskelig å lære av enkeltstående hendelser som aldri vil bli gjentatt, så derfor er det viktig at man utvikler robuste systemer som også kan håndtere uventede hendelser, sier Jaatun.

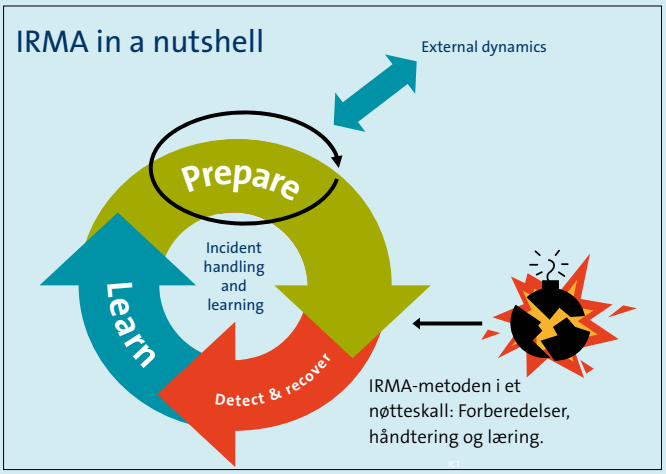
IRMA-metoden er først og fremst utviklet med tanke på oljebransjen, men den kan også anvendes i andre typer industribedrifter som anvender prosesskontrollsystemer og integrerte eller fjernstyrte operasjoner.

Det er veldig viktig at man bruker hendelser som grunnlag for videre læring. Men det forutsetter at hendelsene blir rapportert, og det forutsetter igjen at det finnes gode rutiner som sørger for at rapportene virkelig blir brukt! Ingen ting er så frustrerende som å bruke tid og krefter på å rapportere hvis man ikke ser nytten av det.

I regi av IRMA-prosjektet er det også utviklet et skjemabasert måleverktøy – CheckIT – som kan brukes til å måle den eksisterende sikkerhetskulturen og forbedre den. Statoil, Hydro, Telenor og Nasjonal Sikkerhetsmyndighet (NSM) har deltatt i dette arbeidet.

I regi av Oljeindustriens Landsforeningen (OLF) er det utviklet grunnleggende retningslinjer for informasjonssikkerhet i olje- og gassektoren. IRMA-prosjektet har inngått i og er en del av dette arbeidet.

IRMA-forskerne har også samarbeidet tett med prosjektet AMBASEC, som ble ledet fra Universitetet i Agder (se egen artikkel).



IRMA-metoden i et nøtteskall: Forberedelser, håndtering og læring.

Integrerte operasjoner: En lang ferd mot det ukjente

Oljebransjens overgang fra tradisjonelle til integrerte operasjoner er en lang ferd mot det ukjente, sier professor José Julio Gonzalez. En rask overgang kan skape økt sårbarhet for kostbare feil eller ulykker, men samtidig er det enorme gevinster å hente hvis endringene gjennomføres så fort som mulig.

Overgangen til integrerte operasjoner (IO) er en av de viktigste endringene som nå pågår i petroleumsvirksomheten, og bransjen venter seg tresifrede milliardbeløp i gevinster. StatoilHydros Brage-plattform, som begynte å produsere olje i 1993, gir en god illustrasjon på hva som foregår.

– Brage har vært case i vårt forskningsprosjekt, og der begynte de å planlegge overgangen til IO i 2003/2004. Det første skrittet gikk ut på å overføre planleggingen av den daglige produksjon til det som kalles eDrift, og som går ut på at produksjonen skal bli fullstendig digitalisert og nettverksbasert. Overgangen ble grundig planlagt, og seks-åtte måneder etter starten på prosjektet var den nye prosessen grundig testet og validert. Men det er minst 20 prosesser på en plattform som må igjennom en slik prosess før overgangen til IO er fullført, og alle prosessene er ferder inn i det ukjente, forteller professor José Julio Gonzalez.

Han har vært leder for AMBASEC-prosjektet, som har samarbeidet med SINTEF-miljøets IRMA-prosjekt og utviklet en modellbasert tilnærming til informasjonssikkerheten i oljebransjens IO-baserte fremtid.

Reduserer kunnskapsgapet

I AMBASEC har forskerne tatt utgangspunkt i de mentale modellene oljebransjens egne eksperter har dannet seg av overgangen til IO. – Disse modellene har vi brukt til å lage en simuleringsmodell som kan brukes til å vurdere risikoutviklingen under overgangen. Dette har betydning også for HMS-arbeidet på plattformen, fordi informasjonssikkerhet og HMS er tett knyttet til hverandre, sier Gonzalez.

– Det er altså ca. 20 prosesser bare på Brage-plattformen som skal overføres til ny teknologi. Man begynner med de gamle og plattform-orienterte prosessene, og så innfører man gradvis nye prosesser, som naturlig nok befinner seg i en testingsfase til å begynne med.

Det trengs ny kunnskap for å drifte de nye prosessene, men den kunnskapen finnes ikke i noen lærebøker – den må isteden utvikles underveis. Etter hvert som kunnskapene utvikles og prosessene blir forbedret, utvikles det moden kunnskap, tilføyer han.

Det eksisterer altså et kunnskapsgap mens overgangen pågår, og AMBASEC-prosjektet har dokumentert at kunnskapsgapet øker hvis prosessene drives for fort fremover. Et økende kunnskapsgap innebærer også økende risiko, og i det perspektivet er det en fordel å «ile langsomt». – Men det finnes også en kostnadsanalyse som viser at en langsom overgang reduserer verdien av overgangen til IO. Oljeselskapene må derfor i praksis veie muligheten for store gevinster opp mot en redusert informasjonssikkerhet. Våre modeller er et hjelpemiddel til å undersøke hvilke fordeler og ulemper som oppstår når man tar seg bedre tid til å gjennomføre prosessene, slik at de har mer å holde seg til når de skal vurdere tempoet i fremdriften, sier Gonzalez.

Brage-plattformen begynte med innføringen av eDrift i 2003/2004. (Foto: Marit Hommedal / StatoilHydro)

Prosjektet:

Prosjektleder: Professor José Julio Gonzalez, Universitetet i Agder, Fakultet for teknologi.

A Model-Based Approach to Security Culture (AMBASEC)

Mer informasjon:
http://ikt.hia.no/sqo/

Doktorgradsstipendiater og postdoktorer:
Ying Qian, Universitetet i Agder
Stefanie Hillen, Universitetet i Agder

Viktige publiseringer:

- Rich, E., F.O. Sveen, Y. Qian, S.A. Hillen, J. Radianti, and J.J. Gonzalez. *Emergent vulnerability in Integrated Operations: A proactive simulation study of risk and organizational learning*. In *Fortieth Annual Hawai'i International Conference on System Sciences (HICSS-40)*. 2007. Waikoloa, Hawaii.
- Sveen, F.O., J.M. Sarriegi, E. Rich, and J.J. Gonzalez, *Toward viable information security reporting systems*. Information Management and Computer Security, 2007. 15(5): p. 408-419.
- Rich, E. and J.J. Gonzalez. *Maintaining Security and Safety in High-threat E-operations Transitions*. In *39th Hawaii International Conference on Systems Science (HICSS-39)*. 2006. Kauai, Hawaii.

Som hullene i en sveitserost

AMBASEC-modellene omfatter både harde fakta og «myke» faktorer i form av menneskelige vurderinger.

– Det er bedre å anslå en verdi på en myk faktor enn å neglisjere den. Hvis du neglisjerer en slik faktor gir du den nemlig en verdi, det vil si null, og det er nødt til å være feil. Det er bedre å være omtrent riktig enn nøyaktig feil, sier Gonzalez.

– Redusert informasjonssikkerhet betyr at det oppstår ulike sårbarheter som kan utnyttes av eksterne personer med tvilsomme hensikter, eller som kan føre til at systemene ikke fungerer som de skal. Sårbarheten kan sammenliknes med hullene i en sveitserost. Hvis hullene ligger hver for seg er osten fortsatt fast og fin, men det skjer et uhell hvis hullene ligger på linje slik at du kan falle tvers gjennom osten. I sveitserosten ligger hullene fast hele tiden, men i oljebransjens overgang til IO er hullene i stadig bevegelse, illustrerer Gonzalez.

