Sluttrapport fra prosjekt 1070 Grunnteknologier og trender innen informasjonssikkerhet (GOSIKT)

Eli Winjum

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

10. august 2010

FFI-rapport 2010/00818

1070

P: ISBN 978-82-464-1806-3
E: ISBN 978-82-464-1807-0

Emneord

Informasjonssikkerhet

Offentlige nøkkelsystemer

PKI

Flernivåsikkerhet

Godkjent av

Ole-Erik Hedenstad	Prosjektleder
Vidar S Andersen	Avdelingssjef

Sammendrag

Formålet med prosjekt *1070 Grunnteknologier og trender innen informasjonssikkerhet (GOSIKT)* var å bidra til å øke FFIs kunnskap om informasjonssikkerhet ved å levere grunnleggende innsikt i sikkerhetsteknologi til nåværende og framtidige FFI-aktiviteter.

Prosjektet var fullt ut basisfinansiert, hadde en akademisk innretning og studerte grunnleggende problemstillinger med langsiktig gyldighet og relevans for Forsvarets INI, og dermed for mange av FFIs aktiviteter innen informasjonssikkerhet. Gode sikkerhetsløsninger er generelt ressurskrevende, og prosjektets arbeid har derfor vært spesielt innrettet på å finne løsninger som kan virke over kommunikasjonsnett med lav kapasitet. Her møtes store teoretiske og praktiske utfordringer.

Prosjektet har prioritert områdene sikker nøkkelhåndtering/offentlig nøkkelsystemer og flernivåsikkerhet. Resultatene er publisert i internasjonale akademiske medier og i FFI-rapporter og -notater. Prosjektet har hatt et langsiktig perspektiv, med resultatene har også høy dagsaktuell relevans. Noen foreslåtte løsninger vil bli videreutviklet som demonstratorer av industrien.

Prosjektet har utvidet FFIs kontaktnett innen nasjonal informasjonssikkerhetsforskning og har hatt ledende oppgaver i et større multilateralt prosjekt innen Nato.

Arbeidet blir fulgt opp av prosjekt *1174 Grunnleggende informasjonssikkerhet for mobile operasjoner (GISMO).*

English summary

Project *1070 Basic technologies and trends in information security* (GOSIKT) aimed at increasing FFIs knowledge of information security to support current and future research activities within this area.

The project was fully funded by FFI, had an academic approach and studied basic research challenges with long-term validity and relevance. Generally, high-quality security solutions are designed for environments where communication resources are abundant. Therefore, a main challenge was to study and develop secure concepts that may work given military low-capacity wireless communication networks. Challenges are theoretical as well as practical.

Secure key management/public key infrastructures and *multilevel security* were main research areas. The results are published in international academic media and as FFI reports.
Even though the project studied future solution, the results also have short-term relevance. Some of the proposed solutions will be further developed by industry.

The project has extended FFIs national network within information security research and within NATO.

The work will be followed up by project *1174 Basic information security for mobile operations (GISMO).*

Innhold

1 Innledning

Prosjekt *Grunnteknologier og trender innen informasjonssikkerhet (GOSIKT)* startet 1. januar 2007 og ble avsluttet 31. desember 2009.

Informasjonssikkerhet er et viktig delområde i en rekke FFI-prosjekter. Dette gjelder i særlig grad prosjekter som arbeider med informasjonsinfrastrukturen i det framtidige nettverksbaserte Forsvaret. Sikre løsninger for informasjons- og kommunikasjonssystemer er en målsetting for dette arbeidet, og arbeidet forutsetter gjerne at *grunnleggende* problemer innen informasjonssikkerhet er løst.

Prosjekt *1070 Grunnteknologier og trender innen informasjonssikkerhet (GOSIKT)* ble startet for å bidra til å øke FFIs kunnskap om informasjonssikkerhet. Prosjektet skulle ved hjelp av kunnskap om *state-of-the-art* så vel som egen forskning, levere grunnleggende innsikt i sikkerhetsteknologi til nåværende og framtidige aktiviteter ved FFI. Prosjektet var fullt ut basisfinansiert og ble budsjettert med til sammen 9 FÅ fordelt over tre år.

Oppbygningen av rapporten er som følger:
Kapittel 2 beskriver prosjektets bakgrunn formål og målsetting. Kapittel 3 er rapportens hovedkapittel og gjennomgår de faglige problemstillingene prosjektet har arbeidet med. Kapittel 4 beskriver prosjektets arbeid med interne målsettinger, mens kapittel 5 gjennomgår det eksterne arbeidet. Gjennomføring og administrasjon av prosjektarbeidet er beskrevet i kapittel 6 Rapporten oppsummeres i kapittel 7, som også gir en kort egenvurdering av resultatene.

2 Prosjektets bakgrunn, formål og målsetting

Mer utdypende informasjon finnes i prosjektavtalen for GOSIKT (8).

