

Årsrapport 2017

NTNU Center for Cyber and Information Security

Gjøvik, 1. mars 2018

Innholdsfortegnelse

1	Innledning	1
2	Årsberetning	2
2.1	Styrets arbeid og generalforsamling	2
2.2	Organisasjon og ledelse	2
2.3	Forskning	3
2.4	Utdanning	4
2.5	En synlig samfunnsaktør	4
2.5.1	NISlectures	4
2.5.2	NBL annual workshop	5
2.5.3	Besøk fra statssekretær Sættem (H) – Justis- og beredskapsdepartementet	5
2.5.4	Sikkerhetstoppmøtet	5
2.5.5	Malware forum	5
2.5.6	Besøk fra USA Army Attaché	5
2.5.7	Cyber 9/12 Challenge	5
2.5.8	Møte med Nordisk ministerråd	6
2.5.9	COINS Finse Winter School	6
2.5.10	Training on Darknet and Cryptocurrencies	6
2.5.11	Cyber Symposium	6
2.5.12	Partnerdag med Oppland fylkeskommune	6
2.5.13	COINS Ph.D.-student seminar	6
2.5.14	ArsForensica workshop	6
2.5.15	Immatrikulering med møte med forsvarsministeren	7
2.5.16	European Symposium on Reserach in Computer Security (ESORICS)	7
2.5.17	Norwegian and European Cyber Security Challenge	7
2.5.18	SikkertNOK	7
2.5.19	Dialog og partnernmøter	7
2.5.20	Samfunnsrollen og kunnskapsformidling	7
2.6	Regnskapsrapport	8
3	Faggrupper	9
3.1	Biometrics	9
3.1.1	Samarbeid og samarbeidspartnere	9
3.1.2	Forskning	9
3.1.3	Utdanning	10
3.1.4	Viktige møter og aktiviteter	10
3.1.5	Medlemmer	10
3.2	Critical Infrastructure Security and Resilience	11
3.2.1	Samarbeid og samarbeidspartnere	11
3.2.2	Forskning	11
3.2.3	Utdanning	15
3.2.4	Viktige møter og aktiviteter	15
3.2.5	Medlemmer	15
3.3	Cyber Defence	16
3.3.1	Samarbeid og samarbeidspartnere	16
3.3.2	Forskning	16
3.3.3	Utdanning	16

3.3.4	Viktige møter og aktiviteter	17
3.3.5	Medlemmer	17
3.4	Digital Forensics	17
3.4.1	Samarbeid og samarbeidspartnere	17
3.4.2	Forskning.....	17
3.4.3	Utdanning	18
3.4.4	Viktige møter og aktiviteter	18
3.4.5	Medlemmer	21
3.5	e-Health and Welfare Security	21
3.5.1	Samarbeid og samarbeidspartnere	21
3.5.2	Forskning.....	22
3.5.3	Viktige møter og aktiviteter	23
3.5.4	Medlemmer	23
3.6	Information Security Management.....	24
3.6.1	Samarbeid og samarbeidspartnere	24
3.6.2	Forskning.....	24
3.6.3	Utdanning	25
3.6.4	Viktige møter og aktiviteter	25
3.6.5	Medlemmer	25

1 Innledning

NTNUs Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for forskning, utdanning og kompetansebygging innen cyber- og informasjonssikkerhet. Senteret skal bidra til å styrke samfunnets, virksomhetenes og den enkelte borgers evne til å beskytte sine informasjonsaktiva, oppdage relevante trusler, håndtere aktuelle hendelser og hvis nødvendig etterforske kriminelle handlinger som i cyberdomenet.

I et komplekst samfunn med stort behov for helhetlig kunnskap om cyber- og informasjonssikkerhet svarer NTNU CCIS på disse behovene på -nasjonalt nivå, i samfunnet og hos våre partnere. Kunnskapsutviklingen ved NTNU CCIS har langsiktige perspektiver for utdanning, forskning og formidling, og i et dynamisk trusselbilde skal vi bidra til at det ved våre partnerinstitusjoner utdannes relevante kandidater og produseres varig kunnskap. NTNU CCIS bidrar til effektiv samhandling og utveksling av kunnskap i offentlig og privat sektor ved å forene partnere fra privat og offentlig sektor med academia. Senteret har som mål å bli et av de -fremste -akademiske forsknings- og utdanningsmiljøene innen cyber- og informasjonssikkerhet i -Europa.

NTNU CCIS hadde ved utgangen av 2017 følgende 25 partnere i tillegg til vertsinstitusjonen NTNU: -Cyberforsvaret (CYFOR), Datatilsynet, Eidsiva, -Forsvarets forskningsinstitutt (FFI), Høgskolen i -Innlandet, IBM, Innlandet politi-distrikt, KPMG, Kripos, mnemonic AS, -Nasjonal -sikkerhetsmyndighet (NSM), -Nasjonalt ID-senter, NC-Spectrum AS, Norsk senter for informasjonssikring (NorSIS), Oppland Fylkeskommune (OFK), Oslo Politidistrikt, Politidirektoratet (POD), -Politiets sikkerhets-tjeneste (PST), Politihøgskolen (PHS), PwC, Statkraft, Statnett, Telenor, Watchcom -Security Group og Økokrim.

2 Årsberetning

2.1 Styrets arbeid og generalforsamling

Styret i NTNU CCIS har i løpet av første halvår 2017 gjennomført 4 styremøter. Onsdag 31. mai gjennomførte NTNU CCIS sin generalforsamling. 14 av NTNU CCIS sine 26 partnere var representert da styreleder Jørn Wroldsen og direktør Sofie Nystrøm orienterte om NTNU CCIS sin aktivitet i 2016 og planene fremover. I tillegg ble det gjennomført valg av styre i NTNU CCIS for det kommende året. Det nye styret består av:

- Jørn Wroldsen, Norges teknisk-naturvitenskapelige universitet (NTNU), styreleder – (2017-2019)
- Mona Strøm Arnøy, Nasjonal sikkerhetsmyndighet (NSM), nestleder – (2017-2019)
- Hanne Tangen Nilsen, Telenor – (2017-2019)
- Kristin Ottesen Kvigne, Politidirektoratet (POD) – (2017-2019)
- Ivar Kjærem, Cyberforsvaret (CYFOR) – (2017-2019)
- Ingeborg Dårflot, Statkraft – (2016-2018)
- Tor Tanke Holm, Politihøgskolen (PHS) – (2016-2018)
- Tønnes Ingebrigtsen, mnemonic AS – (2016-2018)
- Erik Hjelmås, NTNU CCIS ansattrepresentant – (2016-2018).

Styret i NTNU CCIS ble konstituert pr e-post i etterkant av generalforsamlingen.

2.2 Organisasjon og ledelse

Fra 1. januar 2017 har NTNU CCIS hatt Institutt for informasjonssikkerhet og kommunikasjonssikkerhet (IIK) ved Fakultet for informasjonsteknologi og elektroteknikk (IE) som vertsinstitutt i Norges teknisk-naturvitenskapelige universitet (NTNU). Instituttet er en sammensmeltning av tidligere Høgskolen i Gjøvik sin seksjon Norwegian Information Security Laboratory (NISlab) og det tidligere Institutt for telematikk ved NTNU, og har 80 ansatte på tvers av NTNUs campus i Trondheim og Gjøvik.

Første kvartal 2017 hadde Sofie Nystrøm permisjon fra stillingen som Direktør for NTNU CCIS for å delta på Forsvarets sjefskurs. Deltagelsen på sjefskurset var en svært spennende mulighet for Sofie Nystrøm og NTNU CCIS gjennom det nettverket og den eksponeringen som dette gir av aktiviteten i senteret. I denne perioden trådte professor Sokratis Katsikas inn i rollen som vitenskapelig leder for NTNU CCIS, mens seniorrådgiver Hilmar Haraldsson fortsatte å koordinere de administrative oppgavene. Første april kom Sofie Nystrøm tilbake fra permisjon og Sokratis Katsikas gikk da ut av rollen som vitenskapelig leder. 30 november 2017 fratradte Sofie Nystrøm stillingen som Direktør for NTNU CCIS for å starte i en nyopprettet avdelingssjefsstilling i Etterretningstjenesten. Vi takker Sofie Nystrøm for den innsatsen som hun har lagt ned i NTNU CCIS, og ønsker henne lykke til videre. Første desember 2017 tok gikk da Sokratis Katsikas igjen inn i rollen som midlertidig vitenskapelig leder for CCIS.

Gjennom hele 2017 har CCIS videreført ordningen med en konstituert vitenskapelig styringsgruppe bestående av førsteamanuensis Bian Yang, førsteamanuensis Geir Olav Dyrkolbotn, professor Katrin Franke, professor Patrick Bours, professor Sokratis Katsikas og professor Stewart Kowalski. NTNU CCIS' aktivitet er basert på de delene av IIK utdannings- og forskningsportefølje som er av særlig relevans for partnerne i senteret. Aktiviteten i senteret er samlet i de tematiske gruppene

- Biometrics
- Critical Infrastructure and Resilience
- Cyber Defence
- Digital Forensics
- E-Health and Welfare Security
- Information Security Management.

Disse gruppene har ulik historikk, oppbygning og modenhetsgrad. Det de har til felles er at de er svært relevante for å adressere de utfordringene som partnerne i NTNU CCIS står ovenfor. Det er også gjennom samarbeidet i disse gruppene at kunnskapsoverføringen mellom partnerne finner sted. Det er derfor av stor viktighet at partnerne engasjerer seg i de grupper de finner relevante. Faggruppene redegjør for sine aktiviteter i de respektive kapitler.

2.3 Forskning

NTNU CCIS samarbeider med partnerne for å legge til rette for god forskning. Dette er et langsiktig og systematisk arbeid med interne og eksterne grenseflater som spenner fra innspill til forskningsstrategier og -programmer via kapasitets- og konsortiabygging, til søknadsskriving og prosjektgjennomføring. Den løpende kontakten mellom private virksomheter, offentlig virksomhet og forsknings- og utdanningsinstitusjoner muliggjør gir senteret et bilde av de samfunnsmessige utfordringene som må adresseres knyttet til cyber- og informasjonssikkerhet. Dette bildet bruker vi til å gi innspill til relevante forskningsstrategier og forskningsprogrammer, både nasjonalt og internasjonalt. Norges forskningsråd (NFR), Justis- og Beredskapsdepartementet (JD), NordForsk (Nordisk ministerråd), Europakommisjonen og National Institute of Technologies and Standards (NIST) er eksempler på organer som er av særlig relevans for NTNU CCIS, våre partnere og våre nettverk. Dette gjøres i form av senterets samarbeide med NTNU om myndighetskontakt gjennom en rekke møter med statsråder, statssekretærer, departementer og politiske partier. I en annen dimensjon gjøres dette gjennom for eksempel deltagelse i Digital Enlightenment Forum, European Cyber Security Organization og Norges forskningsråds referansegruppe for H2020 Secure Societies. I en tredje dimensjon gjøres dette gjennom ekspertdeltagelse i internasjonale organisasjoner som EUROPOL, INTERPOL, ENISA og NATO som i tur gir sine innspill til samfunnsutfordringene.