Foto: Shutterstock

Digitale tidsstempler avslører kriminelle

En av kriminaletterforskernes viktigste oppgaver er å finne ut hva som skjedde, og i hvilken rekkefølge det skjedde. Mange kriminelle databrukere har lært seg å forfalske de elektroniske tidsstemplene som ellers kunne fastslått forbrytelsenes tidspunkt og rekkefølge, men nå er det utviklet metoder og algoritmer som kan avsløre slike forfalskninger.

Hver eneste gang du redigerer eller lagrer et dokument på pc-en, sender en tekstmelding fra mobilen, eller tar et bilde med det digitale kameraet, blir det generert et digitalt tidsstempel som registrerer når handlingen ble utført. Slike tidsstempler kunne i prinsippet vært gull verdt for politiets etterforskere, men problemet er at stemplene ikke er til å stole på.

– Tidsstemplene i en pc forholder seg til datamaskinens klokke, men den kan lett stilles. Det går også an å forandre et tidsstempel etter at det er lagret, og det har derfor vært vanskelig å bruke disse tidsstemplene i etterforskningen. Man var i praksis avhengig av å sammenlikne tidsstemplene med eksterne tidsreferanser, men hvis det ikke fantes slike ble det veldig vanskelig. Derfor har vi ofte sett at forsvarerne i for eksempel saker om barnepornografi bruker falske tidsstempler som grunnlag for å påstå at det er «noen andre» som har lagret bildene, forklarer sikkerhetseksperten Svein Yngvar Willassen.

Ingen lurte programmet

I fremtiden kan det bli vanskeligere for de kriminelle å skjule sine elektroniske spor, for Willassen har utviklet et dataprogram som kan kontrollere og sammenlikne alle tidsstemplene i en maskin – pc, mobiltelefon, kamera osv – med hverandre. Det har nemlig vist seg at det er veldig vanskelig å forfalske alle tidsstemplene i et system på en konsistent måte. Det vil alltid oppstå avvik eller andre spor som kan påvises.

– Underveis i prosjektet utfordret vi en rekke ressurspersoner til å forfalske et gitt dokument på en måte som var inspirert av den såkalte Finance Credit-saken. Der hadde en av de hovedtiltalte skrevet et dokument som overførte aksjer til datteren, men påtalemyndigheten mente at dokumentet var skrevet i ettertid og tilbakedatert. Alle de vi utfordret klarte å forfalske tidsstemplet på sitt elektroniske dokument, men ingen klarte å lure programmet som undersøkte og sammenliknet alle tilgjengelige tidsstempler. Derfor mener vi at dette er en ny metode som kan være veldig anvendelig i digital etterforskning, sier Willassen.

Ligner litt på CSI

Svein Yngvar Willassen har bakgrunn som spesialetterforsker ved Datakrimteamet hos Økokrim. Han begynte på doktorgradsutdannelsen ved NTNUs Institutt for telematikk da TID-prosjektet startet i 2005. Arbeidet med doktorgraden ble godkjent og avsluttet i mai 2008, og nå har Willassen etablert en bedrift hvor han utvikler programvareverktøy som kan brukes innen digital etterforskning.

– Mange spør hva jeg synes om den amerikanske tv-serien CSI (Crime Scene Investigation), og jeg må si at de ofte tar opp prinsipper og metoder som er helt reelle. Men virkeligheten er nok ikke fullt så glamorøs og tabloidisert, kommenterer han.

Willassen forfølger flere gode ideer som selvstendig næringsdrivende. – Jeg er

Mange kriminelle har lært seg å forfalske digitale tidsstempler, men nye analysemetoder kan avsløre forfalskningene. (Foto: Shutterstock)

blant annet i ferd med å lage en søkemotor basert på ansiktsgjenkjenning, som skal kunne sammenlikne politiets «forbryterbilder» av ukjente kriminelle med ansikter som er publisert på internett. Digital ansiktsgjenkjenning er en velkjent teknologi, men jeg kjenner ikke til at funksjonen tidligere er lagt inn i en søkemotor på internett, forteller Willassen.

Den samme teknologien kan brukes til å jakte på overgriperne i barnepornografisaker, antyder han. – Alle kameraer har enten en liten feil i sensoren, eller en flekk på objektivet, eller et annet element som er helt unikt. Det skal gå an å gjenkjenne slike kamera-attributter og fastslå hvilket kamera som er blitt brukt til å ta et bilde. Da blir det mulig for politiet å gå etter de som har tatt de barnepornografiske bildene, som er de reelle overgriperne. I dag fokuserer man isteden på de som har lagret kopier av bildene.

Vitenskapelig grunnlag er nødvendig

Professor Stig Frode Mjølsnes ved NTNUs Institutt for telematikk var Willassens veileder i doktorgradsprosjektet. Da Mjølsnes søkte Forsk-

ningsrådet om bevilgning til prosjektet i 2004, skrev han blant annet at «digital etterforskning har vært – og er – en ad hoc- og praksisdrevet virksomhet som kan mangle et vitenskapelig grunnlag».

– Det er sant også i 2008, men situasjonen er i ferd med å bli bedre. Det er veldig flinke folk som driver med digital etterforskning, og vi ønsker å sette metodene og forståelsen inn i en prinsipiell og faglig sammenheng. Elektroniske spor som bevismateriale har de siste ti årene fått vesentlig økt betydning både i sivile og straffe-rettslige saker. Et vitenskapelig grunnlag og faglig metodikk er opplagt en fordel når digitalt bevismateriale skal føres og benyttes i rettssalen, sier Mjølsnes. Samfunnet etterspør denne innsikten, og NTNU har tatt opp den faglige utfordringen som ligger i dette.

– Elektroniske spor genereres både i VLSI-brikker, harddisker, mobiltelefoner, digitale kameraer, datamaskiner, printere, kopimaskiner, backupløsninger, cd-er, DVD-er, nettverksrutere samt programmer og kommunikasjonsprotokoller. Det er åpenbart at disse kildene inneholder et vell av informasjon for en etterforsker, og det er helt grunnleggende at rekkefølgen og årsakssammenhengen mellom hendelsene må klarlegges og kunne forklares. En etterforsker kommer jo til et åsted – som kan være fysisk eller digitalt – og observerer en del fakta. Deretter blir oppgaven å finne ut hva som skjedde, i hvilken rekkefølge, og etablere sannsynlige årsakssammenhenger innenfor en forklaringshypotese som gir plass til alle observerte fakta. Den digitale etterforskningsprosessen kan sammenliknes med å finne tilbake til hvor feilen oppstod i et datamaskinprogram, vel og merke i ettertid og kanskje uten mulighet for å kjøre programmet pånytt, forklarer Mjølsnes.

Personvern og etterforskning

Professor Mjølsnes og kollegene i Trondheim er opptatt av problemstillinger forbundet med informasjonssikkerhet i IKT-systemer. NTNUs Institutt for telematikk har fordypning i dette feltet på mastergradsnivå og planlegger nå etableringen av et undervisningstilbud innen digital etterforskning som en følge av prosjektet TID og samarbeid med Purdue University i USA. Et stort europeisk faglig kontaktnett er blitt etablert i TID-prosjektet, og professor Mjølsnes leder nå etableringen av et EU-konsortium for videre forskning i «Digital Forensic Investigations», som er den engelske betegnelsen.

– Det er velkjent at digitale spor kan innebære en trussel mot personvernet, og vi vet etter hvert mye om hvordan vi kan lage IKT-systemer uten digitale spor. Det nye anvendelsesaspektet i denne forskningen er at digitale spor også kan utnyttes i legitim etterforskning, konkluderer han.

Prosjektet:

Prosjektleder: Professor Stig Frode Mjølsnes, Institutt for telematikk, NTNU

Doktorgradsstipendiat NTNU: Svein Yngvar Willassen, nå i Inside-Out AS.

Time Stamps, Digital Traces and Forensic Evicence – TID

Mer informasjon:
http://www.item.ntnu.no/~sfm/research/overview.html

http://willassen.blogspot.com/2008/05/phd-thesis-published.html

Viktige publiseringer:

- S.Y. Willassen, «Using Simplified Event Calculus in Digital Investigation», ACM Symposium on Applied Computing 2008, Fortaleza, Brazil, March 2008
- S.Y. Willassen, «Finding Evidence of Antedating in Digital Investigations», ARES 2008, Barcelona, Spain, March 2008
- S.Y. Willassen, «Hypothesis Based Investigation of Digital Timestamps», 4th IFIP WG 11.9 Workshop on Digital Evidence in Kyoto, Japan, January 2008, in Advances in Digital Forensics IV, Springer, 2008

Store kommuner er blitt flinkere på informasjonssikkerhet

Det sto dårlig til med informasjonssikkerheten da Datatilsynet i 2003 undersøkte hvordan norske kommuner håndterte personopplysninger. – Siden den gangen har det skjedd overraskende forbedringer i mange kommuner, sier forsker Tommy Tranvik.