2.1 Bakgrunn

Følgende aspekter var sentrale:

- Forsvarets gjeldende regime for informasjonssikkerhet er i dag forankret i en statisk risikounngåelse framfor en dynamisk risikohåndtering. Dette gjør den lite fleksibel med hensyn til at trusselen mot konfidensialitet, integritet og tilgjengelighet kan variere i ulike deler av informasjonsinfrastrukturen.
- Prosesserings-, lagrings- og overføringskapasiteten vil være svært ulik i de forskjellige delene av informasjonsinfrastrukturen. Dagens sikkerhetsløsninger er sentraliserte og ressurskrevende. De vil trolig være lite egnet til å sikre informasjonen i det framtidige nettverksbaserte Forsvaret (NbF). Dette gjelder i særlig grad taktisk/stridsteknisk nivå der ressursene vil være begrenset.
- Forsvaret har behov for sikre, effektive, robuste og fleksible sikkerhetsløsninger som samtidig er gjennomgående og interoperable. Dette byr på store teoretiske og praktiske utfordringer, og det er ikke gitt at framtidige kommersielle sikkerhetsløsninger vil dekke dette behovet.

– Det er behov for langsiktig forskning innen informasjonssikkerhet og denne bør relateres til sivil akademisk forskning. Å styrke båndene til akademisk forskning innen dette området er dessuten et mål i seg selv både for å få en bedre forståelse av akademiske forskningsresultater og for å på sikt kunne knyttes opp mot eksternt finansierte forskningsprosjekter nasjonalt og internasjonalt.

2.2 Formål og målsetting

Innføring av NbF stiller store krav til informasjonssikkerhet. Forsvarets informasjonsinfrastruktur (INI) vil være underlagt en overordnet sikkerhetspolicy. Arkitektur, tjenester og mekanismer for sikker prosessering, lagring og overføring av informasjon vil være underlagt gjeldende policy. Samtidig vil de ulike delene av infrastrukturen ha ulik evne til å *håndheve* gjeldende policy. Dette må gjenspeiles i FFIs aktiviteter innen INI generelt og informasjonssikkerhet spesielt.

Formålet med prosjekt GOSIKT var å bidra til å øke FFIs kunnskap om informasjonssikkerhet. Dette gjøres ved egen forskning og ved å levere grunnleggende innsikt i sikkerhetsteknologi til nåværende og framtidige FFI-aktiviteter som skal løse mer konkrete problemstillinger

Prosjektets målsettinger ble knyttet til tre innbyrdes avhengige områder:

– Prosjektet skulle arbeide med grunnleggende problemstillinger på områder som er relevante for Forsvaret og FFI. Basert på innsikt i *state-of-the-art* i internasjonal forskning på utvalgte områder, skulle prosjektet bidra med egne resultater. Resultatene ble ønsket publisert i internasjonale konferanse- og journalartikler så vel som i FFI-rapporter og -notater
– Prosjektet skulle være en ressurs for andre FFI-prosjekter knyttet til informasjonssikkerhet. Videre skulle prosjektet bidra med innsikt og inspirere til nye forskningsaktiviteter.
– Prosjektet skulle søke konkret forskningssamarbeid med institusjoner både i inn- og utland. Det var en målsetting å kunne søke på midler fra for eksempel Norges Forskningsråd (NFR) og EU-programmer. Det skulle legges opp til at medarbeidere i prosjektet kunne ta doktorgrad innenfor priorterte områder. Prosjektet skulle også knytte seg opp til forskningsfora innenfor NATO.

3 Faglige problemstillinger

Dette kapittelet presenterer kort de faglige problemstillingene prosjektet har arbeidet med og hvilke resultater som er oppnådd. Utdypende informasjon om resultatene finnes i publiserte artikler, FFI-rapporter og –notater.

Ved prosjektets avslutning forelå fem arbeider i form av draft eller uferdige artikkelmanuskripter I stedet for å ferdigstille disse for å publisere som FFI-rapporter, valgte prosjektet å fortsette arbeidene i det planlagte oppfølgingsprosjektet *1174 Grunnleggende informasjonssikkerhet for mobile operasjoner (GISMO)* for å kunne publisere dem som artikler. En liste over disse arbeidene er tatt med i slutten av kapittelet.

3.1 Sikker nøkkelhåndtering

3.1.1 Bakgrunn

Kryptologi er grunnleggende innen informasjonssikkerhet. Kryptografiske algoritmer inngår i tjenester som ivaretar krav om konfidensialitet og integritet. Symmetriske krypteringsalgoritmer forutsetter at en og samme nøkkel brukes for å kryptere og dekryptere[1]. Asymmetriske algoritmer forutsetter et nøkkelpar bestående av en privat nøkkel for å dekryptere, evt signere og en offentlig nøkkel for å kryptere, evt verifisere signatur[2]. Hemmelige nøkler og verdier spiller dermed en hovedrolle i både krypteringstjenester og autentiseringstjenester.

Nøkkelhåndtering omfatter generering, distribusjon og revokering av nøkler. At nøkkelhåndteringen er sikker, er dermed et grunnleggende krav.

En tradisjonell offentlig nøkkel-infrastruktur (*Public Key Infrastructure* (PKI)) har oftest en sentral autoritet (*Certificate Authority* (CA)) som håndterer nøkler ved hjelp av digitale sertifikater. Offentlig nøkkelsystemer er basert på asymmetrisk kryptografi og brukes i første rekke til autentisering og til å kryptere symmetriske nøkler som igjen benyttes til å kryptere selve informasjonen. Selv om asymmetrisk kryptografi ble utviklet på 70-tallet, er bruk av dette relativt nytt i Forsvaret.