NTNU CCIS jobber for ytterligere å bedre de vitenskapelige ansattes mulighet til å bli en del av konkurransedyktige søkergrupper, til å ha kapasitet til å skrive gode søknader og til å bidra med ressurser til å kvalitetssikre søknader. I 2017 fikk personell med tilknytning til CCIS innvilget følgende søknader fra Norges forskningsråd, Europakommisjonen og Intelligene Advanced Research Project Agency:

- Biometric Authentication with Timeless Learner (BATL, IARPA)
Utvikling av ende-til-ende løsninger som fra sensor til algoritme er motstandsdyktige mot presentation attack detection (se kapittel 3.1.2 for mer informasjon)
- Digital Patients (NFR HELSE-EU)
Tilretteleggelse for digitale, sikre, persontilpassede og skalerbare helsetjenester (se kapittel 3.5.2 for mer informasjon)
- Innovation and Excellence in Cyber-security teaching in Higher Education (SECTECH, H2020)
Fokuserer på strategisk utvikling av informasjonssikkerhetsutdanningene i Europa og utvikle en felles plattform (se kapittel 3.2.2 for mer informasjon).
- Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control (GHOST, H2020)
Fokuserer på flere aspekter ved cybersikkerhetsutfordringer anvendt på smarthus/ IoT miljøer (se kapittel 3.2.2 for mer informasjon)
- SMart mobilLity at the European land borders (SMILE, H2020)
Fokuserer på bruken av biometriske trekk som ansikt, fingeravtrykk og iris for å forbedre og automatisere mobiliteten ved grenseoverganger (se kapittel 3.1.2 for mer informasjon).

Gjennom statsbudsjettet for 2017 og revidert statsbudsjett 2017 fikk NTNU finansiering til 10 nye Ph.D. stillinger i informasjonssikkerhet, hvorav 4 var øremerket NTNU CCIS gjennom Kunnskapsdepartementet.

- Navigation System Security in Unmanned Autonomous Marine Vessels
- Gamification of Information Security Education and Training
- Cybersecurity, Security, and Resilience of Smart Cities
- Quantum Resistant Cryptography
- Chatroom Security
- Modelling and Analyzing Attack-Defence Scenarios for Cyber Ranges
- Security of the Cyber-Enabled Ship
- Information Security Economics
- Blockchain Analytics and Transactions Tracking
- Understanding Resilience of Software-Defined Industrial Control Networks

Dette utgjør en stor nasjonal satsning på forskerutdanningen innen informasjonssikkerhet. Stillingene besettes i slutten av 2017 og starten av 2018

For oversikt over alle publikasjoner til personell med tilknytning til CCIS henviser vi til databasen CRISin (www.cristin.no).

2.4 Utdanning

NTNU CCIS har i tillegg til vertsinstitusjonen NTNU flere utdanningsinstitusjoner i partnerskapet. Forsvarets ingeniørhøgskole, Høgskolen i Innlandet og Politi- og Høgskolen tilbyr alle utdanninger som er relevante for NTNU CCIS sitt arbeid. Den faglige utvekslingen mellom utdanningsinstitusjonene er basert på samarbeid mellom de faglig ansatte, at faglig ansatte ved en institusjon underviser ved en annen institusjon og deltagelse i hverandres interne seminarer. På denne måten er de faglig ansatte brobyggere mellom utdanningsmiljøene.

NTNU er partnerskapets hovedleverandør av studier innen cyber- og informasjonssikkerhet. Utdanninger ved NTNU med særlig fokus på områder av høy relevans for NTNU CCIS er:

- Ph.D. i informasjonssikkerhet og Ph.D. i telematikk
- 5-årig masterstudium i teknologi/sivilingeniør i kommunikasjonsteknologi
- 2-årig engelskspråklig masterstudium «Information Security»
- 2-årig engelskspråklig masterstudium «Telematics – Communication Networks and Networked Services»
- 1.5-årig erfaringsbasert masterstudium «Information Security»
- 3-årig bachelorstudium i IT-drift og informasjonssikkerhet

Erfaringsbasert mastergrad i informasjonssikkerhet tilbys i samarbeid med Politi- og Høgskolen, Cyberforsvaret og NorSIS. Alle masterutdanningene tilbys både på heltid og deltid, og er derfor svært aktuelle tilbud for virksomheter som ønsker å gjennomføre målrettede kompetanseutviklingstiltak for sine ansatte. Det ble ikke gjort opptak på den erfaringsbaserte masteren i 2017, men vi ser frem til å ta i mot et nytt kull i 2018.

NTNU ved hjelp av finansieringen over statsbudsjettet etablert 30 og 44 nye studieplasser på henholdsvis Bachelor i IT-drift og informasjonssikkerhet og Master i Informasjonssikkerhet i 2017. For opptak 2017 var det over tre søkere per studieplass på disse studiene.

Våren 2017 har det vært avholdt to Ph.D. disputaser innen informasjonssikkerhet ved IIK:

- Goitom Kahsay Weldehawayat: *Resilience of Infrastructure Networks: Byzantine Consensus, Interdependencies, and Optimisation in Sparse Networks*
- Gaute Bjørklund Wangen: *Cyber Security Risk Assessment Practices; Core Unified Risk Framework.*

Videre har 25 studenter har presentert sine masteroppgaver på Master i informasjonssikkerhet og 20 studenter har presentert sine bacheloroppgaver på Bachelor i IT-drift og informasjonssikkerhet. Oversikt over utvalgte bachelor, master og PhD oppgaver produsert ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi finnes her <https://brage.bibsys.no/xmlui/handle/11250/227496>, søket avgrenses etter dokumenttype.

2.5 En synlig samfunnsaktør

2.5.1 NISlectures

Foredragsserien NISlectures fortsatte i 2017 og samtlige foredrag er blitt strømmet og er tilgjengelige på <http://nislabs.no/nislecture>. Temaene i 2017 har vært:

- *Enhancement of human performance in military cyber operations by facilitating the application of behavioural science in cyber defense practice*
Øyvind Jøsok og Benjamin Knox, Performance & Applied Cognitive Engineering Cyber Operations Research Group, Forsvarets Ingeniørhøgskole
- *Security aspects of smartphone authentication*
Rolf Lindemann, Senior Director Products and Technology, Nok Nok Labs, Inc.
- *Software Certification for Software-intensive Safety Critical Systems*
Hao Wang, førsteamanuensis, NTNU I Ålesund
- *Biometric Systems Based on Communication Principles*
A.J. Han Vinck, professor in digital communication, University of Duisburg-Essen, Germany
- *The Modern Cybersecurity Stack: Data-driven Network Monitoring with Bro*
Robin Sommer, senior researcher, International Computer Science Institute (ICSI) in Berkeley, California
- *Our Cyber Security Challenge: A Seruius Game*
Stig Frode Mjølåsnes (professor), Simon McCallum (førsteamanuensis), Gaute Wangen (post.doc), NTNU

- *Implementing European Cybersecurity Regulation*
Martin Schallbruch, Senior Researcher, European School of Management and Technology, Berlin
- *20 år med sikkerhetssertifisering – nonstop – fortsatt usikker på om det smaker?*
Trond Laupstad, Chief Security Officer, Norsk Tipping

2.5.2 NBL annual workshop

Den 23. februar gjennomførte Norwegian Biometrics Laboratory sitt syvende årlige workshop (NBLAW). NBLAW er et åpent og gratis arrangement og er for alle som er interessert i teknologi, policyer, applikasjoner og utvidet aksept av smarttelefonbiometri. NBLAW 2017 fokuserte på det kommende og interessante feltet innen smarttelefonbiometri. Spesielt fokuserte NBLAW på muligheter og viktige utfordringer ved å vedta og bruke smarttelefonbaserte biometri. NBLAW ble teknisk sponset av European Association for Biometrics (EAB) og økonomisk støttet av Norges forskningsråd (RCN) under prosjektet Secure Access Control over Wide Area Network (SWAN). Målet med NBLAW 2017 var å ta opp alle aspekter av smarttelefonbiometri som til slutt vil etablere robuste metoder fra perspektivet av programvarearkitektur av biometrisk system på smarttelefon til autentisering av emner i ubegrensede fangstmiljøer via utfordringsresponsprotokoller. NBLAW 2017 har også resultert i å identifisere nøkkelområdene for forskningen som muligens kan føre til en ny EU-COST-handlingsfokusering på smarttelefonbiometri.

2.5.3 Besøk fra statssekretær Sættem (H) – Justis- og beredskapsdepartementet

Den 7. mars besøkte statssekretær Sættem (H) i Justis- og beredskapsdepartementet (JD) NTNU CCIS. Han hadde med seg følge fra JD og Politidirektoratet (POD). Statssekretæren fikk en orientering om NTNU CCIS med særlig fokus på biometri, digital forensics og personvern.

2.5.4 Sikkerhetstoppmøtet

NTNU CCIS er en av partnerne i Sikkerhetstoppmøtet. Sikkerhetstoppmøtet er en unik mulighet for at informasjonssikkerhetsledere, eksperter og nøkkelpersoner innen gitte fagfeltet kan utveksle erfaringer og kunnskap. Deltakerne vil gjennom foredrag og samtaler skaffe seg et klarere bilde av dagens praksis og en innsikt i utviklingen i feltet. Formatet på samtalene er en åpen og kollegial tankesmie hvor synspunkter og argumentasjoner relatert til dagsaktuelle tema utveksles. Nytteverdien for deltakerne ligger i at de kan ta med seg meningsutvekslingen tilbake til sine respektive foretak og styrke sin interne sikkerhet. I 2017 har det vært gjennomført to møter:

- Sikkerhet i skyen
- Personvernforordningen – General Data Protection Regulation (GDPR).

2.5.5 Malware forum

Den 30. mars 2017 arrangerte NTNU Malware Lab det første Malware Forum, i tett samarbeid mellom NTNU CCIS og NSM/NorCERT. Vi kan med stolthet si at forumet var en stor suksess, hvor det var foredragsholdere fra US EUCOM, Telenor, Symantec og NTNU, samt at forumet var fullbooket og vel så det. NTNU Malware Forum kommer til å være et årlig arrangement.

2.5.6 Besøk fra USA Army Attaché

Oberst Reneé Underwood, USA Army Attaché i Norge, besøkte NTNU CCIS den 7. april. Dette var det første møtet med Oberst Underwood hvor hovedfokus var å introdusere for attachéen forskning og utdanning på cybersikkerhet på NTNU på generelt grunnlag og NTNU CCIS spesielt. Attachéen møtte forskere på alle forskningsgrupper og fikk høre gjennom dialog deres forskningsmål og visjoner. Som oppfølging av besøket har Attachéen sett over Digital Border Squad sitt forarbeid til 9/12 Cyber Security Challenge og gitt tilbakemelding før de reiste til konkurransen den 21. april.

2.5.7 Cyber 9/12 Challenge

"The Digital Border Squad", dannet av studenter fra NTNU i Gjøvik (bachelor, master og doktorstudenter) og Forsvarets ingeniørhøgskole (bachelorstudenter), deltok på Cyber 9/12 konkurransen i Genève 20. og 21. april på Geneva Center for Security Policy. Målet med konkurransen var å kombinere teknisk-sikkerhets hendelsesadministrasjon med høyt nivå av politisk veiledning. Professor Stewart Kowalski (Information Security Management Group) var hovedtrener for laget.

Det var 24 lag i konkurransen fra hele verden. Vi kan med stolthet si at Digital Border Squad gjorde en glimrende innsats og kom på 5 plass i konkurransen og slo ut blant annet lag fra Westpoint og Oxford. Laget fra Geneva School of Diplomacy vant konkurransen, Air University fra US Air Force kom på annen plass og Forsvarshøgskolan fra Sverige kom på tredje plass.