Da Personopplysningsloven trådte i kraft i 2001, innebar det blant annet at kommune-Norge måtte stramme inn metodene for håndtering av personopplysninger. Datatilsynet gjennomførte i 2003 en tilsynsrunde som avslørte mange og store problemer, og Tommy Tranvik var derfor forberedt på litt av hvert da han i 2007/2008 gjennomførte en ny kartlegging hos 18 større kommuner på Østlandet.

– Jeg ble faktisk litt overrasket over at tilstanden var såpass bra. Det gjenstår en del arbeid i disse kommunene, og flere av dem er fortsatt i en oppstartsfase, men jeg fant en større etterlevelsesgrad enn jeg ventet på forhånd, forteller Tranvik, som er forsker ved UiOs Avdeling for forvaltningsinformatikk.

Dårlig kommunal informasjonssikkerhet kan i verste fall få dødelig utgang, for eksempel hvis en pasient faller ut av hjemmesykepleiens arbeidslister. (Illustrasjonsfoto: Scanpix Denmark, Mikkel Østergaard)

Ikke representativt
Tranvik understreker at han ikke har studert et representativt utvalg av norske kommuner, men snarere de som skal være spydspissen i en utvikling. Han var nemlig opptatt av å undersøke kommuner som virkelig har gjort noe, for å få innsikt i hva som er utfordringene når det gjelder gjennomføring av Personopplysningsloven.

Rådmannen er ofte uoppmerksom
Tommy Tranvik er statsviter med doktorgrad fra Universitetet i Bergen og har arbeidet mye med spørsmål knyttet til politisk bruk av internettet, statlig styring og kommunalt selvstyre, digital teknologi og organisasjonsendring i frivillig sektor, og implementering av personvernlovverket i kommunal sektor.

– Mine undersøkelser viser at arbeidet er mye avhengig av ildsjeler og pionerer i de kommunene som har gjort fremskritt. Ildsjelene forteller ofte at de har en utfordring i forhold til særlig rådmannen, som er den øverste ansvarlige for at systemene er på plass. De må konkurrere veldig for å få rådmannens oppmerksomhet, og de vinner ikke alltid den kampen, forteller Tranvik.

Informasjonssvikt med dødelig utgang
Tranviks undersøkelser viser blant annet at kommunene ikke har vært utsatt for mange alvorlige hendelser som har truet informasjonssikkerheten. En typisk hendelse er at personnummeret ikke er slettet fra saksdokumenter i en elektronisk postjournal, og den slags fører fort til oppslag i lokale medier. Det finnes også eksempler på at kommuner har vært utsatt for hackingforsøk fra Asia eller Øst-Europa, uten at det har ført til alvorlige skadevirkninger.

Et sjeldent eksempel på at dårlig informasjonssikkerhet kan ha dødelig utgang, fant sted i en østlandskommune i 2003. Ved en feiltagelse ble en eldre pasient, som trengte fire besøk hver dag, slettet fra hjemmesykepleiens arbeidsliste. Etter fire dager uten tilsyn ble pasienten funnet hjelpeløs og sterkt forkommen i omsorgsboligen, og to dager senere døde pasienten på sykehuset. Hendelsen fikk store konsekvenser helt opp til rådmannens nivå, og kommunen har senere ryddet grundig opp.

Fokuserer på skolesektoren
Mer enn 80 kommuner er med i den frivillige organisasjonen KINS (Kommunal Informasjonssikkerhet), som ble etablert i 2003. Tranvik regner med at mange erfaringer fra «spydspiss-kommunene» kan spres gjennom KINS til andre kommuner, og det ligger i kortene at KINS og Kommunesektorens interesse- og arbeidsgiverorganisasjon (KS) er i ferd med å etablere et tettere samarbeid. – Men det er Datatilsynet som er, uten sammenlikning, den viktigste informasjonskilden for kommunene, forteller Tranvik.

Etablert samarbeid
Tranvik har nå etablert et samarbeid med Uninett ABC, som veileder norsk utdanningssektor om IKT og teknologivalg på vegne av Kunnskapsdepartementet.
– Vi skal se nærmere på hvordan personopplysningsloven og informasjonssikkerheten praktiseres i skolesektoren. Skolen har hittil hatt forholdssvikt svakt fokus på dette arbeidet, kanskje fordi skolen ikke behandler så mange sensitive personopplysninger som for eksempel helsesektoren. Man har heller ikke den samme taushetspliktkulturen, sier Tranvik.

Prosjektet:

Prosjektleder:
Professor Dag Wiese Schartum, Senter for rettsinformatikk, Universitetet i Oslo

Tommy Tranvik er forsker ved Avdeling for forvaltningsinformatikk (AFIN) ved Juridisk fakultet, Universitetet i Oslo

Legal Information Security Regulations – an Instrumental Perspective

Doktorgradsstipendiat:
Are Vegard Haug, Institutt for statsvitenskap, Universitetet i Oslo

Viktige publiseringer:
- Are Vegard Haug (2006): Rettslige reguleringer av informasjonssikkerhet. Complex nr. 2/2006. Oslo: Institutt for rettsinformatikk.
- Tommy Tranvik (2009): Lovpålagt selvregulering. Praktiseringen av personopplysningsloven i kommunene (forlag ikke avklart).

Foto: Shutterstock

Kryptografer lærer å tenke som kriminelle

Kryptografien har vært et kappløp mellom kodeutviklere og kodeknekkere helt siden Julius Cæsar fant på å sende hemmelige meldinger til sine generaler. – Det finnes ingen spilleregler. Derfor må kryptografi-studentene våre, som skal være «the good guys» i kappløpet, lære å tenke som om de var kjeltringer, sier professor Tor Helleseth.

Den såkalte Cæsar-koden var svært enkel, men illustrerer hva kryptografi går ut på. Den romerske hærføreren erstattet bokstavene i den egentlige meldingen med bokstaver som var forskjøvet et visst antall plasser i alfabetet. Med Cæsar-metoden og nøkkeltallet «3» kan for eksempel «Selmer» bli til «Vhophu».

– Kryptografi var tidligere en vitenskap som hadde størst interesse for militære og andre grupper med stort behov for hemmelighold, men i dag er vi alle sammen blitt avhengige av godt fungerende kryptografiske løsninger i dagliglivet. Hver gang du bruker nettbanken, slår på mobilen eller surfer på et trådløst nettverk, starter du en kryptografisk funksjon, sier Helleseth. Han er professor ved Selmer-senteret ved Universitetet i Bergen, som er oppkalt etter matematikeren Ernst Sejersted Selmer som «oppfant» de norske personnumrene i 1964. De siste to sifrene i personnummeret er i parentes bemerket lagd som en kombinasjon av de ni første, og Selmer lagde algoritmen («regneregelen») som brukes for å beregne kontrollsifrene.

En usikker hverdag

Det er lett å knekke Cæsar-koden, selv om antall skift er ukjent, for eksempel ved å prøve alle muligheter eller ved enkel frekvensanalyse. I både norsk og engelsk er nemlig «e» den hyppigst brukte bokstaven, og man kan derfor regne med at denne bokstaven forekommer oftest i en tekst. De kryptografiske løsningene som brukes i dag er mye mer avanserte enn Cæsars, men baserer seg fortsatt på hovedprinsippet om at en melding fra en avsender skal «forvrenges» ved hjelp av en nøkkel. Mottakeren må kjenne nøkkelen for å dekode og lese meldingen.

– I dag lever vi i en nokså usikker hverdag, fordi vi er avhengige av krypteringsløsninger som enten ikke er gode nok eller blir brukt på feil måte. De som bruker krypteringsløsninger trenger også mennesker som kan vurdere systemene og passe på at de blir brukt riktig. Det finnes en mengde knep som kan brukes for å lure kryptografiske systemer, og derfor må vi lære studentene våre å tenke som kjeltringer. Vi jobber hele tiden med å utvikle nye løsninger, og så utfordrer vi kolleger ved andre forskningsinstitusjoner til å «knekke» dem. På den måten utvikler faget seg hele tiden, forteller Helleseth.