De tradisjonelle systemene er svært ressurskrevende. Erfaringer fra den sivile verden tyder på at selv med ”uendelig” kommunikasjons- og prosesseringskapasitet, er store infrastrukturer vanskelige i praksis. Mange forskere innen informasjonssikkerhet stiller seg tvilende til om denne vegen i det hele tatt er farbar. Det er derfor all grunn til å være skeptisk til at tradisjonell PKI er egnet i et mobilt og dynamisk taktisk/stridsteknisk miljø der kommunikasjonskapasiteten også er lav. Sikker nøkkelhåndtering i mobile trådløse nett (MANETs) er et aktivt forskningsfelt i sivil akademisk forskning.

Både Nato og Forsvaret er nå i ferd med å innføre PKI basert på sivile standarder. En rekke applikasjoner og tjenester som er forslått for Forsvarets fremtidige INI, baserer autentiseringsbehov på at det finnes en PKI ”i bunnen”. Det gjør også planlagte nettverksløsninger som for eksempel neste generasjons IP-sikkerhet i Nato.

3.1.2 Skaleringsstudie

Formålet var å finne ut hvor mye kommunikasjonskapasitet som kreves for å operere en offentlig nøkkel-infrastruktur. Etter det prosjektet kjenner til, er det ikke publisert skaleringsstudier av en generisk offentlig nøkkel-infrastruktur, verken sivilt eller innen Nato.

[1] Systemer basert på symmetriske algoritmer benyttes i første rekke for å beskytte konfidensialitet ved å kryptere informasjonen.
[2] Systemer basert på asymmetriske algoritmer benyttes i større grad til å beskytte autentisitet og integritet, for eksempel ved digitale signaturer.

Som utgangspunkt for studien benyttet prosjektet de samme standardene som Nato planlegger. Modell og spesifikasjon for analysen er dokumentert i (22). Analysen tar utgangspunkt i en svært enkel infrastruktur over trådløse kommunikasjonsnett. Bare helt grunnleggende PKI-funksjoner modelleres. Scenarier og modeller for sertifikatvalidering er beskrevet i (13). Simulatoren (3) ble bygget som en modell av et taktisk ad hoc-nett, er dokumentert i (2), se også avsnitt 3.4.

For å skaffe til veie realistiske grunnlagsdata for simuleringene, gjennomførte prosjektet eksperimenter med kommersielle PKI-produkter. Et konsulentfirma med kommersielle PKI-produkter som spesialfelt, gjennomførte og dokumenterte flere av eksperimentene prosjektet spesifiserte.

Foreløpige resultater av studien er presentert i (1). De indikerer at PKI med standardsertifikater og en svært enkel standardprotokoll til å kontrollere sertifikatenes revokeringsstatus, ikke er egnet over stasjonære radionett som opererer i den lave enden av radiofrekvensspekteret. Bruk av tradisjonell PKI over tilsvarende *mobile* nett anses derfor som unødvendig å undersøke.

En konklusjon som kan trekkes på bakgrunn av prosjektets arbeid er at en ikke bør gjøre regning med et PKI ”i bunnen” for taktiske/stridstekniske systemer, med mindre en har undersøkt - og kan leve med - overføringskapasiteten dette vil kreve. Prosjektet har lagt et godt grunnlag for å utvide skaleringsanalysen til å omfatte mulige optimaliseringer av NATO PKI. Andre løsninger for sikker nøkkelhåndtering bør også analyseres på samme måte.

Gjennom eksperimentene med kommersielle PKI-produkter, avdekket prosjektet en rekke administrative og praktiske utfordringer knyttet til bruk av kommersielle PKI-produkter. Disse utfordringene er diskutert i (22) og understøtter indikasjonen på at PKI er uegnet for taktiske/stridstekniske systemer.

3.1.3 Optimaliseringstudie

Tradisjonelle PKI-systemer kan optimaliseres, for eksempel ved å lempe på kravene til hyppig kontroll av sertifikatenes revokeringsstatus eller ved å distribuere sertifikatvalideringstjenesten, noe som også forutsetter reduserte sikkerhetskrav.

Prosjektet har studert sistnevnte tilnærming og foreslått en mulig løsning. Motivasjonen for den foreslåtte løsningen er at den lave overføringskapasiteten til mobile trådløse nett og disse nettenes varierende kvalitet på linkene og hyppige brudd på konnektiviteten, gjør det umulig å garantere at en sentralisert sertifikatvalideringstjeneste alltid er tilgjengelig. Idéen er at tidligere svar på valideringsforespørsler lagres og tilgjengeliggjøres i distribuerte proxy-tjenere som former et overliggende nett. Nettet blir konstruert ved hjelp av rutingprotokollen. Dette krysslagsdesignet er beskrevet i (11).

Studien var basert på eksperiment og forsøk i testnett. Testnettet emulerer et mobilt ad hoc-nett (MANET) og er dokumentert i (12). En ny mobilitetsmodell basert på karakteristiske trekk ved militære operasjoner, er benyttet. Denne er dokumentert i (10).

Resultatene fra studien er dokumentert i (9) og indikerer at den foreslåtte løsningen både reduserer PKI-trafikken og øker valideringstjenestens tilgjengelighet signifikant. Resultatene er sannsynligvis relevante for generelle oppslagstjenester i MANETs.

3.2 Flernivåsikkerhet

3.2.1 Bakgrunn

Både militære og sivile organisasjoner trenger å kunne separere informasjon på ulike sikkerhetsnivåer og å kunne kontrollere informasjonsflyten mellom nivåene. Militære organisasjoner har vektlagt flernivå *konfidensialitet*, der målet er å hindre informasjonsflyt fra høyere til lavere konfidensialitetsnivåer. Innen bank og finans har en vektlagt flernivå *integritet*, der målet er å hindre informasjonsflyt fra lavere til høyere integritetsnivå.