2.5.8 Møte med Nordisk ministerråd

Nordisk ministerråd annonserte nylig et økt fokus på digitalisering. Dette initiativet inkluderer også økt samarbeid rundt cybersikkerhet. NTNU CCIS hadde den 20. april 2017 et nytt møte med nordisk ministerråd vedrørende kunnskapsutvikling og nordisk-baltisk samarbeid for å få cybersikkerhet enda høyere på politikkagendaen.

2.5.9 COINS Finse Winter School

Den 8.–12. mai ble COINS Finse Winter School avholdt. Det kan trygt sies at samlingen var en suksess. Foredragene spente bredt over teoretiske og praktiske emner inkludert; maskinlæring, kryptografi, biometri, robuste (anti fragile) systemer og datasimulering. Studentpresentasjonene ga en mulighet for doktorandene til å få tverrfaglige tilbakemeldinger på deres forskning fra eksperter.

2.5.10 Training on Darknet and Cryptocurrencies

I samarbeid med Politidirektoratet, NTNU Digital Forensics Group og Interpol, ble det 8.–12. mai gjennomført et kurs i Darknet og Cryptocurrencies. Kurset ble avholdt ved Politihøgskolen (PHS) i Oslo. Kurset fokuserte på ulike sider ved utnyttelse av Darknet (kryptert Internett) i det nye landskapet for kriminalitet. Det krever ny kompetanse og utførelse av politiarbeid på nye måter. Norge har den siste tiden fått synliggjort flere alvorlige kriminelle hendelser på Darknet. Politidirektoratet styrker gjennom kurset politiets evne til å operere i denne spesielle delen av Internett der det utøves alvorlig kriminalitet. Dette kurset er det første i en satsning på å bygge kapasiteten til distriktene og særorganene innenfor dette feltet, er det ønskelig at deltakerne stilles til disposisjon og kan inngå som ressurs i gjennomføring av lignende kurs i fremtiden.

2.5.11 Cyber Symposium

For andre år på rad ble Cyber Symposium gjennomført med Simula Research Laboratory på Litteraturhuset i Oslo den 23. Mai. Statsrådene Ketil Solvik-Olsen (SD) og Per-Willy Amundsen (JD) åpnet symposiet etterfulgt av foredragsholdere fra ECSO, Europol, Telenor, mnemonic, Politihøgskolen og selsagt NTNU CCIS og Simula. Programmet er tilgjengelig her: <https://ccis.no/cyber-information-security-symposium-2017-digital-resilience/>

2.5.12 Partnerdag med Oppland fylkeskommune

For fjerde gang gjennomførte NTNU CCIS den 2. juni partnerdag, nå med Oppland fylkeskommune (OFK). Både politiske representanter fra OFK og administrasjon møtte NTNU CCIS for å lære mer om cyber- og informasjonssikkerhet og hvordan aktørene sammen kan styrke miljøet i Oppland.

2.5.13 COINS Ph.D.-student seminar

I samarbeid med SWITS, the Swedish IT Security Network for PhD Students, ble det gjennomført et Ph.D.-student seminar på Voksenåsen Kultur- og konferansehotell i Oslo den 7.–9. juni. Deltakere var Ph.D.-studenter fra både Sverige og Norge og det var mange gode presentasjoner, engasjert publikum, god mat og tid til å utveksle idéer.

2.5.14 ArsForensica workshop

Den årlige workshopen i forskningsprosjektet Ars Forensica (finansiert ved Norges Forskningsråd, IKTPLUSS) ble arrangert 6.-7. juni 2017 ved Kripos, Oslo. Forskningsprosjektet fokuserer på å forebygge og bekjempe datakriminalitet, svindel, økonomisk kriminalitet, hvitvasking og terrorisme i Norge og internasjonalt. Prosjektet bidrar til å sette en internasjonal standard for digital etterforskning. Forskingen har stor aktualitet, og målet er at det enkelte politidistrikt skal få tilgang til nye digitale etterforskningsmetoder, noe som igjen vil styrke gjennomslagskraften i etterforskningen til politiet. Workshopen samlet representanter fra de norske politiorganisasjonene ved Politidirektoratet, Politihøgskolen, Kripos, Økokrim og Oslo politidistrikt. I tillegg deltok prosjektrepresentanter fra FinansCERT og mnemonic.

I løpet av workshopens første dag ble status for sentrale forskningstemaer i prosjektet presentert. Ved samlingen andre dag ble presentasjoner om malware-analyse, Open Source Intelligence, Big Data Forensics, Blockchain technology, Internet of Things (IoT) og IoT Forensics gitt.

2.5.15 Immatrikulering med møte med forsvarsministeren

Forsvarsminister Ine Marie Eriksen Sørreide deltok på immatrikuleringen 2017 ved NTNU i Gjøvik. Som en del av arrangementet ble det gjennomført et møte mellom Forsvarsdepartementet, Cyberforsvaret, Forsvarets ingeniørhøgskole og NTNU ved rektor, IIK og CCIS. Temaet for møtet var gjensidig samarbeid med særlig fokus på utdannings samarbeid og etableringen av en cyber range.

2.5.16 European Symposium on Reserach in Computer Security (ESORICS)

ESORICS er en av de ledende akademiske konferansene for informasjonssikkerhet i Europa. NTNU var vertskap for den 22. utgaven av ESORICS som ble arrangert i Oslo 11.-15. september. Det var i underkant av 200 deltagere på konferansen. Som en del av konferansen ble det gitt inviterte forelesninger fra Cormac Herley (Microsoft Reserch), Paul Syverson (U.S. Naval Research Laboratory), Sandro Etalle (Eindhoven University of Technology) og følgende workshops ble arrangert:

- 3rd Workshop on the Security of Industrial Control Systems & of Cyber Physical Systems
- 1st International Workshop on Security and Privacy Requirements Engineering
- International Workshop on Secure Software Engineering in DevOps and Agile Development
- 6th International Workshop on Qualitative Aspects of Security Assurance
- International Workshop on Cryptocurrencies and Blockchain Technology
- 12th DPM International Workshop on Data Privacy Management
- 13th International Workshop on Security and Trust Management
- The international Workshop on Secure Internet of Things.

Mer informasjon om arrangementene finnes på <https://www.ntnu.edu/web/esorics2017>.

2.5.17 Norwegian and European Cyber Security Challenge

På oppdrag fra Justis- og beredskapsdepartementet arrangerte IIK gjennom samarbeidet i NTNU CCIS Norwegian Cyber Security Challenge i 2017 og Norges deltagelse i European Cyber Security Challenge fra 30.10 til 3.11 i Malaga, Spania. Norwegian Cyber Security Challenge (NCSC) har som målsetning å finne unge talenter (i aldersgruppen 16 - 25 år) innen cybersikkerhet og motivere disse til å utvikle seg videre. Gjennom to kvalifiseringsrunder i form av en åpen catch the flag konkurranse og en nasjonal finale organisert på Gjøvik den 30. september ble følgende deltagere med på landslaget i cyber sikkerhet: Odin Jenseg (kaptein), Christian Resell, Daniel Isaksen, Eirik Holde, Kristian Johansen, Magnus Håland, Martin Ingesen, Nikolai Magnussen, Simen Lybekk, Stian Lysnes, Anders Wilhelmsen (1. reserve), og Simen Linderud (2. reserve). For mer informasjon se <https://www.ntnu.no/ncsc>.

2.5.18 SikkertNOK

SikkertNOK ble i 2017 arrangert for sjuende gang på Gjøvik som en åpen og fritt tilgjengelig avslutningskonferanse for Nasjonal sikkerhetsmåned i samarbeid med NorSIS. I 2017 var utdanninger i cybersikkerhet tema, med foredragsholdere fra akademia og virksomheter. Professor Matt Bishop fra UC Davis innledet med foredraget «Teaching Security Programming» som blant annet ble etterfulgt opp med paneldebatten «Secure Programming Education: Specialised or Integrated Approach». Konferansen er i sin helhet publisert på <https://youtu.be/X-DvBaXs4FY>.

2.5.19 Dialog og partnernmøter

Gjennom året gjennomføres løpende dialogmøter med departementene som finansierer NTNU CCIS og oppfølgingsmøter med våre partnere.

2.5.20 Samfunnsrollen og kunnskapsformidling

Det har vært høy aktivitet fra alle faggruppene på formidling både nasjonalt og internasjonalt. NTNU CCIS har i perioden kraftig økt sin aktivitet innen kunnskapsformidling og samfunnsdebatt både i riksdekkende medier og regionalt rundt Ålesund, Trondheim og Gjøvik. Fokuset har vært kunnskapsformidling fra de akademiske miljøene og helt opp til stortingspolitikere og regjering. Det har vært mange innlegg på konferanser både nasjonalt og internasjonalt. I tillegg har NTNU CCIS hatt en rekke besøk på campus Gjøvik for å formidle viktigheten av videre satsning rundt cyber- og informasjonssikkerhet. Det årlige Cyber Symposiet er et av mange tiltak for å nå både offentlige, private og akademiske miljøer.

2.6 Regnskapsrapport

Regnskapsrapporten under viser totaløkonomien for NTNU CCIS. Dette inkluderer bevilgninger, partnerbidrag og NTNU sine bidrag som vertsinstitusjon. Senteret har i 2017 økt sin aktivitet og vi ser at flere ansettelse har kommet på plass og at gruppene er aktive og i produksjon. Vi ser også i 2017 effekten av de forsinkede ansettelsesprosessene i form av at det både fra Helse- og omsorgsdepartementet og Justis- og beredskapsdepartementet ble overført 2016 midler over til 2017. Vi ser at aktiviteten finansiert fra JD og OFK i 2017 var i henhold til bevilgning og driftsmidler. På bevilgningen fra HOD var et underforbruk som i hovedsak er forårsaket av en stipendiat som avsluttet sitt ansettelsesforhold.

Oversikten for 2017 viser at CCIS økonomisk nå er inne i en mer stabil driftsfase. Udisponerte midler fra 2017 er budsjettert inn i aktiviteten for 2018.

Finansieringskilde	Sum	HOD	JD	NTNU	OFK	PARTNER
Inntekter						
Øverføring udisponerte midler 2016	3 511 553	1 166 349	2 345 204			
Bevilgning statsbudsjettet – JD	5 000 000		5 000 000			
Bevilgning statsbudsjettet – HOD	2 000 000	2 000 000				
Tilskudd driftsmidler – OFK	1 000 000				1 000 000	
Bidrag partnere	9 805 840					9 805 840
Bidrag NTNU	7 573 240			7 573 240		
Totale inntekter 2017	28 890 633	3 166 349	7 345 204	7 573 240	1 000 000	9 805 840
Utgifter						
Administrasjon						
Lønn	1 055 574	55 574			1 000 000	
Reiser	120 815	120 815				
Utstyr	34 563	34 563				
Utvikling	57 895	57 895				
Partner- og avtaleoppfølging	71 750	71 750				
Forskning, utdanning og formidling						
Lønn	21 650 979	747 517	3 524 382	7 573 240		9 805 840
Reiser	455 697	61 110	394 587			
Utstyr	583 647	24 568	559 079			
Publikasjoner, trykking, annonser	53 210		53 210			
Møter og arrangementer	279 632		279 632			
Formidling og markedsføring	111 064		111 064			
Totale utgifter 2017	24 474 826	1 173 792	4 921 954	7 573 240	1 000 000	9 805 840
Udisponerte midler overføres 2018	4 415 807	1 992 557	2 423 250	0	0	0

3 Faggrupper

3.1 Biometrics

3.1.1 Samarbeid og samarbeidspartnere

- IDIAP, Switzerland
- IDEMIA, France
- NR, Norway
- Telenor, Norway
- UIO, Norway

3.1.2 Forskning

3.1.2.1 Selected ongoing projects:

BATL (IARPA, USA): Raghavendra Ramachandra & Christoph Busch:

Biometric Authentication with Timeless Learner (BATL) is funded by Intelligence Advanced Research Projects Activity (IARPA). The primary objective of this project is to develop an end-to-end solution from sensor-to-algorithm to combat the presentation Attack Detection on the biometric system based on face, fingerprint and iris. NTNU is extensively involved in this project by developing an end-to-end solution for both fingerprint and iris Presentation Attack Detection algorithms and attack resistant sensors.