Vakte stor oppsikt

Det hører med til sjeldenhetene at doktorgradsstudenter blir intervjuet av en nokså samlet norsk presse, men det skjedde da IKT SoS-stipendiaten Thomas Tjøstheim avslørte nettbankenes dårlige sikkerhetsløsninger i 2004. – Tjøstheim jobbet egentlig med digitale signaturer, men han tok også en titt på sikkerheten i Skandiabanken og ble sjokkert. Det var omtrent som å finne kredittkort på gaten! sier Helleseth, som var Tjøstheims veileder for masteroppgaven.

Skandiabanken har aldri innrømmet at det var Selmer-forskerne som fikk

dem til å endre rutinene, men det tok ikke lang tid før banken endret innloggingsprosedyrene og innførte et ekstra passord fra et kodekort eller via tekstmelding.

Forskerne ved Selmer-senteret har også vært opptatt av det som kalles Denial of Service (DoS) i norske nettbanker.
– I de første nettbankene logget man seg inn med et personnummer eller et kontonummer samt en kode. Da kunne du taste inn naboens personnummer samt feil kode tre ganger, og vips – så var han utestengt fra kontoen sin. Dette illustrerer at man bør passe godt på personnummeret sitt, og at det er viktig å utvikle gode kryptografiske løsninger som både er sikre mot at uvedkommende logger seg inn, og mot at uvedkommende saboterer tjenesten, sier Helleseth.

Høk over høk-chiffer
Selmer-senteret er med i et europeisk Network of Excellence (NoE) med 20 universitetspartnere og 10 industripartnere. Senteret er blant annet med på utviklingen av et nytt og veldig raskt

Den tyske Enigma-maskinen fra annen verdenskrig er verdenshistoriens mest myteomspunne krypteringsmaskin. I dag har kryptografene kommet atskilling lenger. (Foto: Shutterstock)

strømchiffer. Dette kan bli et supplement til den nåværende AES-standarden (Advanced Encryption Standard) for blokkchiffer.

– Kryptering ved hjelp av blokkchiffer går ut på at man deler opp meldingen i blokker på typisk 128 bit hver, og så krypterer man blokkene hver for seg. Det har vært jobbet i flere år med et EU-prosjekt som skulle utvikle et mye raskere strømchiffer, som kan kryptere meldinger fortløpende uten oppdeling. Til slutt utlyste prosjektet en konkurranse hvor postdoktorstudenten Aleksander Kholosha og nederlenderen Cees Jansen deltok, med meg som tredjemann i teamet. Vi kom helt til finalen med et chiffer som var veldig sikkert men litt for langsomt, forteller Helleseth.

Konkurransen er ennå ikke avsluttet, for nå forsøker Selmer-senteret å finne svakheter i de andre finalistenes chiffer – og omvendt. – Dessuten har vi funnet på noe smart som gjør det mulig å øke hastigheten på chifferet vårt med en faktor på 30. Da er vi blant de beste, sier en optimistisk Helleseth.

Analyserer hash-funksjoner

Professor Helleseths IKT SoS-prosjekt har – i tillegg til mange presseoppslag og finaleplass i en europeisk chiffer-konkurranse – gitt opphav til artikler i flere vitenskapelige journaler, sterk profilering på internasjonale konferanser, og sogar en film om kryptografi som ble vist på NRKs kunnskapskanal i april 2007. Thomas Tjøstheim har også analysert elektroniske valgsystemer og foreslått en sikker og skalerbar løsning for stemmegivning over internett.

Nå jobber Selmer-forskerne med såkalte hash-funksjoner, som brukes til å komprimere store filer før de skal signeres. – Vi har analysert flere eksisterende hash-algoritmer og funnet svakheter i dem. Dette kommer til å bli et hett internasjonalt emne de kommende årene, spår Helleseth.

Forskerne er også med i Norges forskningsråds VERDIKT-program med et prosjekt som handler om å bygge sensorer og mikrobrikker med innebygde kryptografiske algoritmer.

– Selv de beste kryptografene opplever av og til at systemene deres blir knekt. Jeg tror ikke at man noensinne kommer til å utvikle et praktisk system som er absolutt sikkert – og hvis man skulle klare det, kan man ikke være sikker på at systemet blir brukt riktig. Det er derfor stort behov for å drive en kontinuerlig forskning og utdanning på dette feltet, oppsummerer professor Helleseth.

Prosjektet:

Prosjektleder: Professor Tor Helleseth, Selmer-senteret, Universitetet i Bergen

Advanced Cryptographic Techniques (ACT)

Presseomtaler:
http://www.nowires.org/Press/Press.html

Doktorgradsstudenter og postdoktorer:
Thomas Tjøstheim, nå i EDB Business Partner
Alexander Kholosha, Institutt for informatikk, Universitetet i Bergen

Viktige publiseringer:

- C. Jansen, T. Helleseth and A. Kholosha, «Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher,» /New Stream Cipher Design - The eSTREAM Finalists, Lecture Notes in Computer Science (LNCS), /vol. 4986, pp. 224-243, /2008./
- H. Molland and T. Helleseth, «An improved correlation attack against irregularly clocked and filtered keystream generators,» /Proceedings 24th Annual International/ /Cryptology Conference (CRYPTO 2004), Lecture Notes in Computer Science (LNCS)/, Santa Barbara, CA, Aug. 15-19, 2004, vol. 3152, pp. 373-389.
- T. Tjøstheim, T. Peacock, and P. Y. A. Ryan, A Case Study in System-Based Analysis: The Three Ballot Voting System and Pret a Voter» presented at VoComp, Portland, USA, July16-18, 2007.

Tillit i digitaliseringens tidsalder

Det var vanskelig nok i «gamle dager» å vite hvem du kunne stole på, da du kunne ta folk i hånden og se vedkommende i øynene. Men hvordan skal vi håndtere tillit i digitaliseringens tidsalder? – Vi trenger nye metoder for å analysere og vurdere tillit, sier Ketil Stølen.

Hva skal til for å ha tillit til datamaskinen i den andre enden av forbindelsen? Det trengs nye metoder for tillitsstyring i den digitale tidsalderen. (Foto: Shutterstock)

Derfor tok Ketil Stølen, sjefsforsker ved Sintef IKTs Avdeling for samvirkende og tiltrodde systemer, initiativet til et prosjekt hvor det er blitt utviklet en metode for å analysere tillit i forhold til risiko i den digitale tidsalderen. Det er også utviklet et språk for å dokumentere resultatene av en slik analyse, og språket kan brukes til å lage retningslinjer for håndteringen av digital tillit i organisasjoner. Forskerne har dessuten vurdert hvordan risiko og tillit skal håndteres i forhold til kontrakter.

– Psykologer og filosofer har studert tillit i mange år, men i dag har vi fått behov for å vite hva det betyr at en datamaskin kan stole på en annen. Etter hvert som ulike datasystemer blir flinkere og flinkere til å samhandle, tar de stadig flere avgjørelser selv. Det har skapt et veldig behov for å forstå hvordan vi kan bygge systemer som kan gjøre dette på en sikker måte, sier Stølen.

Tillit er mer enn sikkerhet
– De fleste nettbankløsninger er lagd på en veldig sikker måte, men samtidig vet vi at datasystemer aldri blir 100 prosent sikre. Derfor vil du sannsynligvis kreve noe mer enn datasikkerhet for å ha tillit til nettbanken, for eksempel i form av lover og regler som sikrer at sparepengene dine ikke blir borte selv om noen hacker seg inn i nettbanken. Eksemplet viser at tillit er et mer generelt begrep enn sikkerhet, sier Stølen.

Jurist, filosof og IKT-forsker
Databehandleren Stølen inviterte derfor både juristen Jon Bing ved Universitetet i Oslo og filosofen Dag Elgesem ved Universitetet i Bergen med i prosjektet, som veiledere for to doktorgradsstipendiater.

– Eksemplet med nettbanken illustrerer behovet for juridisk kompetanse når vi skal jobbe med digital tillit. Filosofikompetansen var også viktig, fordi humanvitenskapene har studert tillitsbegrepet og bygd opp solide kunnskaper lenge før begrepet «tillitsstyring» (trust management) dukket opp i IKT-bransjen i 1996, forteller Stølen.