Prosjektet har stilt spørsmål ved den ensidige vektleggingen av *konfidensialitets*beskyttelse. Særlig i internasjonale operasjoner, der informasjon ønskes utvekslet mellom mange ulike aktører, trengs løsninger som kan kontrollere informasjonens *autentisitet* og *integritet*. Videre, i trådløse kommunikasjonsnett, vil generelt beskyttelse av integritet/autentisitet trolig være en større utfordring enn beskyttelse av konfidensialitet.

For at en sikkerhetspolicy skal være verifiserbar, må den uttrykkes formelt. Policy-modeller er et nyttig verktøy for analyse av policy så vel som av mekanismene som skal håndheve policyen, for eksempel mekanismer for tilgangskontroll. En rekke flernivåmodeller er utviklet for henholdsvis konfidensialitets- og integritetspolicyer. Det finnes også modeller som kombinerer konfidensialitets- og integritetskrav, men de fleste forutsetter at informasjonen er klassifisert i henhold til konfidensialitetsnivåer og at integritetsnivå følger implisitt. Denne antagelsen er ikke gyldig. En uverifisert observasjon eller et rykte er for eksempel mindre troverdig enn en verifisert etterretning, men slike informasjonsobjekter kan i prinsippet ha samme konfidensialitetsnivå, lavt eller høyt.

Flernivåsikkerhet (*Multilevel Security* (MLS)) beskriver et system som inneholder informasjon klassifisert for ulike sikkerhetsnivåer, som opprettholder separasjon mellom nivåene og som håndterer samtidige brukere med ulike rettigheter til de ulike nivåene. De klassiske modellene ble utviklet alt på 70-tallet, men systemer bygget på disse konseptene ble komplekse, dyre og upraktiske. Dette har blant annet ført til overklassifisering av informasjon (”all” informasjon ”havner” til slutt på systemets høyeste klassifiseringsnivå). Dette fører i sin tur til ressurskrevende deklassifisering som involverer manuelle *review&release*-funksjoner.

3.2.2 Nytt MLS-konsept

Prosjektet har utviklet et MLS-konsept som forenkler de underliggende teoretiske modellene og samtidig ivaretar de fundamentale reglene for sikker envegs informasjonsflyt mellom nivåene. Konseptet er flerdimensjonalt i den forstand at det håndterer flere innbyrdes uavhengige flernivå sikkerhetsaspekter samtidig, for eksempel konfidensialitet, integritet og tilgjengelighet. Konseptet

er foreslått og beskrevet i (25). Konseptet er et ”lettvekts”-alternativ til de klassiske modellene, og kan tenkes brukt i for eksempel mindre kommando- og kontrollsystemer.

Å håndtere ulike sikkerhetsdimensjoner uavhengig, muliggjør effektiv verifisering av tilgangsrettigheter til de ulike nivåene. En mekanisme som eksekverer slik verifikasjon i løpet av noen få klokkesykler, er patentert (23). Mekanismen er senere gransket av *Europeean Patent Organisation* (EPO) som har gitt en positiv uttalelse. Dette vil gjøre det relativt enkelt å få internasjonale patenter.

3.2.3 Anvendelser og videreutvikling

Prosjektet har videreutviklet MLS-konseptet for ulike anvendelser. Et mulig bruksområde er rutinginformasjonen som blir utvekslet mellom IP-rutere, prosessert og lagret i form av rutingtabeller. Flernivåsikre rutere er et alternativ til separate IP-nett for hvert klassifiseringsnivå. Et flernivåsikkert rutingkonsept er foreslått, beskrevet og evaluert i (24). Konseptet vil kunne være nyttig i koalisjonsoperasjoner ved at partene kan etablere et felles kommunikasjonsnett, men samtidig kontrollere sikkerheten for ruter som involverer egne nettnoder.

Tilgjengelighetsaspektet ved informasjonssikkerhet er studert i (16) og (15) som foreslår og beskriver en sikkerhetsmodell for ressurstilgjengelighet. Modellen uttrykker policies for informasjonsflyt mellom ressurser fra ulike administrative domener ved hjelp av *type enforcement*. Modellen blir kombinert med en MLS-modell som håndterer flernivå konfidensialitet og integritet.

Integritetsaspektet ved informasjonssikkerhet er studert og vi foreslår en måte å konstruere ulike integritetsnivåer og diskuterer kriterier for klassifisering i henhold til disse nivåene, se Tabell 3.1. Denne studien blir ferdigstilt i GISMO.

Basert på sikkerhetsmerker som knytter filene til sine sikkerhetsnivåer vil en flernivåsikker filtjener kunne håndtere disse på en sikker måte gitt at den er konstruert for nødvendig separasjon av nivåene og gitt mekanismer som håndhever en MLS-policy for rettigheter til filene. Et konsept for en MLS filtjener som håndterer flere nivåer av konfidensialitet og integritet er beskrevet, se Tabell 3.1. Denne studien blir ferdigstilt i GISMO.

MLS er tradisjonelt assosiert med regelbasert (*mandatory*) tilgangskontroll som regulerer enkeltsubjekters rettigheter til informasjonsobjekter. Vi knytter MLS til rollebasert tilgangskontroll, der rettighetene er regulert på basis av enkeltsubjektenes *roller*, se Tabell 3.1. Rollebasert tilgangskontroll er mindre ressurskrevende enn tradisjonelle konsepter og kan uttrykkes gjennom standardiserte formelle språk. Denne studien blir ferdigstilt i GISMO.