SMILE (H2020): Raghavendra Ramachandra:

Smart Mobility at the European land border (SMILE) is funded by H2020 with a primary objective to improve the mobility at the European border crossing. NTNU is primarily involved in contributing for privacy, legal aspects and biometrics. NBL is involved in contributing to the biometrics part of the project.

SWAN (NFR, IKTPLUSS-ICT): Kiran B Raja, Pankaj Wasnik, Martin Stokkenes, Raghavendra Ramachandra & Christoph Busch: Crimes involving illegal access to accounts are simpler than ever based? on the widespread password-based approach, which is proven to be vulnerable and no longer user-friendly. Identity theft and impersonation to steal money from personal accounts is one of the most critical threats that directly concerns economic development. The SWAN project will research and develop countermeasures and innovative technologies, which lead to a usable, economic, and privacy-preserving access control platform based on biometrics. Our research will allow the authentication of banking transactions and secure access to services over wired and mobile networks, using biometric identifiers. This can be extended to other eServices (e.g. eHealth). Biometric references will be stored, controlled, and verified locally based on a pre-shared secret, which can be used to seal and authenticate transaction data. This overcomes the need of centralized storage of biometric data. Furthermore, smartphones will act as hardware tokens to which the additional functionalities will be integrated to capture the biometric characteristics like (face, fingerprint, voice and eye). Processes are designed to serve scalable security needs. The biometric authentication will be designed to be privacy compliant and to align with existing and emerging standards in the field.

Awesome Possum (NFR, BIA): Patrick Bours & Guoqiang Li:

Remembering various PINs and passwords is a major challenge for most people, but despite this it is still the most prevalent way of identifying to log into mobile application. To relieve people for memorizing these codes, we are developing an authentication mechanism to automatically recognize the user by analysing the data from the smart phone sensors, including camera, microphone, accelerometer, gyroscope, Bluetooth, WIFI and GPS. The goal of the project is to develop "Data Driven Authentication" where, in short, the behaviour of a person on his/her mobile phone is used to allow secure and user-friendly access to applications.

3.1.2.2 Proposal Preparations:

- CALL: H2020 SEC-21-GM-2016-2017
Project Name: ENTIRE (rejected)
- CALL: IND-NOR IKTPLUSS from RCN,
Project name: SMART; COSED & NEST
- CALL: H2020-MSCA-ITN-2017
Project name: TRIBE+ (Rejected)

3.1.2.3 Selected publications

Total 50 publications of which 36 conference proceedings, 9 journal publications and 5 book chapters.

Selected publications are:

- R. Raghavendra and Chr. Busch, "Presentation Attack Detection Methods for Face Recognition Systems - A Comprehensive Survey", ACM Computing Surveys, Vol. 50, Issue 1, pp. 1-37, April 2017
- K.B. Raja, R. Raghavendra, S. Venkatesh, and Chr. Busch, "Multi-patch deep parse histograms for iris recognition in visible spectrum using collaborative subspace for robust verification", Pattern Recognition Letters, Vol. 91, pp. 27-36, May 2017
- S. Mondal and P. Bous, "Person Identification by Keystroke Dynamics Using Pairwise User Coupling", Transactions on Information Forensics and Security, Vol. 12, Issue 6, pp. 1319-1329, June 2017
- S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics", Neurocomputing, Vol. 230, pp. 1-22, 2017
- R. Raghavendra, K.B. Raja, and Chr. Busch, "ContlensNet: Robust Iris Contact Lens Detection Using Deep Convolutional Neural Networks", Proceedings of IEEE Winter Conference on Applications of Computer Vision-WACV 2017, USA, 2017
- R. Raghavendra, S. Venkatesh, K.B. Raja, F. Cheikh, and Chr. Busch, "On the Vulnerability of Extended Multispectral Face Recognition Systems Towards Presentation Attacks", IEEE International Conference on Identity, Security and Behaviour Analysis (ISBA2017), Delhi, India.

3.1.3 Utdanning

Master students that finished in 2017:

- Kristina Schäfer: Behavioural Data Analysis for Smartphone User Verification
- Jonathan Ness: Presentation Attack and Detection in Keystroke Dynamics
- Merita Haklaj: New approach to authentication - considering background and untrusted devices when taking the authentication decision

3.1.4 Viktige møter og aktiviteter

- ISO/IEC JTC1/SC37 meeting, Israel
- NBL Annual Workshop, Gjøvik
- Norwegian Biometric Forum, OSLO

3.1.5 Medlemmer

Akademisk ansatte, fulltid:

- Prof. Christoph Busch
- Prof. Patrick Bours
- Prof. Raghavendra Ramachandra
- Dr. Kiran Bylappa Raja
- Dr. Guoqiang Li

Akademisk ansatte, deltid:

- Ass.Prof. Bian Yang
- Prof. Mohammad Derawi
- Ass.Prof. Sule Yildirim-Yayilgan
- Prof. Faouzi Alaya Cheikh
- Ass.Prof. Erik Hjelmås
- Prof. Katrin Franke
- Prof. Ivar Farup

Tilknyttede akademiske ressurser:

- Frøy Løvåsdaal, National Police Directorate

PhD-kandidater:

- Ctirad Sousedik
- Edlira Martiri
- Patrick Schuch
- Martin Stokkenes
- Pankaj Wasnik
- Pawel Drozdowski
- Ali Khodabakhsh
- Hareesh Mandalapu
- Parisa Rezaee Borj

3.2 Critical Infrastructure Security and Resilience

3.2.1 Samarbeid og samarbeidspartnere

- Collaboration with partners listed in section 2.2 below towards proposal writing and submission in the respective fields.
- Collaboration with Statkraft towards implementing joint research and education activities.
- Collaboration with ColourLab towards writing and submitting a FRINATEK proposal.
- Collaboration with the University of Cape Town, South Africa
- Collaboration with the University of Pretoria, South Africa,
- Collaboration with IIIT Indore, India
- Collaboration with IIIT Allahabad, India
- Collaboration with the Institute for Energy Technology (IFE), Norway
- Collaboration with Indian Institute of Technology, Kanpur, India (IITK)
- Collaboration with Peace Research Institute Oslo, Norway
- Collaboration with Indian Institute of Management, Raipur, India (IIM Raipur)
- Collaboration with the Democritus University of Thrace, Greece

3.2.2 Forskning

3.2.2.1 Ongoing research activities

Prof. Katsikas, Dr Pandey and Dr Spathoulas started working in the H2020 project GHOST on May 1, 2017. The project aims to build a software-enabled 'usable security' solution for smart homes. The CCIS team is focusing on deep packet inspection for suspicious pattern recognition on one hand and on leveraging block chain technology and smart contracts for ensuring the integrity of communication among devices. Prof. Katsikas continued his research on the security of the AIS system; on privacy in online social networks; on the security awareness of digital natives (with V. Gkioulos and G. Wangen); on risk analysis for cyber physical systems; on intrusion detection in wireless sensor networks; and initiated research on the security of the cyber-enabled ship. Prof. Katsikas, jointly with Prof. Kowalski and Prof. Gligoroski have started working on the ERASMUS+ project SecTech (Innovation and Excellence in Cyber-security teaching in Higher Education), that aims at developing a cyber-security curriculum for higher education. Prof. Katsikas supervised (jointly with Prof. Wolthusen) Dr Kalman's work on a project developing a training course on cyber security for Statkraft's process control engineers.

Prof. Wolthusen concluded a project together with the University of Cape Town on security in micro-grids with two doctoral students at UCT still being co-supervised until graduation in the coming months. Continued work on security in power networks and micro grids in particular has led to new collaborations with the Smart Grid Centre at the University of Pretoria, South Africa and IIIT Indore, India, in continuation of this line of inquiry, with additional collaboration with the newly established EE department at Royal Holloway, University of London. A preliminary study on the effects of SDN on various critical infrastructure sectors with a focus on energy systems was undertaken by Dr Weldehawaryat (who graduated in April 2017 with a dissertation entitled "Resilience of Infrastructure Networks: Byzantine Consensus, Interdependencies, and Optimisation in Sparse Networks". Prof. Wolthusen also co-supervises (with Dr Katsikas) a research project conducted by Dr Baiocco on monitoring mechanisms for the security of energy systems OT protocols, in collaboration with Statkraft. This is also supported by a grant held by Dr Wolthusen at Royal Holloway, U. of London (UK) researching security issues in the ISO/IEC 61850/64283 series of standards by EPSRC/GCHQ and ongoing work on security studies of state estimators funded by the Higher Education Commission Pakistan for a doctoral candidate.

Dr Baiocco's ongoing research is on microgrids stability and resilience when under time-based attacks to the multilevel Hierarchical State Estimator; on the security of SCADA system related to power plants sites (Statkraft) and distribution system (Statnett) with emphasis on the communication standard IEC 60870-5-104 and vital control systems; and on recreating a framework simulation environment which relies on IEC communication protocol emulator and Intrusion Detection System and Anomalies Detection Systems in order to determinate the response provided by a real system (partially composed by the Statkraft network) both in normal and under attack operational modes.

Dr Pandey's current research activities lie in the areas of blockchain and smart contracts for IoT with respect to Horizon 2020 project 'GHOST - Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control.

Dr Spathoulas's current research activity relates to IoT security, secure computation methods and blockchain applications. Specifically research is conducted on how IoT devices can be monitored, in order to detect abnormal situations or malicious activity. Additionally a lot of effort has been concentrated on developing and implementing privacy preserving techniques on various fields such as cybersecurity, mobile computing or authentication, by using either homomorphic encryption or secure multi party computation methods. Finally the applicability of blockchain technology on various problems has been researched and some prototypes have been implemented.

Dr Kalman's current research is aimed towards security in cloud environments with focus on financial infrastructures and relation to IoT. Security and privacy challenges related to wide scale data gathering and fusion of data from different sources from both implementation and legal (GDPR) viewpoint. Security implications on critical infrastructures partially moved into cloud environments and adaptation of security requirements from on-premises to cloud environments. Monitoring capabilities for software-defined infrastructures.

Dr Weldehawaryat's current research activities lie in the areas of resilient power consumption scheduling in resource constrained smart micro-grids, attack modelling for Software Defined Networking (SDN) enabled IEC 61850-based substation communication systems, systematic literature review on SDN for military networks, and quantitative security assurance metrics.

V. Gkioulos and S. Wolthusen successfully completed the finalizing milestones and the overall project TACTICS. V. Gkioulos, in collaboration with S. Wolthusen, S. Katsikas and H. Lannweg prepared and administered the ESORICS 2017 doctoral consortium event.