Validering av sertifikater
Den nye metoden blir nå anvendt i et prosjekt ved Det Norske Veritas (DnV), som er i ferd med å utvikle et dataprogram som skal kunne validere elektroniske sertifikater.

– Tenk deg at du skal kjøpe noe fra en netthandel i for eksempel Latvia og ønsker å sjekke kvaliteten på det elektroniske sertifikatet som er nødvendig for å gjennomføre handelen. Ideen er at man kan sende sertifikatet til DnVs valideringsprogram, som skal kunne avgjøre om sertifikatet er til å stole på. Prosjektet omfatter en stor analyse hvor DnV og Sintef bruker vår metodikk til å sammenlikne to alternative løsninger, forklarer Stølen.

Ketil Stølen påpeker at det alltid er viktig å analysere hvor komplekse dataløsninger som trengs i forhold til det målet som ønskes oppnådd.

– Det vi ser i praksis, er at systemer som gjøres for sikre, med for mye kompleksitet, kan føre til at mange begynner å lete etter måter å omgå systemet på. Hvis IT-avdelingen for eksempel bytter passord for ofte og krever at de skal være for komplekse, ender det med at brukerne skriver passordet på en lapp, og da blir sikkerheten svekket istedenfor styrket. Derfor gjelder det alltid at man må velge rett løsning, med rett kompleksitetsnivå, ut fra den målsetningen man har, sier Stølen.

Prosjektet:

Prosjektleder: Sjefsforsker Ketil Stølen. (Foto: Sintef)

Tool supported methodology for the formalization, analysis and enforcement of policies within trust management (Enforce)

Doktorgradsstipendiater og postdoktorer:
Tobias Mahler, Institutt for rettsinformatikk, Universitetet i Oslo
Bjørnar Solhaug, Institutt for informasjons- og medievitenskap, Universitetet i Bergen
Atle Refsdal, Sintef IKT

Viktige publiseringer:
- Atle Refsdal, Ketil Stølen: Extending UML sequence diagrams to model trust-dependent behaviour with the aim to support risk analysis. Antatt for publikasjon i Science of Computer Programming.
- Atle Refsdal, Bjørnar Solhaug, Ketil Stølen: A UML-based method for the development of policies to support trust management. Konferansepublikasjon, 2nd IFIP Conference on Trust Management, 2008.
- Tobias Mahler, Jon Bing: Contractual risk management in an ICT context - Searching for a possible interface between legal methods and risk analysis. Scandinavian Studies in Law (ISSN 0085-5944), 2006.

Helsepersonellet er bedre enn teknologien

Å legge fortrolige pasientopplysninger inn i datasystemer er en komplisert affære. Forskere som har sett på hvordan slike systemer fungerer i helsevesenet, konkluderer med at sunn fornuft og høy moral gir det beste personvernet. Det er et langt stykke igjen før teknologien kan sikre en god håndtering av pasientinformasjon.

I «gamle dager» ble opplysninger om pasienten sirlig skrevet ned og arkivert hos familielegen eller på sykehuset. I vår elektroniske hverdag forventer vi at det vi trenger å vite er et tastetrykk unna, noe som også har endret informasjonshåndteringen i helsevesenet. Et viktig aspekt er hvem som skal ha tilgang til hva slags informasjon. Fallgruvene er nemlig mange i forhold til personvern, taushetsplikt og administrasjon.

– Lovverket krever at det lages avanserte tekniske systemer for tilgangskontroll, og reglene er strenge. Et helseforetak har for eksempel ikke lov til å utlevere informasjon uten pasientens samtykke, og den som mottar informasjonen må ha rett til å behandle den

De som jobber med pasientjournaler og annen helseinformasjon har utviklet en praksis som er bedre enn det er mulig å oppnå med dagens datasystemer. (Foto: Bjørn Rørslett / NN / Samfoto)

aktuelle pasienten. Prinsippet er at ingen skal få informasjon de ikke trenger, sier førsteamanuensis Øystein Nytrø.

Ikke tilpasset virkeligheten

Nytrø har – sammen med seks forskere fra NTNU, SINTEF og UiO – sett på hvordan ulike sykehus og helseforetak kontrollerer tilgangen til helseinformasjon, både praktisk og teknisk.

– Vi har sett på hva personalet får lov til og ikke får lov til. Grensene er nokså klare i forhold til personvern, lovverk og administrative regler. Tilgangskontroll skal være bygget inn i helseinformasjonssystemene, men det gjenstår mye før vi har pasientjournalsystemer som er tilpasset behov og praksis. Intet system kan i dag forutsi nøyaktig hvem som har behov for hvilken informasjon i alle sammenhenger. Dagens modell for tilgang til helseinformasjon antar at alle sitter alene på kontor foran skjermen og jobber med en og en sak. Det passer dårlig med virkeligheten på et travelt sykehus, sier Nytrø.

Teknologien på etterskudd

En hovedkonklusjon fra forskerne er at det beste vernet mot overtramp er det som sitter i hodet på helsepersonellet selv. Det er allerede «innebygd» en god forvaltning hos dem som har tilgang til denne type informasjon:

– Praksisen som er utviklet er rett og slett bedre enn muligheten for et godt datasystem på dette feltet, slår Nytrø fast. Med et aldri så lite hjertesukk:

– Som teknolog blir jeg litt frustrert over at det er så vanskelig å få på plass velfungerende IT-løsninger. De finnes, men de er svært krevende å administrere og vedlikeholde. Vi må erkjenne at vi kanskje er urealistiske i troen på skreddersydde systemer som kan gjøre denne jobben. Norge har flere millioner pasienter, med mange mulige «avvik» og unntak per pasient, som egentlig er umulig å håndtere i et strømlinjeformet system med dagens teknologi, sier han. Om ti år tror han imidlertid situasjonen vil være en annen.

Bedre samsvar

I det videre arbeidet skal prosjektet blant annet se på såkalt «optimistisk tilgangskontroll». Her er det bærende prinsippet at helsepersonell gjør det de tror er riktig, men at «noen ser det de gjør» – altså at de må stå til ansvar. Det er delvis slik i dag, men Nytrø mener det må bli mer samsvar mellom praksis og policy.

– Vi må ta utgangspunkt i det som gjøres i praksis. Vi kan ikke bygge personvern gjennom kontrollregimer, da vil folk bare måtte sno seg rundt teknologien. Derfor trengs en teknologi som støtter opp om det som er naturlig å gjøre. Det har jo fungert nokså bra med papirbaserte systemer, så det er ingen grunn til å sette opp kontrollsystemer som ikke fungerer i den digitale virkeligheten.

Prosjektet:

Prosjektleder:
Førsteamanuensis Øystein Nytrø, NTNU, Institutt for datateknikk og informasjonsvitenskap

Integrated Access Control for Health Care Information Systems

Doktorgradsstipendiater:
Herbjørn Andresen, Avdeling for forvaltningsinformatikk, UiO
Gunnar René Øie, Institutt for datateknikk og informasjonsvitenskap, NTNU

Viktige publiseringer:

- Øie, Gunnar Rene; Andresen, Herbjørn and Tøndel, Inger Anne. Handling Consent to Patient Data Access in a Hospital Setting [online]. In: Medinfo 2007: Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems; pages: 242-246. Kuhn, Klaus A (Editor); Warren, James R (Editor); Leong, Tze-Yun (Editor). Amsterdam: IOS Press, 2007. Studies in health technology and informatics, ISSN 0926-9630
- Meland, Per Håkon; Rostad, Lillian; Tøndel, Inger Anne and Nytrø, Øystein. The iAccess Handbook: A Methodology for Access Control Integration [online]. In: Medinfo 2007: Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems; pages: [2015]-[2016]. Kuhn, Klaus A (Editor); Warren, James R (Editor); Leong, Tze-Yun (Editor). Amsterdam: IOS Press, 2007. Studies in health technology and informatics, ISSN 0926-9630
- Herbjørn Andresen. The Policy Debate on Pseudonymous Health Registers in Norway (Under utgivelse i bok.)