3.3 Andre områder

3.3.1 Inntrengingstolerante systemer

Slike systemer skal i utgangspunktet være i stand til å detektere angrep, levere essensielle tjenester under angrepet og gjenopprette sikker tilstand etter angrepet. Mens *feiltolerante* systemer skal motstå spontane/tilfeldige feil, skal *inntrengingstolerante* motstå målrettede angrep fra ressurssterke aktører. Angrepene kan også være rettet mot deteksjons- og gjenopprettingsmekanismene. Forskning innen inntrengingstolerante systemer bygger på kunnskap fra flere andre felter som for eksempel informasjonssikkerhet, distribuerte systemer, feiltolerante systemer og sikker systemutvikling. Prosjektets studie av dette feltet er dokumentert i (14).

3.3.2 Sikring av nettinformasjon

Med nettinformasjon menes den informasjonen som må utveksles for å få et kommunikasjonssystem til å virke, for eksempel å kunne beregne rutetabeller og håndtere krav til tjenestekvalitet. Sikres ikke denne informasjonen tilstrekkelig, vil en angriper relativt lett kunne ta ned, evt kontrollere, kommunikasjonsnettet med et "logisk angrep". Trådløse mobile nett er særlig sårbare. Prosjektet har sett på åpenlyse svakheter ved utveksling av tjenestekvalitetsparametre over IP-nett og foreslått en konkret løsning for militære anvendelser i (17).

3.3.3 Autentisering

Autentisering regnes av mange som det mest grunnleggende innen informasjonssikkerhet og handler i første rekke om å verifisere en påstått identitet. Identiteten kan for eksempel hevdes av en kommunikasjonspart eller en informasjonskilde. En autentiseringstjeneste forventes å også verifisere at informasjon ikke er endret på uautorisert vis. Autentisering er grunnleggende for å sikre autorisert tilgang til informasjon og ressurser. Autentiseringstjenester vil være nødvendig i alle deler av INI og på flere kommunikasjonslag.

PKI kan sees som en infrastruktur for autentisering, men prosjektet har også arbeidet med selve autentiseringsprosessen. Sikre autentiseringsprotokoller er i dag basert på kryptografi og medfører dermed nøkkelhåndtering. Ønsker en å unngå/redusere bruken av hemmelige nøkler, er det nærliggende å anta at algoritmer som speiler biologiske/evolusjonære prosesser, vil kunne benyttes til ulike former for autentisering, for eksempel til å verifisere om en påstått identitet med stor sannsynlighet er "en av oss". Prosjektet gjennomførte tidlig en studie av denne typen algoritmer uten å komme fram til konkrete løsninger, men antar fortsatt at denne typen algoritmer representerer en mulighet.

Vi har gjennomgått autentiseringsbehovene i et taktisk/stridsteknisk scenario, se Tabell 3.1. Formålet med denne studien er å få oversikt over alle identiteter som bør autentiseres for deretter å kunne foreslå hensiktsmessige optimaliseringer, for eksempel ved krysslagsløsninger. Prosjektet er ikke kjent med at autentisering er behandlet på en helhetlig måte i militær forskning. Studien vil bli ferdigstilt i GISMO.

En viktig problemstilling relatert til autentisering er valg av konsistente og gjennomgående identiteter for personer, prosesser og terminaler, og hvordan disse identitetene skal representeres og adresseres. Identitetshåndtering er et voksende område innen sivil forskning. Prosjektets foreløpige arbeid innen dette området er beskrevet, se Tabell 3.1, og GISMO vil evt gå videre med arbeid innen identitetshåndtering.

3.4 Simulator og testomgivelser

Prosjektets innretning på sikkerhetsløsninger i taktiske/stridstekniske systemer medførte at det har vært lagt stor vekt på å bygge opp en god simulator for taktiske radionett. Flere andre FFI-prosjekter hadde samme behov.

Siden en ikke får tilgang til kildekoden, kan det være problematisk å bruke kommersielle simulatorer til forskningsformål. Blant flere ikke-kommersielle alternativer med åpen kildekode (*open source*) ble OMNeT++ valgt som det beste utgangspunktet for å utvikle en simulator som modellerer taktiske radionett. OMNeT++ er et objekt-orientert modulært rammeverk for diskret hendelsessimulering.

Utviklingen av simuleringsverktøy basert på OMNeT++ har vært et omfattende arbeid og er utført som et samarbeid mellom flere FFI-prosjekter. GOSIKTs bidrag er:

– En simulator som modellerer taktiske ad hoc-nett. Denne er dokumentert i (2).
– En generell modul som forbedrer muligheten for statistisk analyse i OMNeT++. Denne er dokumentert i (4).

Begge disse bidragene er publisert som åpen kildekode (3) og (5). Prosjektet kjenner ikke til at FFI tidligere har benyttet denne publiseringskanalen.

Prosjektet har også bygget testnett som emulerer et MANET i et vanlig kablet lokalnett. Trådløse topologier emuleres ved å filtrere *medium access control* (MAC)-adresser. *Dynamisk* topologi emuleres ved hjelp av sekvensielle konnektivitetstabeller. Testnettet er dokumentert i (12).