V. Gkioulos completed and submitted his doctoral thesis. He also established research collaboration with CNR (IT).

3.2.2.2 Collaborating partners

- DELTA: Centre for Research and Technology - Hellas (GR); HIT HYPERTECH INNOVATIONS LTD (CY); Electricity Authority of Cyprus (CY); UNIVERSITY OF CYPRUS (CY); KIWI POWER LTD (UK); JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION (BE); C.C.I.C.C. LIMITED (IE); E7 ENERGIE MARKT ANALYSE (AT); UNIVERSIDAD POLITECNICA DE MADRID (ES)
- Heat Metering and Billing via Blockchain-Technology: consider it GmbH (DE); SingularLogic (BG); HAW Hamburg (DE); MOTIVIAN (BG).
- Blockchain-based Smart Contracts for Securitization of Cyber Risk: Democritus University of Thrace (GR)
- Privacy Assured Intelligent Cyber Vision Systems: Centre for Research and Technology – Hellas (GR); Karlstad University (SE); Los Alamos National Laboratory (USA).
- Cybersecurity, Safety, and Resilience of Smart cities: NTNU IDI
- Navigation System Security in Unmanned Autonomous Marine Vessels: NTNU ITK
- ABSOLUTE: NTNU CCIS; NORIS; SINTEF; University of Plymouth (UK); University of Regensburg (DE); University of California Davis (US); Nelson Mandela University (SA).
- ARMOR: NTNU; CERTH (GR); Universite de Geneve (CH); EXUS Software (UK); Micrel Medical Devices (GR); Institute of medical technology and equipment (PL); Boston Scientific Clonmel (IE); TSB Real time location systems (ES); Servizio Andaluz de Salud (ES); Emtel (PL); Vidavo (GR).
- CyberSec: University of Cyprus (CY); Guardtime AS (ET); CNRS&IRIT (FR); FORTH-ICS (GR); Budapest University of Technology and Economics (HU); Waterford Institute of Technology (IE); TSSG (IE); Consiglio Nazionale delle Ricerche – IIT (IT); Universita' degli Studi di Milano (IT); University of Luxembourg - Interdisciplinary Centre for Security, Reliability and Trust (LU); Tilburg University (NL); Universidade de Coimbra (PT); Politehnica University of Timisoara (RO); Institut Jozef Stefan and University of Ljubljana (SL); University of La Laguna (ES); University of Malaga (ES); Chalmers University of Technology (SE); University of Edinburgh (UK)

- HEALTHINUIITY: EXODUS (GR); FUNDACION TEKNIKER (ES); Sociedad Europea de Analisis Diferencial de Movilidad (ES); Crowd Dynamics (UK); Diginext (FR); Telesto (GR); CERTH (GR); CINI (IT); Engineering – Ingegneria Informatica (IT); Gobierno Vasco (ES); Akershus universitetssykehus (NO); Neuromed (IT); Universita campus Bioemmedica (IT); Eticas (ES); Nextel (ES); Institute of accelerating systems and applications (GR); SNV Engineering (GR); Servicio Vasco de Salud (ES); Ministero dell Interno (IT)

3.2.2.3 Proposals submitted

1. Using Financial Engineering Methods to Develop Novel Financial Instruments for Information Security Risk Financing - NTNU internal PhD funding application, Submitted: Jan 2017, Status: Unsuccessful, Pankaj Pandey and Sokratis Katsikas
2. Future tamper-proof Demand rEsponse framework through self-configured, self-optimized and collaborative virtual distributed energy nodes (DELTA) H2020-LCE-2016-2017, Topic: LCE-01-2016-2017, Type of action: RIA, Submitted: Feb 2017, Status: accepted, funded, Sokratis Katsikas and Pankaj Pandey
3. Heat Metering and Billing via Blockchain-Technology, EUROSTARS, Submitted: Mar 2017, Status: Unsuccessful, Sokratis Katsikas and Pankaj Pandey
4. Blockchain-based Smart Cyber Derivatives to Hedge Security Risk - FORNY 2020, Project Number: 273571, Submitted: Apr 2017, Status: Unsuccessful, Pankaj Pandey and Sokratis Katsikas
5. Blockchain-based Smart Contracts for Securitization of Cyber Risk, FRIPRO Mobility, Application Number: ES596906, Submitted: May 2017, Status: Unsuccessful, Pankaj Pandey and Sokratis Katsikas
6. Privacy Assured Intelligent Cyber Vision Systems, FRINATEK, Application Number: ES596586, Submitted: May 2017, Status: Unsuccessful, Pankaj Pandey and Sokratis Katsikas
7. Security of the cyber-ship, proposal for NTNU IE faculty sponsored PhD position, Submitted: April 2017, Status: Accepted, Sokratis Katsikas.
8. Cybersecurity, Safety, and Resilience of Smart cities, proposal for NTNU IE faculty sponsored PhD position, Submitted: April 2017, Status: Accepted, Jingyue Li, Sokratis Katsikas.
9. Navigation System Security in Unmanned Autonomous Marine Vessels, proposal for NTNU IE faculty sponsored PhD position, Submitted: April 2017, Status: Accepted, Nadia Sokolova, Sokratis Katsikas.
10. Assurance for system-of-systems security: modeling measuring, managing, proposal to Telenor & FFI, Submitted: June 2017, Status: Unsuccessful, Stewart Kowalski, Sokratis Katsikas
11. Enhancing societal security awareness by promoting a security culture through education (ABSOLUTE), FINNUT, Application Number: ES609391, Submitted: November 2017, Status: Under evaluation, Sokratis Katsikas and Vasileios Gkioulos
12. Cyber-Physical Security in Energy Infrastructure of Smart Cities (CPSEC), IKTPLUSS proposal. Status: Under Evaluation, Pankaj Pandey and Sokratis Katsikas
13. ID based E-governance: Innovation, Challenges and Benefits to Individuals and Society at large in 'Aadhaar' (IDEA), IKTPLUSS proposal. Status: Under Evaluation, Pankaj Pandey and Sokratis Katsikas
14. Artificial Intelligence driven Cybersecurity trustworthy platform in connected medical devices environment (ARMOR): H2020-DS-SC7-2017, Activity: DS-07-2017-RIA, Submitted: August 2017, Status: accepted, not funded, Sokratis Katsikas, Pankaj Pandey, and Vasileios Gkioulos
15. CyberSec: Improving European Capacity for Securing Next-Generation Cyberspace, COST, Submitted: September 2017, Status: Under evaluation, Sokratis Katsikas
16. HEALTHinuity: A total security solution for safeguarding the well-being and continuity of the healthcare sector against physical and cyber threats, H2020 CIP-2016-2017-2, Activity: CIP-01-2016-2017, Submitted: August 2017, Status: Unsuccessful, Sokratis Katsikas and Bian Yang

3.2.2.4 Invited talks

- 3rd ACM Workshop on Cyber-Physical Systems Security (CPSS'17), Abu Dhabi, UAE, April 2, 2017. Sokratis Katsikas

- 11th International Crisis Management Workshop (CrIM'17) and Oulu Winter School, Oulu, Finland, November 8-10, 2017. Sokratis Katsikas
- Invited speaker on Norsk Forening for Automatisering: Cyber Security 2017: OWASP Top 10 in an industrial context. György Kalman
- Invited speaker on KraftCERT forum 2017: OWASP Top 10 in an industrial context (reprise of the NFA presentation). György Kalman
- Invited speaker on Energi Norge: IKT-Forum: Sikkerhet og sårbarhet i energibransjen: Felles sikkerhetsopplæring av IT og OT. György Kalman
- Keynote speaker on IARIA Energy17: OWASP Top 10 Security Vulnerabilities in an Industrial Context (extended). György Kalman

3.2.2.5 Awards

May 9: Bernhard Hämmerli received the Outstanding Performance Award of the Swiss Academy of Engineering Sciences for acting as President of Cyber Security Activities

3.2.2.6 Selected publications

V. Anastopoulos and S.Katsikas, "A structured methodology for deploying log management in WANs", Journal of Information Security and Applications, available online, 6 March 2017, ISSN 2214-2126, <https://doi.org/10.1016/j.jisa.2017.02.004>.

Bernhard Hämmerli (Editor in Chief) European CIP Newsletter: <https://www.ciprnet.eu/ecn.html>

Alcaraz, C., Lopez, J., and Wolthusen, "S. Policy Enforcement System for Secure Interoperable Control in Distributed Smart Grid Systems", IEEE Transactions on Smart Grid, pp. 1–9 (Feb. 2017).

Chamatidis Ilias, Katsika Aggeliki and Spathoulas Georgios. "Using deep learning neural networks for ECG based authentication." 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 2017, pp. 1-6.

Spathoulas, Georgios and Vennou, Paraskevi and Loukidis, Alexandros. "Privacy Preserving Platform for Profitable Mobile Crowd Sensing and Users' Adoption." Proceedings of the 21st Pan-Hellenic Conference on Informatics. ACM, 2017.

Myridakis, Dimitrios and Spathoulas, Georgios and Kakarountas, Athanasios. "Supply Current Monitoring for Anomaly Detection on IoT Devices." Proceedings of the 21st Pan-Hellenic Conference on Informatics. ACM, 2017.

Chioktour, Vasileios and Spathoulas, Georgios and Kakarountas, Athanasios "Systolic Binary Counter Using a Cellular Automaton-based Prescaler." Proceedings of the 21st Pan-Hellenic Conference on Informatics. ACM, 2017.

C. Becker Westphall, Y. W. Lee, B. Duncan, A. Olmsted, M. Vassilakopoulos, C. Lambrinouidakis, S. K. Katsikas, R. Ege, Proceedings of CLOUD COMPUTING 2017, The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, IARIA Publications, 2017.

N. Cuppens-Boulaiah, C. Lambrinouidakis, F. Cuppens, S. Katsikas (Eds.), Security of Industrial Control Systems and Cyber-Physical Systems, Lecture Notes in Computer Science, Springer, 2017.

S.K. Katsikas and V. Zorkadis (Eds.), E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services, Communications in Computer and Information Science, Springer, 2017.

S. Katsikas and S. Gritzalis, "Digitalization in Greece: State of play, barriers, challenges, solutions", in Alois Paulin, Leonidas G. Anthopoulos, and Christopher G. Reddick (Eds.), Beyond Bureaucracy: Towards Sustainable Governance Informatisation, Springer, pp. 355-375, 2017.

E. Darra and S. Katsikas, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", in George Kambourakis, Asaf Shabtai, Konstantinos Kolias, and Dimitrios Damopoulos (Eds.), Intrusion Detection and Prevention for Mobile Ecosystems, CRC Press, 2017.

S. Katsikas, "Cyber security of the autonomous ship", in Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security (CPSS'17), Abu Dhabi, UAE, pp. 55-56, 2017.

V. Gkioulos, G. Wanger, S. Katsikas, G. Kavallieratos, P. Kotzanikolaou, "Security Awareness of the Digital Natives", *Information*, 8, 42; doi:10.3390/info8020042, 2017.

V. Gkioulos, G. Wanger, S. Katsikas, "User Modelling Validation Over the Security Awareness of Digital Natives", *Future Internet*, 9, 32; doi:10.3390/fi9030032, 2017.

A. Michota and S. Katsikas, "Default OSN Privacy Settings: Privacy Risks", in S.K. Katsikas and V. Zorkadis (Eds.): *E-Democracy 2017*, CCIS 792, pp. 64–78, 2017.

3.2.3 Utdanning

PhD-students that are finished so far in 2017

- Goitom Weldehawaryat (April 2017)

Teaching activities so far in 2017

Prof. Wolthusen has taught IMT 4125 (Network Security) in the spring 2017 term, covering core aspects of network infrastructure protocol security.