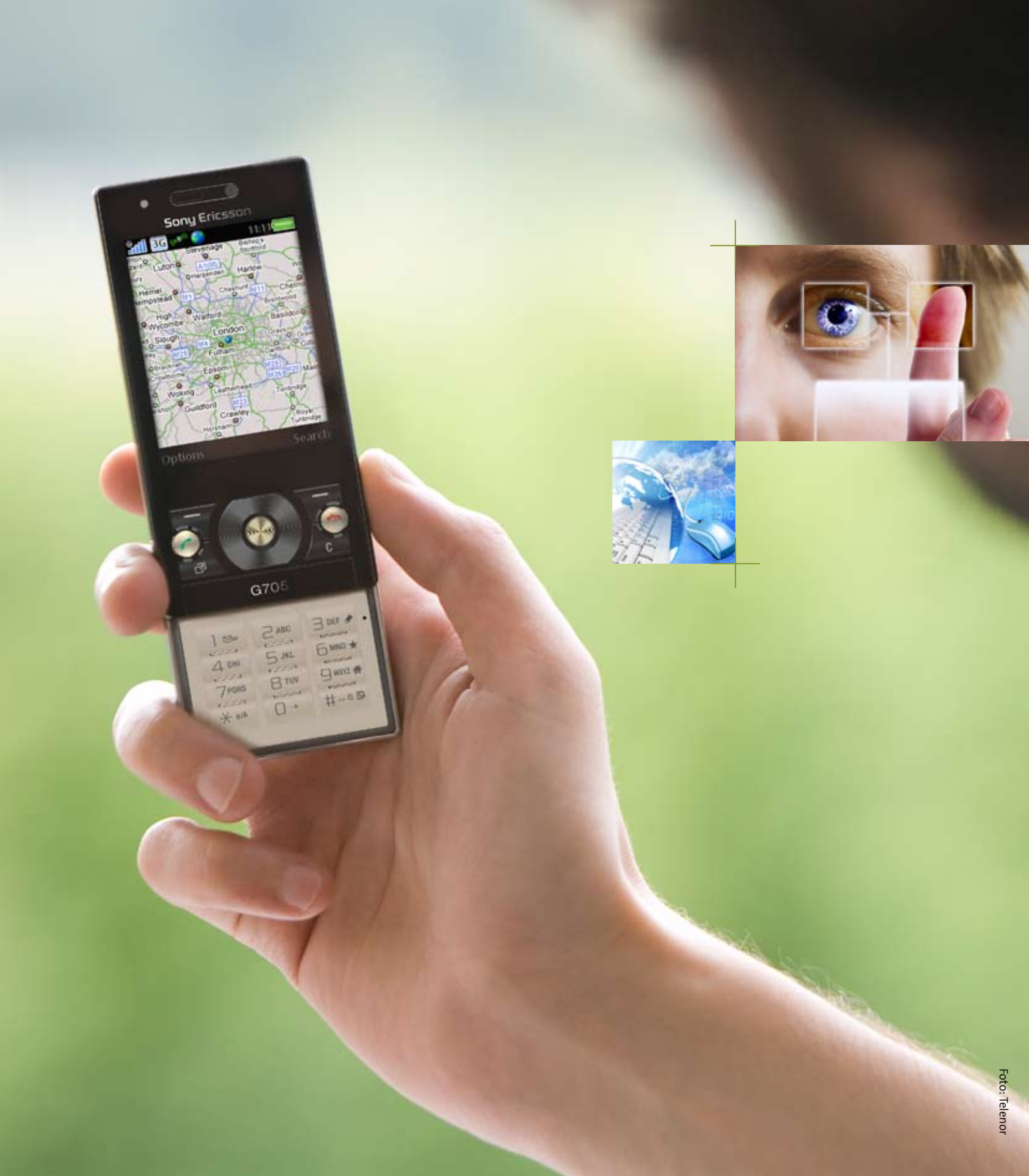


Foto: Telenor

Mobil nettbruk trenger økt sikkerhet

Mobiltelefonen er i ferd med å bli vår nye pc, men det er fortsatt store sikkerhetsmangler knyttet til internett-tjenester på telefonen. Det vil professor i datasikkerhet, Kjell Jørgen Hole, gjøre noe med.

Trenden er klar: Stadig flere internett-tjenester tilbys på mobiltelefonen, spesielt på de nye «smartphones» med gode skjermer og kraftige prosessorer. Å dra fram mobilen fra lomma når du skal betale en regning, er ingen fjern framtidsdrøm. Spørsmålet er om dette lar seg gjøre på en sikker måte.

– Det gjelder å finne gode rammeverk for sikker kommunikasjon. Hvis vi får til det, slipper vi å finne opp hjulet hver gang en ny tjeneste lanseres, sier Kjell Jørgen Hole, som er professor i datasikkerhet ved Universitetet i Bergen.

Han har ledet et prosjekt som har vurdert sikkerhetsnivået på mobiltjenester per i dag, evaluert og beskrevet svakheter, og sett på hvilke bedringer som trengs.

Avslørt svakheter

I framtida vil det sannsynligvis være mulig å ha full tilgang til tjenester på internett via mobiltelefon. Dermed vil alt vi gjør på nettet i dag teoretisk sett være mulig å gjøre via mobiltelefonen – enten man vil kjøpe en vare online eller fylle ut et skjema som skal sendes til en offentlig etat. Bankene er blant dem som ligger lengst framme i løypa.

– Det er allerede mobilbanker oppe og går. Riktignok er ikke alle tjenester tilgjengelige, bankene holder litt tilbake, men du kan i alle fall sjekke konto og betale regninger, sier Hole.

Men så var det sikkerheten, da. Hole fikk mye medieoppmerksomhet både i Norge og utenlands da han med enkle hacker-grep viste omverdenen at nettbankenes BankID var langt fra sikker nok.

– Vi fikk sparket i gang en viktig debatt om sikkerhet, selv om vi ikke hadde ant at det skulle bli så voldsomt. Én ting er at det fortsatt er store svakheter på internett – men når det gjelder mobiltelefonen er teknologien enda mer umoden. Telefonen har flere feil, sier Hole.

Han mener hovedutfordringen ligger i å få til bedre sikkerhet på selve telefonen og et bedre rammeverk for utvikling av sikre applikasjoner.

Lager oppskrift

Sammen med sine doktorgradsstudenter har Hole utviklet oppskrifter på hvordan man lager sikker programvare. Det dreier seg om «security patterns», som er måter å standardisere sikkerheten på. Men: Er det forskerne eller industrien som har kommet lengst med utvikling av sikkerhetssystemer?

– Når det gjelder utvalgte områder innen design av sikre systemer – avanserte kommunikasjonsprotokoller, hemmelig koding og den slags – ligger forskningen i front. Men når det gjelder forståelse av og tilgang til teknologi, ligger programvareindustrien i forkant. Bankene har for eksempel mange hundre programmerere, så vi kan ikke konkurrere på det nivået, svarer Hole.

Risiko i Norge

Kjell Jørgen Hole mener Norge er preget av at vi er raskt ute med ny teknologi, mens holdningen til sikkerhet ikke er like god. Den anerkjente amerikanske forskeren Gary McGraw har også sagt dette – at sikkerhetstenkningen i Norge ligger betydelig tilbake for den i USA, mens Norge er langt framme i bruken av teknologi.

– Dette er en dårlig kombinasjon. Hittil har vi vært så heldige at ingen har utnyttet det i stor skala. Norge er jo nokså skjermet, vi er ikke midt i Europa, og vi snakker et rart språk. Men det er ikke sikkert det forblir slik i framtiden. Det er stor fare for at også nordmenn skal oppleve identitetstyverier og sensitive opplysninger på avveie, sier Hole.

Han understreker at Universitetet i Bergen ønsker å ta sin del av ansvaret for bedret sikkerhet, blant annet gjennom å bli flinkere til å utdanne folk.

– Dette prosjektet har vært med å sette trykk på sikkerhet i undervisningen. Vi har flere og bedre kurs, og vi vil fortsette å utdanne doktorgradsstudenter i anvendt datasikkerhet. Vi har også fått større kontaktflate, blant annet gjennom et godt samarbeid med Datatilsynet og Kredittilsynet samt en dialog med industrien.