Et oppsett med kommersielle PKI-produkter ble laget først og fremst for å kunne estimere realistiske størrelser på sentrale inndata til simuleringer. Produkter som Forsvaret har valgt å innføre, ble benyttet i oppsettet (22).

Simulator og testomgivelser er tilgjengelig for gjenbruk.

3.5 Upubliserte arbeider

Tabell 3.1 gir en oversikt over upubliserte arbeider som overføres til prosjekt GISMO for ferdigstilling.

Fongen Anders	Cross Domain Identity Management in Tactical Environments
Hedenstad Ole-Erik	A multidimensional MLS file server model
Hedenstad Ole-Erik Winjum Eli	Multilevel Integrity and Classification Criteria
Hedenstad Ole-Erik Winjum Eli Oleshchuk Vladimir	Role-based access control and MLS
Hegland Anne Marie Winjum Eli	Authentication in Network Centric Operations

Tabell 3.1 Oversikt over upubliserte arbeider ved prosjektets avslutning

4 Internt arbeid

Prosjektet skulle spille en aktiv rolle overfor andre prosjekter knyttet til informasjonssikkerhet. Prosjektets viktigste interne bidrag var en kollokvieserie fra våren 2007 fram til våren 2009 da dette arbeidet ble overført til kompetansedimensjonen som aktivitetsområde *datasikkerhet* under kompetanseområde IKT. 16 møter ble arrangert, hvert med mellom 12 og 22 deltakere. Omtrent halvparten hadde ekstern innleder/foredragsholder, resten var fordelt mellom GOSIKT (4) og andre FFI-prosjekter.

Høsten 2008 utarbeidet avdeling Ledelsessystemer en strategisk innretning for arbeid med informasjonssikkerhet. Prosjektet spilte en sentral rolle i dette.

5 Eksternt arbeid

Prosjektet hadde som målsetting å styrke FFIs kontakt med akademisk forskning ved å søke samarbeid med relevante eksterne forskningsinstitusjoner. Prosjektet skulle også knytte seg opp mot relevante forskningsmiljøer innen Nato. På bakgrunn av dette har prosjektets viktigste eksterne samarbeid vært knyttet til *Norsk ressursnettverk for informasjonssikkerhet* (NISNet) og *Coalition Networks for Secure Information Sharing* (CoNSIS).

5.1 Nisnet

Høsten 2007 ble NISNet dannet som ett av flere forskernettverk tilknyttet *Kjernekompetanse og verdiskaping i IKT* (VERDIKT), Norges forskningsråds hovedsatsning innen IKT. NISNet har i dag 25 medlemsinstitusjoner og omfatter alle nasjonale forskningsmiljøer innen informasjonssikkerhet samt private og offentlige aktører med interesse for forskning innen fagfeltet (19).

Målet til NISNet er å identifisere nasjonale forskningsutfordringer innen informasjonssikkerhet, profilere informasjonssikkerhet innen IKT-forskning og å bidra til formidling av problemstillinger, forskningsresultater og innovasjon

Prosjektleder representerte FFI i dette nettverket siden det startet og var med i arbeidsutvalget hele prosjektperioden. Av NISNets mange aktivitetene trekkes særlig fram utarbeiding av et strategidokument for norsk forskning (20) og NISNets Forskerskole, et årlig kurs ment for doktorgradsstipendiater innen informasjonssikkerhet. Kurset er imidlertid for forskere som trenger grundig kunnskap innen informasjonssikkerhetsområdet, og hvert år har flere FFI-forskere deltatt.

Kontaktnettet som er bygget gjennom deltakelse i NISNet har vært til god nytte for FFIs forskning innen informasjonssikkerhet.

5.2 CoNSIS

Det viktigste eksterne samarbeidet har imidlertid vært innen CoNSIS, et multilateralt prosjekt av flere Nato-nasjoner (7), ledet av USA.

Målet til CoNSIS er å utvikle, teste og demonstrere løsninger for sikker kommunikasjon og informasjonsutveksling i koalisjonsoperasjoner. CoNSIS setter deployerbare, taktiske og stridstekniske scenarier i fokus og har arbeidsgrupper innen kommunikasjon, informasjon og tjenester, informasjonssikkerhet og netthåndtering (*network management*).

Tre FFI-prosjekter har deltatt siden høsten 2007 da det forberedende arbeidet startet. Prosjektleder har vært nasjonal koordinator og også ledet CoNSIS' arbeidsgruppe for informasjonssikkerhet.

Den norske leveransen innen informasjonssikkerhet er i all hovedsak knyttet til GOSIKTs aktiviteter.
CoNSIS-arbeidet har ført til at prosjektet har hatt utstrakt kontakt med relevant norsk industri. Industrien skal for eksempel utvikle demonstratorer basert på prosjektets arbeid med flernivåsikkerhet i IP-ruting (24) og prosjektets forslag til sikring av tjenestekvalitetsparametre (17). Prosjektets teoretiske resultater vedrørende PKI, autentisering og flernivåsikker filtjener vil også være del av leveransen.

Prosjekt GISMO overtar GOSIKTs rolle i CoNSIS.

5.3 Annet eksternt arbeid

Prosjektet har vært involvert i flere initiativer i samband med EUs 7. rammeprogram, men dette arbeidet har foreløpig ikke ført til noe konkret.

Tre masterstudenter har hatt veiledning fra prosjektet (6), (18), (19). Den ene var direkte tilknyttet prosjektet og skrev oppgaven sin på FFI. Prosjektets medlemmer har også vært benyttet som sensorer ved mastergradseksamener.