Prof. Katsikas and Prof. Wolthusen offered the IMT 4203 MSc course on Critical Infrastructure Security in Autumn 2017. Dr Baiocco, Dr Weldehawaryat, and Vasileios Gkioulos contributed to the course offering with tutorials.

Dr Kalman taught two courses at ITS (UniK): UNIK 4750, Measureable security for the internet of things: developed and held whole of the course; and UNIK 4290, Mobility in internet: responsible for approx. 40% of the tasks related to the course: two lectures, correction of 5 small and one large deliverable.

3.2.4 Viktige møter og aktiviteter

- CASCADING EFFECTS CONFERENCE, Brussels, March 16-17, B. Hämmerli
- Oslo Blockchain Day, Apr 2017, P. Pandey
- CCIS Symposium, P. Pandey, V. Gkioulos
- ECSO working group 2 meetings
- Indo-Norwegian Proposal Meeting, June 2017, S. Katsikas, P. Pandey
- 11th International Conference on Complex, Intelligent, and Software Intensive Systems 2017 (CISIS), V. Gkioulos
- Meetings and milestones related to TACTICS project, V. Gkioulos

3.2.5 Medlemmer

Akademisk ansatte, fulltid

- Prof. Sokratis K. Katsikas
- Dr Pankaj Pandey
- Dr Alessio Baiocco

Akademisk ansatte, deltid:

- Prof. Stephen D. Wolthusen
- Prof. Bernhardt Hämmerli
- Dr György T. Kalman

Tilknyttede akademiske ressurser:

- Dr Georgios Spathoulas

PhD-kandidater:

- Vasileios Gkioulos
- Håkon Gunleifsen

3.3 Cyber Defence

Cyber Defence gruppen er under oppbygging. Gruppens forskning fokuserer på å styrke organisasjoners motstandsdyktighet mot og håndtering av dataangrep. Håndtering vil fokusere på å redusere konsekvensen av disse angrepene på individ, - organisasjon eller samfunn i tillegg til den underliggende årsaken (f.eks. tap av informasjon eller nedetid av tjenester). Dette vil fordre forskning som kombinerer dyp teknisk analyse og kontekstinformasjon om hva som er kritiske verdier for individet, organisasjonen eller samfunnet.

3.3.1 Samarbeid og samarbeidspartnere

Forskningsgruppe Cyberforsvar samarbeider tett med forskningsgruppe Testimon forensics innen forskning, undervisning og formidling rundt etablering av en CCIS/NTNU malware lab på Gjøvik. Gruppen har tett samarbeid med Cyberforsvaret (bl.a. Forsvarets ingeniørhøgskole (FIH) og avdeling for beskyttelse av kritisk infrastruktur (BKI)).

Utvidet samarbeidet med NSM, NorCERT og BDO CERT med fokus på malware analyse gjennom gjesteforelesere, master oppgaver og workshop.

Bidrar i etableringen av Norwegian Cyber Range og har startet relaterte prosjekter tilknyttet dette, og samarbeid med andre CCIS partnere (Telenor og FFI) er også initiert.

3.3.2 Forskning

Gruppens forskning fokuserer på å styrke organisasjoners motstandsdyktighet mot og håndtering av dataangrep. Håndtering vil fokusere på å redusere konsekvensen av disse angrepene på individ, organisasjon eller samfunn i tillegg til den underliggende årsaken (f.eks. tap av informasjon eller nedetid av tjenester). Dette vil fordre forskning som kombinerer dyp teknisk analyse og kontekstinformasjon om hva som er kritiske verdier for individet, organisasjonen eller samfunnet.

Gruppen har etablert NTNU CCIS malware lab, et fagmiljø for undervisning, forskning og utvikling, og en arena for samarbeid og kompetanseutvikling. Målet er økt kunnskap om malware i både offentlig og privat sektor. Pågående forskning fokuserer på å øke kunnskapen innen deteksjon og triage av malware.

3.3.2.1 Utvalgte vitenskapelige publikasjoner

- Kirsi Helkala et al., Supporting the Human in Cyber Defence, CyberICPS 2017
- Mass Soldal Lund. Cyber som operasjonsdomene. Norsk Militært Tidsskrift, 186(1):28-34, 2017. (<https://www.oslomilsamfund.no/wp-content/uploads/2017/03/NMT-1-2017.pdf#page=28>)
- DFRWS EU 2017, Gunnar Alendal et al., "Forensics Acquisition — Analysis and Circumvention of Samsung Secure Boot enforced Common Criteria Mode

3.3.2.2 PhD stipendiater

PhD kandidat Sergii Banin (2016-2020), tittel på oppgaven "Applying low-level features for malware dissection and detection", hovedveileder Geir Olav Dyrkolbotn, medveileder Katrin Franke. Stillingen er finansiert av CCIS (JBD).

PhD Kandidat Gunnar Alendal (2016-2020), tittel på oppgaven "Security vulnerability research for use in digital forensics", hovedveileder Geir Olav Dyrkolbotn, medveiledere Stefan Axelsson, Lasse Øverli og Katrin Franke. Stillingen er finansiert gjennom forskningsrådets ArsForensica 248094/O70, ledet av Katrin Franke.

PhD Kandidat Martin Karresand (2017-2019), tittel på oppgaven "Utnytte iboende data strukturer for digital etterforskning", hovedveileder Geir Olav Dyrkolbotn, medveileder Stefan Axelsson, Stillingen er finansiert av CCIS (JBD)

3.3.3 Utdanning

Gruppen har ansvaret for studieretning Cyber Operation i erfaringsbasert master i informasjonssikkerhet. Oppstart var høsten 2016. Studieretningen introdusere tre nye fag ved NTNU; cyber tactics, cyber intelligence og reverse engineering and malware analysis. Geir Olav Dyrkolbotn har ansvaret for studieretningen i tillegg til å underviser reverse engineering and malware analysis. Første gjennomføring av reverse engineering and malware analyse fikk svært positiv tilbakemelding, Pågangen virker stor og 15 studenter tok faget som valgfag.

To masteroppgaver ble gjennomført våren 2017:

- Automated triage of samples for malware analysis, Halvor Mydske Thoresen

- Multinomial malware classification based on call graphs, Morten Oscar Østbye
- Mind the Gap – An Exploratory Study of Commercial and Military Computer Security Incident Response Teams

3.3.4 Viktige møter og aktiviteter

- Malware Forum March 30th (første gang)
- Norwegian Cyber Security Challenge (NCSC)
- Samarbeidsmøter (BDO CERT, NSM/NorCERT, Telenor, CYFOR)
- Diverse foredrag
 - Digital Society Conference, Berlin
 - DND Sikkerhetskonferansen, Bergen
 - STARMUS 2017, Trondheim
 - Yata, Trondheim
- Gjennomført undervisning, veiledning og presentasjoner for NTNU, CYFOR og FIH/CYFOR
- Deltatt i planlegging og gjennomføring av Cyber Defence Exercise (CDX) ved FIH/CYFOR

3.3.5 Medlemmer

Akademisk ansatte, fulltid:

- Geir Olav Dyrkolbotn, førsteamanuensis

Tilknyttede akademiske ressurser:

- Mass Soldal Lund, førsteamanuensis (gjesteforsker)
- Kirsi Helkala, professor (gjesteforsker)

PhD-kandidater:

- Sergii Banin
- Martin Karresand
- Gunnar Alendal

3.4 Digital Forensics

3.4.1 Samarbeid og samarbeidspartnere

Noen sentrale samarbeidspartnere er:

Politidirektoratet; Politihogskolen (PHS); Kripas; Økokrim; Oslo politidistrikt; National Sikkerhetsmyndighet (NSM); FinansCERT; KraftCERT; United Nations Interregional Crime and Justice Research Institute, Italia; Netherlands Forensics Institute (NFI); mnemonic AS; Hitachi Central Research Laboratory, Tokyo, Japan; Synergetics N.V. Group, Belgia; Advanced Technology Institute, Romania; Reality NET System Solutions, Italia; Ericsson AB, Sverige; National Research Council of Italy; University California Santa Cruz, USA; Kyushu Institute of Technology, Japan; University of Groningen, Nederland; University of Malta; National Intelligence Academy, Romania; Edith Cowan University, Australia; Universitetet i Oslo; Norsk Regnesentral (NR).

3.4.2 Forskning

3.4.2.1 Pågående forskningsprosjekter

NTNU Digital Forensics Group har følgende pågående forskningsprosjekter:

- "ACT", Partial Automation of Cyber Investigations and Threat Intelligence; Data enrichment and data fusion methods for cyber threat intelligence; 2016-2019; finansiering Norges Forskningsråd, BIA,, Principal Investigator Professor Katrin Franke.
- "Ars Forensica", Computational Forensics for Large-scale Fraud Detection, Crime Investigation and Prevention; Advanced methods for Big Data Forensics & Forensics as a Service; 2015-2019; finansiering Norges Forskningsråd, IKTPLUSS; Principal Investigator Professor Katrin Franke.

- “Blockchain Technology”, Førsteamanuensis Mariusz Nowostawski, finansiering NTNU CCIS.
- “ESSENTIAL”, Innovative Training Networks: Evolving Security Science through Networked Technologies; Information policy And Law; Forensic Technology, Society, Policies, and the Rule of Law; finansiering EU MSCA-ITN-2016; Principal Investigator Professor Katrin Franke.
- “Hansken”, Feasibility study of “Hansken” – forensics as a service platform – developed by the Netherlands Forensics Institute from a research and future development perspective, 2016-2018, finansiering Justis- og Beredskapsdepartementet og Politidirektoratet, seniorforsker Carl Stuart Leichter, Professor Katrin Franke.
- “Malware lab”, Institusjonalisering av forskning på malware ved NTNU Digital Forensics Group, og en åpen plattform for det norske samfunnet, finansiering CCIS, 2016-, Førsteamanuensis Geir Olav Dyrkolbotn, Professor Katrin Franke.
- “PaySim”, finansiell simulator, Postdoctoral Researcher Edgar Lopez

3.4.2.2 Søknader forskningsfinansiering

- Privacy Assured Intelligent Cyber Vision Systems” (PACVIS), FRINATEK
- “enTrust”, FRIPRO/FRINATEC

3.4.2.3 Utvalgte vitenskapelige publikasjoner

- Arnes, Andre (Ed.) Digital Forensics, ISBN: 978-1-119-26238-1, 376 pages, July 2017.
- Hansen, Hallstein Asheim; Andersen, Stig; Axelsson, Stefan; and Hopland, Svein, "Case Study: A New Method for Investigating Crimes Against Children" (2017). Annual ADFSL Conference on Digital Forensics, Security and Law. 11. <http://commons.erau.edu/adfsl/2017/papers/11>
- Johnsen, Jan William; Franke, Katrin. (2017) Feasibility Study of Social Network Analysis on Loosely Structured Communication Networks, Procedia Computer Science, Volume 108, Pages 2388-2392, ISSN 1877-0509, <http://dx.doi.org/10.1016/j.procs.2017.05.172>.

See online for complete list https://www.ntnu.edu/iik/digital_forensics#/view/publications

3.4.3 Utdanning

NTNU Digital Forensics Group bidrar til utdanninger innenfor følgende områder på Bachelor/Master/PhD nivå:

- BSc, Digital Forensics, Software Security, Introduction to Cryptology
- MSc Digital Forensics, Digital Forensics, Open Source Forensics, Windows Forensics, Cybercrime Investigation, Forensic Intelligence and Data Analytics, Apple-device Forensics, Cryptology, Machine Learning and Pattern Recognition, Computational Forensics, Intrusion Detection and Prevention
- PhD studies, Intrusion Detection and Prevention, Cryptology (selected topics), Wireless Communication Security, Computational Forensics, Computational Intelligence
- Experience-based MSc Digital Forensics.