Prosjektet:

Prosjektleder: Professor Kjell Jørgen Hole, Universitetet i Bergen, Institutt for informatikk

Secure Wireless Application Programming (SWAP) for laptops and handheld devices

Doktorgradsstipendiater:
Vebjørn Moen, Thomas Tjøstheim, Yngve Espelid, André N. Klingsheim, Lars-Helge Netland

Viktige publiseringer:

- N. Klingsheim, V. Moen, and K. J. Hole, "Challenges in Securing Networked J2ME Applications," IEEE Computer, February 2007.
- K.J. Hole, L.H. Netland, Y. Espelid, A.N. Klingsheim, H. Helleseth, and J.B. Henriksen, «Open Wireless Networks on University Campuses,» IEEE Security & Privacy, July/August 2008.
- K.J. Hole, V. Moen, A.N. Klingsheim, and K.M. Tande, «Lessons from the Norwegian ATM System,» IEEE Security & Privacy, November/December 2007.
- K. J. Hole, V. Moen, and T. Tjøstheim, «Case Study: Online Banking Security,» IEEE Security & Privacy, March/April 2006.

Elektronisk analyse av ganglaget åpner nye muligheter

Vi er for lengst blitt vant til å taste et passord for å starte pc-en og en PIN-kode for å åpne mobiltelefonen. – En ny mulighet er å bruke ganglaget til gjenkjenning. Vi har testet elektroniske sensorer som kan analysere menneskers ganglag og bekreftet at dette kan få mange praktiske anvendelser, forteller professor Einar Snekkenes.

Det finnes et rikt utvalg av teknikker for autentisering (gjenkjenning) og identifisering av enkeltpersoner: Fingeravtrykk, irismønster, brukernavn og passord, PIN-koder, og så videre. Det finnes også eksempler på videobasert ansiktsgjenkjenning og til og med ganglagsgjenkjenning, basert på at de fleste mennesker går på en unik måte.

– Videokartlegging av ganglaget brukes mest til overvåking eller etterforskning, men vi ønsket å undersøke om også elektroniske bevegelsessensorer festet på kroppen kunne brukes til automatisk gjenkjenning (autentisering) av enkeltmennesker. Svaret er «ja», forteller professor Einar Snekkenes ved Høgskolen i Gjøviks NISlab (Norwegian Information Security laboratory).

En bevegelsessensor festet på ankelen kan identifisere ulike ganglag på en rimelig sikker måte. (Foto: Høgskolen i Gjøvik)

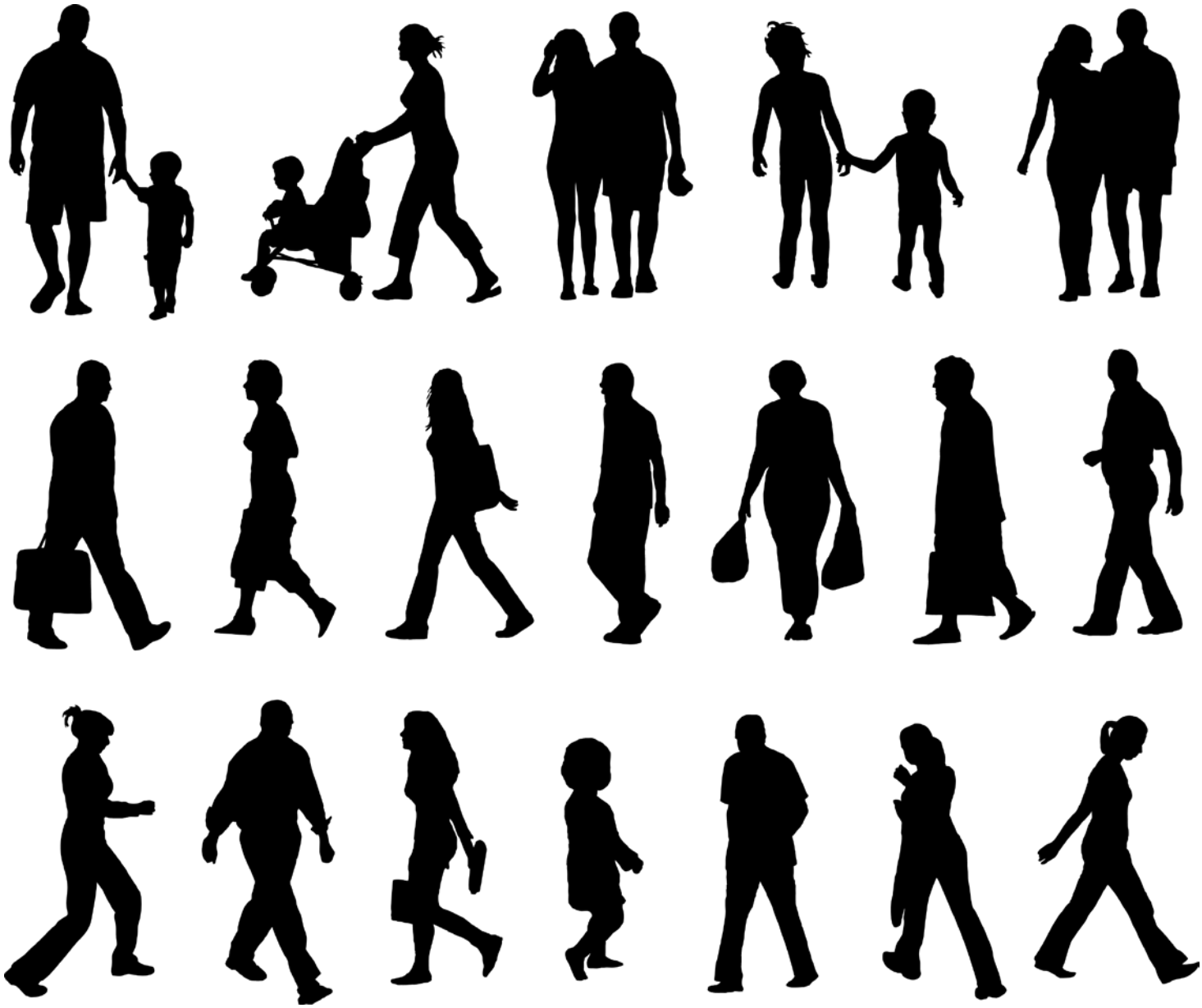
Alle nye biler er i dag utstyrt med kollisjonsputer som utløses av små elektroniske akselerasjonsmålere når de registrerer en tilstrekkelig brutal fartsreduksjon. Det er liknende sensorer basert på den såkalte MEMS-teknologien (Micro Electronic Mechanical Systems) som er blitt brukt i forsøkene med ganglagsgjenkjenning på Gjøvik. Sensorene er «hyllevare» fra store internasjonale elektronikkprodusenter, men forskerne ved Høgskolen i Gjøvik har utforsket nye bruksområder.

Forskerne på Gjøvik har blant annet festet sensorer ulike steder på kroppen, for å finne den optimale plasseringen for en trygghetsalarm. Det viser seg at ankelbevegelsene i sideretningen gir de største individuelle forskjellene. Det viser seg også at det er stor forskjell på menns og kvinners ganglag, og det ser ut til å være større forskjell innbyrdes mellom kvinner enn mellom menn.
– Dette høres kanskje opplagt ut, men det er viktig å dokumentere slike forhold hvis teknologien skal finne praktiske anvendelser, kommenterer Snekkenes.

Automatisk trygghetsalarm

– For å utnytte vår kunnskap om sensorteknologien og bevegelsesanalyse har vi sett nærmere på mulighetene for å utvikle en automatisk trygghetsalarm for eldre og syke mennesker. En trygghetsalarm basert på bruk av MEMS-sensorer vil for eksempel kunne sende et automatisk varsel, gjerne i form av en tekstmelding, til pårørende eller pleiere hvis den overvåkede personen faller eller blir liggende rolig påfallende lenge. Vi har et sterkt helsefaglig miljø ved Høgskolen i Gjøvik, og sammen med tidligere master-

Menneskers ganglag kan variere mye – så mye at elektroniske sensorer kan analysere bevegelsene og gjenkjenne enkeltpersoner. (Illustrasjon: Shutterstock)





student Torkjel Søndrol har vi utviklet en prototype på en slik trygghetsalarm, forteller Snekkenes.

Sensorene som er brukt i forsøkene er på størrelse med en halv lillefingernegl. De må kobles sammen med en mikroprosessor, et batteri og en liten radiosender for å kunne brukes, så derfor må en automatisk trygghetsalarm bli noe større.

Teknologi med store muligheter

Professor Snekkenes understreker at det er lang vei fra forskning til ferdig produkt.