Prosjektets medlemmer har holdt flere eksterne forelesninger og foredrag, både i sivile og militære sammenhenger.

6 Gjennomføring

Dette kapittelet beskriver kort selve gjennomføringen av prosjektet og avsluttes med noen erfaringer som kan tenkes å være av interesse for framtidige basisfinansierte prosjekter.

6.1 Faglige prioriteringer

Områder som tidlig ble pekt ut som sentrale, var autentisering, nøkkelhåndtering, flernivåsikre policy-modeller og inntrengingstolerante systemer. Prosjektet benyttet det første året til å opparbeide kunnskap om *state-of-the-art* innen internasjonal forskning på disse områdene.

På basis av dette, var den videre planen å prioritere og planlegge egen forskning i samråd med prosjektrådet. Som en følge av dette prioriterte prosjektet de siste to årene studier av systemer for nøkkelhåndtering og flernivåsikkerhet. Teoretiske, analytiske, simuleringsbaserte og eksperimentelle metoder ble benyttet.

6.2 Erfaringer fra prosjektgjennomføringen

Prosjektet var fullfinansiert fra basismidler, skulle ha en klar akademisk innretning og var derfor ikke tilknyttet spesifikke framskaffelsesprosjekter, organisasjonsenheter eller prosesser i Forsvaret. Til tross for et engasjert prosjektråd medførte dette forholdet lite kontakt med Forsvaret. Prosjektet så på et tidlig tidspunkt at både problemstillinger og funn var høyst dagsaktuelle og at resultatene burde formidles Forsvaret raskt, og da ikke bare i form av artikler. Samtidig ønsket prosjektet hjelp fra operative, særlig i forbindelse med utarbeidelse av scenarier for simuleringer. Denne ønskete kontakten ville opplagt vært enklere å få til med en formell knytning til Forsvaret, for eksempel til Forsvarets prosjekter innen de områdene GOSIKT prioriterte. Det kunne vært riktigere om en del av prosjektets arbeid hadde hatt ekstern finansiering og dermed et uttrykt mål om støtte til pågående framskaffelsesprosjekter slik det planlegges for oppfølgingsprosjektet.

7 Oppsummering og egenvurdering av resultatene

Prosjektet har arbeidet med problemstillinger som er grunnleggende for Forsvarets INI, og dermed for mange av FFIs aktiviteter innen informasjonssikkerhet. Arbeidet har i særlig grad vært innrettet på å understøtte løsninger egnet for kommunikasjonsnett med lav kapasitet, - spesielt på taktisk og stridsteknisk nivå. Det er stort behov for løsninger som gir tilstrekkelig informasjonssikkerhet, men som krever lite kommunikasjonsressurser.

I forhold til målsettingene har prosjektet mer enn oppfylt framdriftsplanen med hensyn til egne forskningsresultater/publikasjoner. Med hensyn til intern funksjon mener prosjektet å ha bidratt aktivt med innsikt i grunnleggende problemstillinger innen informasjonssikkerhet og til å øke FFIs kunnskap om dette feltet. Eksternt samarbeid er i første rekke ivaretatt gjennom NISNet og CoNSIS

Selv om prosjektet har vært fullt ut basisfinansiert, har hatt en akademisk innretning og studert grunnleggende problemstillinger med *langsiktig* gyldighet og relevans, har resultatene etter prosjektets vurdering også høy *dagsaktuell* relevans for Forsvaret. Dette gjelder i særlig grad resultatene innen nøkkelhåndtering/PKI og flernivåsikkerhet, som har vært prosjektets to viktigste forskningsfelter.

Tidligere FFI-prosjekter har i liten grad gått dypt inn i problemstillingene GOSIKT har arbeidet med. Prosjektet startet dermed fra ”scratch”, også med hensyn til verktøy som simulator og testomgivelser. Prosjektets ambisjoner om publisering i internasjonale akademiske medier med fagfellevurdering har likevel vært styrende for arbeidet og har vært den viktigste målestokken for faglig kvalitet. Slik publisering regnes som et kvalitetsstempel og skal borge for at forskningen representerer noe *nytt* i forhold til tidligere kjente resultater, noe *originalt* og noe som betraktes som *relevant* innen forskningsfeltet. En artikkel må i tillegg oppfylle en del andre krav.

På bakgrunn av dette er prosjektet tilfreds med at sju artikler fra flere ulike områder av prosjektets arbeid har blitt publisert. I tillegg er fem manuskripter mer eller mindre klar for publiseringsprosess når prosjektet avsluttes. Disse ferdigstilles i oppfølgingsprosjektet. Publiseringsprosesser er generelt langdryge, og det kan gjerne ta et år fra et manuskript leveres til artikkelen er publisert.

Prosjektet har også levert fem FFI-rapporter og fire FFI-notater. De fleste beskriver analysemetoder og verktøy prosjektet har utviklet. De fleste av disse er generelle og kan gjenbrukes/videreutvikles av andre prosjekter.

To programvareprodukter er publisert som åpen kildekode.

Ett patent er innvilget.