3.4.4 Viktige møter og aktiviteter

INTERPOL Darknet and Cryptocurrencies Training for the Nordic Countries in Oslo. The training event was initiated by NTNU Digital Forensics group, i.e. Katrin Franke, and launched in a close cooperation between INTERPOL, the Norwegian Police Directorate, NTNU and Police University College (PHS). The event was aimed at law enforcement officials working in the fields of digital forensics and cybercrime investigations. Participants engaged in case-study analysis and game simulations to acquire an in-depth understanding in the investigation of the Darknet and the use of cryptocurrencies. Screening tests was applied before the application’s approval as the seating availability was limited. EUROPOL EC3 representative participated as observer at the training. 08.-12.05.2017.

Digital Forensics textbook published by Wiley, (<http://amzn.to/2vFNtdp>). July 2017.

See list of publications at the end of this report for more details.

ISO Standard Norge is creating a new technical group to discuss the standards in the FinTech area. The project is lead by Standard Norge and two representatives from the research group, Mariusz Nowostawski and Edgar Lopez, became members of the expert group. In this role they are participating in the regular meetings. August 2017.

GEMINI Centre for BigData is a strategic cooperation between SINTEF ICT and the Department of Information and Computer Science at NTNU. Carl Stuart Leichter and Katrin Franke joined the centre as affiliated members. 03.03.2017.

Politi i det digitale samfunn, Research group at the Norwegian Police University College (PHS), headed by Inger Marie Sunde. Stig Åsmund Andersen and Katrin Franke joined as affiliated members contributing to the groups regular meetings and activities. 13.02.2017.

EUROPOL EC3, representative attends the monthly NTNU Digital Forensics Group seminar to gain insides in the ongoing research activities and projects at the NTNU Digital Forensics group. 26.01.2017.

EUROPOL EC3 Awareness campaign against the online coercion and extortion of children. Upon the invitation from Europol, NTNU Digital Forensics Group took part in the awareness campaign. The outreach activities from NTNU Digital Forensics Group were as follows: A landing page for the campaign established, under the main NTNU Digital Forensics Group website - https://www.ntnu.edu/iik/digital_forensics/europol-awareness - containing all relevant information about the campaign, including link to Europol campaign website. Stig Åsmund Andersen gave an interview regarding the campaign, published in Oppland Arbeiderblad, <https://www.aa.no/nyheter/ntnu-i-gjovik/seksuelle-overgrep/seksuelle-overgrep-over-nett-dette-ma-vi-forholde-oss-til/s/5-35-449904>. 19.-25.06.2017.

United Nations Interregional Crime and Justice Research Institute (UNICRI). Professor Katrin Franke has continued the fruitful cooperation with UNICRI. As a prolongation of this cooperation, UNICRI entered into an additional project in May 2017. The projects is titled: "Identification And Analysis Of Malware On Selected Suspected Copyright Infringing Websites". Andrii Shalaginov from NTNU Digital Forensics group has been allocated the project contribution task. The idea of the project is investigate how the malware is disseminated using these websites and what is the harm that such software can cause to end user interested in content like games, movies, TV shows and music. The research methodology included desk review of the existing malware categorisation and relevant cyber threats in 2017. Copyright-infringing website identification and malware collection has been performed during the study. The final point of the study was to analyse collected malware samples using static and dynamic approach to understand their harmfulness.

CCIS / Simula Cyber and Information Security Symposium 2017, Litteraturhuset, Oslo. <http://tinyurl.com/y7q3scx3> The event was organised and coordinated by the NTNU Digital Forensics Group team members, under the leadership of Katrin Franke. She was also the host of the event together with a Simula Research Laboratory representative. The symposium included contributions from the NTNU Digital Forensics Group several members and Ars Forensica project members. Inger Marie Sunde, Norwegian Police University College (PHS) presented on "Cybercrime Prevention and Cybercrime Investigation – What's the Difference from a Rule of Law Perspective?". Mariusz Nowostawski talked about "Virtual Currencies and Crypto Assets: An Overview". PhD fellows from the research group also presented their ongoing research in the poster session of the symposium. 23.05.2017.

NTNU Malware Forum, NSM Sikkerhetskonferansens 2017.

<https://www.ntnu.no/malwarelab/arrangementer> was delivered as an extension of the NSM Sikkerhetskonferansen 2017 <http://tinyurl.com/y8u7zpov>. NTNU Digital Forensics Group co-organised the event in close cooperation NSM NorCERT. The idea behind the malware forum is to gather malware analysts around relevant topics, to establish and to further strengthen the Norwegian community of malware experts. Doctoral research fellow Andrii Shalaginov gave a presentation on "Machine Learning Aided Malware Analysis" at the forum. 30.03.2017.

INTERPOL Cyber Research Seminar, ASEAN Cyber Capacity Development Project, Singapore. Presentation by Carl Stuart Leichter. "NTNU Cyber Security Research and the Testimon Digital Forensics Group". 11.-13.09.2017.

NATO Research Specialists - Content-based Real-Time Analytics of Multi-media Streams (CBMA), work group meeting in London. Professor Katrin Franke upon invitation held a presentation on Multimedia Forensics. The main topic for the meeting was "Content-based information multi-media retrieval and analytics", <https://innsida.ntnu.no/start#/feed//02058439-f8ce-333a-889f-150e95734e32>. 06.09.2017.

SwissRE Blockchain event, Zürich. Mariusz Nowostavski participated in panel, and held an invited keynote talk on "Insurers are building up trust", http://institute.swissre.com/events/Blockchain_insurers_are_building_up_trust.html, talk title: "Preventing the use of blockchain for nefarious purposes". Subsequently, Mariusz Nowostawski published an article in the RISK DIALOGUE MAGAZINE titled "Blockchain: Coming to terms with its virtuous and nefarious capabilities", 23.-24.01.2017.

EUROPOL EC3 Virtual Currencies Conference, The Hague. Mariusz Nowostawski participated, upon invitation only. 21.-22.06.2017.

Max Planck Society, Berlin. "Change from the Inside Out", Keynote presentation by Katrin Franke. 30.09.2017.

Swedish Data Science workshop (SweDS) in Skövde, presentation of current research, "Approximate Search in Large Intrusion Detection and SPAM Filtering Data Sets", professor Slobodan Petrović, November 2017.

COINS Finse Winter School 2017. Carl Leichter (digital forensics) was school instructor, holding the Opening Evening Session talk on “Fundamentals of Computational Forensics: Machine Learning and Predictive Analytics”, and a presentation by Edgar Lopez (simulation) <http://bit.ly/2qUJG5C>. March 2017.

Oslo Blockchain Day. NTNU Digital Forensics group represented by PhD candidate Dmytro Piatkivskyi presented a paper titled “A Collusion Attack on the Lightning Network - Implications for Forensics”. 25.04.2017.

Simula@UiB, seminar lectures, at the Simula@UiB, University in Bergen: Edgar Lopez held lectures upon invitation from Simula. Theme: Financial Transactions for Fraud Research. March 2017.

Annual Ars Forensica Workshop and NTNU Digital Forensics Group Master Student Seminar, at Kripos, Oslo. The workshop assembled project work package leaders, project members, affiliated scientific staff and PhD research fellows. On the first day of the workshop the participants got an update on the research within the project, by presentations by work package leaders and the PhD research fellows. In addition to the status updates from each work package, the cooperation and exchange among the project work packages was discussed, as well as the coordination and reporting within each work package. The future planning of the research activities within the Ars Forensica project for the coming year was also part of first day of the annual workshop. The second day was devoted to master student presentations. 06.-07.06.2017.

INTERPOL Global Cybercrime Expert Group (IGCEG), Katrin Franke continued her advisory services and attended the annually meeting of the group in Singapore, 03.-06.07.2017.

EUROPOL EC3 Academic Advisory Group, Katrin Franke continued her advisory services and transferred from the Internet Security to the Academic Advisory Group. She joined the spring meeting in the The Hague Headquarter on 20.04.2017. For related activities, please see also Section 3. Dissemination and exploitation of results.

United Nations Interregional Crime and Justice Research Institute (UNICRI), Cooperation and exchange with UNICRI was further strengthened, which lead to the engagement of PhD research fellow Andrii Shalaginov in an ongoing **UNICRI malware project**. For related activities see also Section 3. Dissemination.

The Netherlands Forensics Institute (NFI): The research group in the project period continued its cooperation with the Netherlands Forensics Institute (NFI) on Big Data Forensics and the HANSKEN computing platform.

NTNU delegation visiting Japan, NTNU vice-rector research Karin Mellbye lead a NTNU delegation to promote cooperation and exchange with higher education and research institutions in Japan. Katrin Franke was selected to join and to represent NTNU ICT research together with Torbjørn Svendsen, NTNU Digital. Activities included presentations and research planning meetings visits at Kyoto University, [Graduate School of Informatics](#), Nara Institute of Science and Technology (NAIST), [Graduate School of Information Science](#), University of Tsukuba, [Center for Computational Sciences](#), and Department of Statistical Modeling, [Institute of Statistical Mathematics \(IMS\)](#), Tokyo. 24.-28.04.2017.

US Embassy meeting, “Cybersecurity and international crime with FBI Special Agents Jason Lowder and Adrian Hawkins”, by invitation only, Katrin Franke participated, Oslo, 29.09.2017.

ESSENTIAL — H2020-MSCA-ITN-2016, Grant Agreement #722482:

<http://www.essentialresearch.eu/> The Essential team includes members and contributions from Australia, Belgium, Malta, Italy, Romania, the Netherlands, Norway, and Sweden.

ESSENTIAL seeks to develop security science by addressing two of its main problems: the ad-hoc approach to security research and the growing complexity of the security environment. To do so, ESSENTIAL has set itself two main goals: a) to train inter-disciplinary security experts and professionals, to tackle security threats in a systematic manner and b) to increase societal resilience and security by addressing in an interdisciplinary manner 15 research topics, each associated with long-standing problems in the field of security science, ranging from modelling security perception and democratising intelligence to improving security and privacy in data ecosystems.

Out of these 15 research projects, four projects are primarily supervised by members of the NTNU Digital Forensics Research group, i.e. Interoperability and reverse engineering of data policies (ESR-2), Big Data Forensics: Large-scale crime analysis and prevention (ESR-3), Aggregation and linkage of evidential values (ESR-9), and Reliability and admissibility of forensic evidence (ESR-12.)

Research in these topics will further drive and evolve the research profile and direction initiated with the Ars Forensic project, in particular the much stronger interdisciplinary nature of the ESSENTIAL research carried out with an European and International perspective.