– De gjenkjenningsforsøkene vi har gjort hittil, har fokusert på mennesker som går i vanlig tempo innendørs. Det som er kjernen i prosjektet, er at vi har verifisert en teknologi som kan brukes til veldig mye forskjellig. Forsøkene indikerer nemlig at elektroniske sensorer festet på kroppen også kan brukes til å analysere enkeltmenneskers ganglag og dermed gjenkjenne for eksempel eieren av en mobiltelefon. Det er fullt mulig å lage et system som opererer med 95 prosent sannsynlighet for riktig autentisering, og det vil i flere tilfeller være godt nok, forteller professor Snekkenes.

Flere mobiltelefonprodusenter har allerede begynt å montere inn bittesmå sensorer, på størrelse med et knappenålshode, i de mest påkostede modellene. Sensorene er kanskje i hovedsak tenkt brukt til spill og til å navigere i menyer ved å bevege telefonen. Men når mobiltelefonen først er utstyrt med en slik sensor, kan det også bli mulig å skrive et program som gjenkjenner eieren på ganglaget – eller kobler ut telefonen hvis den plutselig befinner seg i lomma på en tyv med et annet ganglag.

– I så fall må programvaren utformes på en gjennomtenkt måte. Det er ingen som vil ha en mobiltelefon som slutter å virke hvis du plutselig må løpe for å rekke toget, men man vil kanskje godta at mobilen ber om autentisering i form av en PIN-kode når sensoren registrerer uvante bevegelser. Hovedmålet må være at det skal bli mindre attraktivt å stjele mobilen, påpeker Snekkenes.

På vei mot forbrukermarkedet

For øvrig setter knapt nok fantasien grenser for hva denne teknologien kan brukes til.

– Skoprodusenten NIKE har innledet et samarbeid med Apple og iPod og utstyrt enkelte joggesko med et lite hull i skoen som gir plass til en bevegelsessensor. Denne kobles trådløst til en mottager som kan plugges inn i iPoden. Dermed er musikkmaskinen straks omgjort til en skritteller som også kan fortelle hvor langt du har løpt og med hvilken hastighet, forteller Snekkenes.

Prosjektet:

Prosjektleder: Professor Einar Snekkenes, Høgskolen i Gjøvik.

Security of Approaches to Personnel Authentication

Doktorgradsstipendiat:
Davrondzhon Gafurov, Høgskolen i Gjøvik

Viktige publiseringer:

- Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. Spoof attacks on gait authentication system. IEEE Transactions on Information Forensics and Security, 2(3), 2007. Special Issue on Human Detection and Recognition.
- Davrondzhon Gafurov and Einar Snekkenes. Towards understanding uniqueness of gait biometric. In Proceedings of the 8th IEEE International Conference on Automatic Face and Gesture Recognition, 2008.
- Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. Gait authentication and identification using wearable accelerometer sensor. In 5th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pages 220-225, Alghero, Italy, June 7-8 2007.

Prosjektoversikt 2003–2008

Advanced Cryptographic Techniques
Institutt for informatikk, Universitetet i Bergen. Professor Tor Helleseth, 2003–2007

PENNE: A distributed, secure and resiliant storage system based on sage application of cryptography
Det matematisk-naturvitenskapelige fakultet, Universitetet i Tromsø. Førsteamanuensis Anders Andersen, 2004–2007

Cross-faculty Research Programme in Information Security organized within the strategic focus area of ICT established at Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk, Norges teknisk-naturvitenskapelige universitet. Professor Stig Frode Mjølsnes, 2003–2008

Defining Standards in Digital Forensics (DESDIFOR)
Norsk Regnesentral.
Forsker Knut Håkon T. Mørch, 2003–2005

Mapping Statutory Rules on Information Security in Norway
Institutt for rettsinformatikk, Universitetet i Oslo.
Professor Dag Wiese Schartum, 2003–2005

Security of Approaches to Personnel Authentication
Høgskolen i Gjøvik, Avdeling for teknologi. Professor Einar Snekkenes, 2003–2008

Large Scale PKI Applications
Institutt for telematikk, Norges teknisk-naturvitenskapelige universitet. Professor Stig Frode Mjølsnes, 2004–2008

Secure Wireless Application Programming (SWAP) for laptops and handheld devices
Institutt for informatikk, Universitetet i Bergen. Professor Kjell Jørgen Hole, 2005–2008

BAS5-Critical Information Infrastructure Protection
Forsvarets forskningsinstitutt.
Forsker Håvard Fridheim, 2005–2009

Security reporting
Høgskolen i Gjøvik, Avdeling for teknologi. Professor Einar Snekkenes, 2005–2008

Integrated Access Control for Health Care Information Systems
Institutt for datateknikk og informasjonsvitenskap, Norges teknisk-naturvitenskapelige universitet. Førsteamanuensis Øystein Nytrø, 2005–2009

From Incident Response to Incident Response Management: Case studies from the oil and gas industry
Informasjonssikkerhet og sårbarhet, SINTEF IKT. Forskerne Odd Helge Longva og Martin Gilje Jaatun, 2005–2007

Time Stamps, Digital Traces and Forensic Evidence – TID
Institutt for telematikk, Norges teknisk-naturvitenskapelige universitet. Professor Stig Frode Mjølsnes, 2005–2008

Tool supported methodology for the formalization, analysis and enforcement of policies within trust managment
Samvirkende og tiltrodde systemer, SINTEF IKT. Sjefsforsker Ketil Stølen, 2005–2009

A Model-Based Approach to Security Culture
Fakultet for teknologi og realfag, Universitetet i Agder. Professor José Julio Gonzalez, 2005–2010

Legal Information Security Regulations – an Instrumental Perspective
Det juridiske fakultet, Universitetet i Oslo. Professor Dag Wiese Schartum, 2005–2008

Safecomp 2005 in Halden/Fredrikstad
Institutt for energiteknikk – Halden.
Seniorforsker Bjørn Axel Gran, 2005–2006

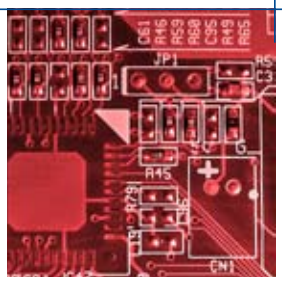
Forensics Readiness and Electronic Evidence
Norsk Regnesentral. Forskningssjef
Åsmund Skomedal, 2007

Workshop TTeC 2007: Legal and security issues – who cares?
Nasjonalt Senter for Telemedisin, Universitetssykehuset
Nord-Norge. Sikkerhetsrådgiver
Eva Henriksen, 2007

iAccess additional partner
Institutt for datateknikk og informasjonsvitenskap, Norges teknisk-naturvitenskapelige universitet.
Førsteamanuensis Øystein Nytrø

Workshop to strengthen the Security Awareness within the Oil and Gas Industry and Electrical Power Supply
Informasjonssikkerhet og sårbarhet, SINTEF IKT. Sjefsforsker Odd Helge Longva

iAccess International Workshop: Bringing Together Experts on Access Control and Healthcare Informatics
Institutt for datateknikk og informasjonsvitenskap, Norges teknisk-naturvitenskapelige universitet.
Førsteamanuensis Øystein Nytrø



Utgiver:
© Norges forskningsråd
IKT Sikkerhet og sårbarhet – IKTSOS
www.forskningsradet.no/IKTSOS

Om publikasjonen
Dette er en sluttrapport fra Norges forskningsråds forskningsprogram IKT Sikkerhet og sårbarhet (IKT SoS). Rapporten gir noen innblikk i forskningen som har foregått. Programmet har hatt varighet 2003–2008 og det totale budsjettet har vært 57,8 MNOK, finansiert med midler fra Nærings- og handelsdepartementet og Fornyings- og administrasjonsdepartementet.
www.forskningsradet.no/iktsos

Publikasjonen kan bestilles på
www.forskningsradet.no/publikasjoner

Norges forskningsråd
Stensberggata 26
Postboks 2700 St. Hanshaugen
N0-0131 Oslo

Telefon: +47 22 03 70 00
Telefaks: +47 22 03 70 01
post@forskningsradet.no
www.forskningsradet.no

Oktober 2008
ISBN 978-82-12-02584-4 (trykk)
ISBN 978-82-12-02585-1 (pdf)
Opplag: 500
Trykk: 07 Gruppen AS
Produksjon: BR Media
Intervjuer: Bjarne Røsjø
Synnøve Aspelund (side 26-30)
Design: Melkeveien designbyrå
Foto omslag: Bjarne Røsjø, Photodisc, Shutterstock