Forkortelser

CA	Certificate Authority
CoNSIS	Coalition Networks for Secure Information Sharing
F3	Forsvarets forskningsforum
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FK KKIS	Forsvarets kompetansesenter for kommando og kontrollinformasjonssystemer
FLO/IKT	Forsvarets logistikkorganisasjon/Informasjons- og kommunikasjonstjenester
FOST	Forsvarets sikkerhetstjeneste
GISMO	Grunnleggende informasjonssikkerhet for mobile operasjoner (nytt FFI-prosjekt)
GOSIKT	Grunnteknologier og trender innen informasjonssikkerhet
IKT	Informasjons- og kommunikasjonsteknologi
INI	Informasjonsinfrastruktur
KDS	Kongsberg Defence Systems
MANET	Mobile ad hoc network
MLS	Multilevel security
Nato	North Atlantic Treaty Organisation
NbF	Nettverksbasert Forsvar
NISNet	Norsk ressursnettverk for informasjonssikkerhet / Norwegian Information Security Network
NSM	Nasjonal sikkerhetsmyndighet
PKI	Public key infrastructure
VERDIKT	Kjernekompetanse og verdiskaping i IKT

Referanser

(1) Berg Tore J., Fongen Anders (2009): Performance of NATO PKI in tactical domains – a preliminary study, FFI-notat 2009/02178.

(2) Berg Tore J.(2009): oTWLAN - a simulator modelling tactical ad-hoc networks, FFI-rapport 2009/00911.

(3) Berg Tore J. (2009): oTWLAN - a simulator modelling tactical ad-hoc networks, http://www.omnetpp.org/, juli 2009 (åpen kildekode).

(4) Berg Tore J.(2007): oProbe – an OMNeT++ extension module, FFI-rapport 2007/02578.

(5) Berg Tore J. (2007): oProbe - an OMNeT++ Extension Module, http://www.omnetpp.org/, november 2007 (åpen kildekode).

(6) Borgi Tor Kristian (2007): Access control and availability aspects using wireless solutions based on IEEE 802.11 technologies, providing access to classified networks, Høgskolen i Agder, http://student.grm.hia.no/master/ikt07/ikt590/g04 (Medveiledning)

(7) CoNSIS MoU, Draft (2009) (fortsatt under forhandling ved prosjektets avslutning).

(8) FFI (2006): Prosjektavtale 1070 – II/912 *Grunnteknologier og trender innen informasjonssikkerhet* (GOSIKT), 2006.

(9) Fongen Anders, Winjum Eli (2009): The Effect of a MANET Proxy Overlay for Certificate Validation Services, in Proceedings of the IEEE Military Communications Conference 2009 (MILCOM 2009), Boston, Massachussetts, USA, October 2009.

(10) Fongen Anders, Gjellerud Morten, Winjum Eli (2009): Military Mobility Model for MANET research, in Proceedings of IASTED Parallel and Distributed Computer Network Conference, Innsbruck, Austria, February 2009.

(11) Fongen Anders, Johnsen Frank Trethan, Winjum Eli (2008): Certificate Validation in Military MANET Based on overlay Network of XKMS Proxies, in Proceedings of the IEEE Military Communications Conference 2008 (MILCOM 2008), San Diego, California, USA, November 2008.

(12) Fongen Anders (2008): A Simple MANET Emulation Testbed, FFI-notat 2008/02290.

(13) Fongen Anders (2008): Scalability Analysis of Selected Certificate Validation Scenarios, FFI-notat 2008/01016.

(14) Fongen Anders (2007): Intrusion tolerant systems, FFI-rapport 2007/02611.

(15) Hedenstad Ole-Erik (2009): Multilevel Security models for cross-domain information flow – the integrity and availability aspects, FFI-notat 2009/02226.

(16) Hedenstad Ole-Erik (2009): Resource Availability – Subject and Object Type Enforcement, in Proceedings of the IEEE Military Communications Conference 2009 (MILCOM 2009), Boston, Massachusetts, USA, October 2009.

(17) Hegland Anne Marie, Winjum Eli (2008): Securing QoS Signaling in IP-based Military Ad Hoc Networks, IEEE Communication Magazine, vol. 8, No.11, 2008, pp. 42-48.

(18) Larsen Øystein (2007): Security aspects of OSPF as a MANET routing protocol, Universitetet i Oslo, http://www.duo.uio.no/sok/work.html?WORKID=67090 (Hovedveiledning)

(19) Norsk ressursnettverk for informasjonssikkerhet, http://www.nisnet.no/index.php/omnisnet

(20) Norsk ressursnettverk for informasjonssikkerhet, ”Research Priorities in Information Security”, 27. October, 2008.

(21) Stenberg Eystein Måløy (2009): Distributing a private key generator in Ad hoc Networks, Universitetet i Tromsø, http://www.ub.uit.no/munin/handle/10037/2074 (Medveiledning)

(22) Winjum Eli, Fongen Anders (2009): Model and specification for analyzing the scalability of a Public Key Infrastructure (PKI), FFI-rapport 2009/01546.

(23) Winjum Eli, Mølmann Bjørn Kjetil (2009): Fremgangsmåte og anordning for verifikasjon av informasjonstilgang i IKT-system med flere sikkerhetsdimensjoner og sikkerhetsnivå, Patent nr.: 326590, Patentstyret, 2009.

(24) Winjum Eli, Berg Tore J. (2008): Multilevel Security for IP Routing, in Proceedings of the IEEE Military Communications Conference 2008 (MILCOM 2008), San Diego, California, USA, November 2008.

(25) Winjum Eli, Mølmann Bjørn Kjetil (2008): A multidimensional approach to multilevel security, Information Management & Computer Security, Vol. 16, No. 5, 2008, pp. 436-448.