3.4.5 Medlemmer

Akademisk ansatte, fulltid:

- Katrin Franke, PhD, Professor
- Carl Leichter, PhD, Seniorforsker, POD/Økokrim
- Slobodan Petrovic, PhD, Professor
- Stefan Axelsson, PhD, Førsteamanuensis, POD/Kripos
- Edgar Lopez, Postdoktor forsker, simulation, JD/CCIS
- Dimitra Anastasoupoulou, MSc, forsker, NFR/ACT

Akademisk ansatte, deltid:

- Jeffery D. Hamm, foreleser, Mandiant/FireEye
- Thomas Walmann, PhD, Førsteamanuensis, Økokrim
- Andre Arnes, PhD, Førsteamanuensis, Telenor
- Lasse Øverlier, PhD, Førsteamanuensis, Forsvarets forskningsinstitutt (FFI)

Tilknyttede akademiske ressurser:

- Inger Marie Sunde, Professor, Politihøgskolen (PHS)
- Hallstein Hansen, PhD, Oslo politidistrikt
- Mariusz Nowostawski, PhD, Førsteamanuensis, NTNU
- Christoffer V Hallstensen, Sikkerhetskonsulent, NTNU

PhD-kandidater:

- Jens-Petter Sandvik, MSc, Kripos
- Gunnar Alendal, MSc, Kripos
- Jul-Fredrik Kaltenborn, MSc, Politihøgskolen (PHS)
- Stig Åsmund Andersen, MSc, Oslo Politidistrikt
- Takashi Watanabe, MSc, Hitachi Central Research Laboratory, Tokyo, Japan
- Andrii Shalaginov, MSc
- Ambika Shrestha Chitrakar, MSc
- Dmytro Piatkivskyi, MSc
- Kyle Porter, MSc
- Jan William Johnsen, MSc
- NN – Ars Forensica
- 4 x NN – ESSENTIAL

Tilknyttede administrativt ansatt:

- Maria Henningson, NTNU

3.5 e-Health and Welfare Security

3.5.1 Samarbeid og samarbeidspartnere

- Collaboration with partners listed in section 2.2 below towards proposal writing and submission in the respective fields.
- Collaboration with Direktoratet for e-helse on long-term research and innovation collaboration.
- Collaboration with Sykehuset Innlandet on long-term research and innovation collaboration.
- Collaboration with Akershus universitetssykehus in the EU proposal HEALTHINUIITY.
- Collaboration with Total Innovation, Sykehuset Innlandet, and Sør-Aurdal Kommune og Weisstech AS in innovation in biometric cryptosystems in local healthcare sector
- Collaboration with Sintef Digital in the PRINATEK proposal on medical device security
- Collaboration with NTNU's Center for Care Research and Norwegian Centre for e-health research in the research proposal towards Helse Midt-Norge research call

3.5.2 Forskning

3.5.2.1 Research activities:

- Assoc. Prof. Bian Yang
 - Biometric cryptosystem technology adaptation in healthcare sector
 - Blockchain technology and on-chain privacy-preserving technologies
 - Data democracy platform architecture for health data management
 - Secure and flexible sharing of outsourced healthcare data, for example, on the public cloud
- Dr. Huihui Yang
 - Literature survey about the security and privacy challenges of Norwegian healthcare
 - Blockchain technology on healthcare, to secure share healthcare data in a decentralized environment.
 - Attribute-based access control and encryption for healthcare services
- Dr. Vivek Agrawal
 - Electronic Community of Practice in healthcare sector
 - Investigation of the conflict between the information security compliance requirements and the operational requirements of the healthcare.
 - Secure knowledge transfer mechanism

3.5.2.2 Proposals:

EU proposals

- HEALTHINUIITY: EXODUS (GR); FUNDACION TEKNIKER (ES); Sociedad Europea de Analisis Diferencial de Movilidad (ES); Crowd Dynamics (UK); Diginext (FR); Telesto (GR); CERTH (GR); CINI (IT); Engineering – Ingegneria Informatica (IT); Gobierno Vasco (ES); Akershus universitetssykehus (NO); Neuromed (IT); Universita campus Bioemica (IT); Eticas (ES); Nextel (ES); Institute of accelerating systems and applications (GR); SNV Engineering (GR); Servicio Vasco de Salud (ES); Ministero dell Interno (IT)
- OPEN: TALLINNA TEHNIKAULIKOOL (EE), UNIVERSITAT ZU LUBECK (DE), UNIVERSITATSKLINIKUM SCHLESWIG-HOLSTEIN (DE), UNIVERSITATSMEDIZIN ROSTOCK (DE), UNIVERSITAET ROSTOCK (DE), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (DE), SysTek GmbH (DE), HOGSKULEN PA VESTLANDET (NO), HELSE BERGEN HF*HAUKELAND UNIVERSITY HOSPITAL (NO), Medisoft AS (EE), Estonian Health and Welfare Information Systems Center (EE), ARSENAL.IT - CENTRO VENETO RICERCAE INNOVAZIONE
- PER LA SANITA DIGITALE (IT), Martest Research OÜ (EE), International Business Machines AS (NO), UNIVERSITAET AUGSBURG (DE)
- I-SMART: MEDTRONIC IBERICA SA (ES), INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM (BE), FUNDACIO TICSALUT (ES), TSB REAL TIME LOCATION SYSTEMS SL (ES), ENGINEERING - INGEGNERIA INFORMATICA SPA (IT), FUNDACIO PRIVADA UNIVERSITAT I TECNOLOGIA (ES), ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (GR), PHARMATICS LIMITED (UK), Ajuntament de Mataró (ES), Fundació Privada Salut del Consorci Sanitari del Maresme (ES).
- PIMAS: BANTEC CONSULTORES INICIATIVAS EMPRENDEDORAS SL (ES), FUNDACION TECNALIA RESEARCH & INNOVATION (ES), UAB E-BROS (LT), CONSORZIO PER IL SISTEMA INFORMATIVO (CSI PIEMONTE) (IT), FUNDACIO TICSALUT (ES), STELAR SECURITY TECHNOLOGY LAW RESEARCH UG (DE).
- PriMa: University of Twente (NL), University of Kent (UK), Norsk Regnesentral Stiftelse (NO), Julius-Maximilians Universitaet Wuerzburg (DE), Katholieke Universiteit Leuven (BE), Universidad Autonoma de Madrid (ES).
- SafetyIntelligence: Danish Institute of Fire and Security Technology (DK), Lund University (SE), Aalborg University (DK), University of Wuerzburg (DE), Fraunhofer Institute for Computer Graphics Research (DE).

Other proposals

1. OPEN (H2020 EINFRA-12-2017) OPEN PSEUDONYMISED HEALTH DATA AND DISTRIBUTED COMPUTING E-INFRASTRUCTURE FOR MEDICAL SCIENCE AND CLINICAL PRACTICE. Unsuccessful. Thomas Kemmerich and Bian Yang
2. HEALTHinuity (H2020 CIP-2016-2017-2): A total security solution for safeguarding the well-being and continuity of the healthcare sector against physical and cyber threats. Unsuccessful. Sokratis Katsikas and Bian Yang
3. I-SMART (H2020-IOT-2016-2017) IoT-enabled service platform for the creation of cross-sectorial SMART services for smart actuation and knowledge generation, through integration of existing IoT ecosystems in health and cities. Unsuccessful. Bian Yang and Stephen Wolthusen

4. PIMAS (H2020-DS-08-2017) Private Identities Management Across Services. Unsuccessful. Bian Yang
5. Helse Midt-Norge research call: Implementation of shared electronic patient records (EPR) across multiple health institutions and administrative levels. Unsuccessful. Staal Vinterbo and Bian Yang
6. FORNY 2017: A Biometric Cryptosystem for Healthcare. Unsuccessful. Bian Yang
7. FRINATEK 2017: Cybersecurity in Connected Medical Devices. Under evaluation. Marie Moe and Bian Yang
8. PriMa (ITN- H2020-MSCA-ITN-2018) Privacy Matters. Under evaluation. Bian Yang and Christoph Busch
9. SafetyIntelligence (ITN- H2020-MSCA-ITN-2018) Multi-Modal Sensing and Intelligent Safety Analytics for Human Behaviours Understanding in Context. Under evaluation. Bian Yang and Christoph Busch
10. RFF INNLANDET PreProject 2017: Fingerprint as a Key Box. Granted. Guoqiang Li and Bian Yang
11. Helse-EU: Digital patients: tilrettelegge for digitale, sikre, persontilpassete og skalerbare helsetjenester. Granted. Stewart Kowalski, Einar Snekkenes, and Bian Yang

3.5.2.3 Projects:

- iSeelce (RFF-INNLANDET): ice intelligence and welfare network
- FingerKeyBox (RFF-INNLANDET): privacy-preserving fingerprint based private credential management

3.5.2.4 Invited talks

- Enhancing the Trust in e-Health by Secure and Privacy-Preserving Identity Management, Digital Enlightenment Health Data Workshop, Oct.25th, Brussels, Bian Yang
- Secure data management towards DLT for eHealth, IOTA workshop at Oslo Med Tech, June 21th, 2017, Oslo, Bian Yang

3.5.2.5 Selected publications

- Huihui Yang, Bian Yang, "A Blockchain-based Approach to the Secure Sharing of Healthcare Data," NISK 2017
- Jialiang Peng, Bian Yang, "A Novel Binarization Scheme for Real-Valued Biometric Feature," COMPSAC (2) 2017: 724-729
- Hao Luo, Tien-Szu Pan, Jeng-Shyang Pan, Shu-Chuan Chu, Bian Yang, "Development of a Three-Dimensional Multimode Visual Immersive System With Applications in Telepresence," IEEE Systems Journal 11(4): 2818-2828, 2017
- Mohamed Abomhara, Huihui Yang, Geir M. Kjøien and Mehdi Ben Lazreg, "Work-based Access Control Model for Cooperative Healthcare Environments Modeling and Verification", Journal of Healthcare Informatics Research, Vol. 1, Issue 1, pp 19-51, 2017.
- Edlira Martiri, Marta Gomez-Barrero, Bian Yang, Christoph Busch: Biometric template protection based on Bloom filters and honey templates. IET Biometrics 6(1): 19-26 (2017)
- Mohamed Abomhara and Huihui Yang, "Collaborative and Secure Sharing of Healthcare Records Using Attribute-based Authenticated Access", International Journal on Advances in Security, vol.9, no. 3&4, 2016.
- Utdanning

3.5.3 Viktige møter og aktiviteter

- Oslo seminar organized by HoD (March 1st, 2017): eHWS with its strategy goals and ongoing research work are presented to colleagues in HoD
- eHealth Week 2017 (May 10-12th, 2017): eHWS was promoted via social chats in the meeting venue
- Meeting with IKT colleagues from Sykehuset Innlandet (May 9th, 2017): research profiles and collaboration methodology were discussed
- Meeting with Clinical informatics people from Akershus universitetssykehus (June 19th, 2017): research profiles and collaboration methodology were discussed

3.5.4 Medlemmer

Akademisk ansatte, fulltid:

- Assoc. Prof. Bian Yang

- Dr Vivek
- Dr Huihui Yang

Akademisk ansatte, deltid:

- Prof. Einar Snekkenes
- Prof. Stewart James Kowalski
- Prof. Stephen Wolthusen
- Assoc. Prof. Marie Moe
- Assoc. Prof. Thomas Kemmerich

Master student

- Øyvind Toftegaard

3.6 Information Security Management

3.6.1 Samarbeid og samarbeidspartnere

- Professor Staal A. Vinterbo join the group in March 1st. and has been initiated dialog with Datatilsynet. He gave an invited lecture "A Brief intro to anonymity, disclosure control and randomness".
- Colonel Renee Underwood, United States Army attache of the Embassy of the United States of America provided valuable feedback and assistance in the Digital Board Squad submission to the brief work assistance to the Cyber 9/12 Challenge
- A panel discussion with NKOM, Simula, and CSO of Telenor was organized on the topic of "Is Cyber Security as a Public Good. Who Decides and Who Pays was organized by members of the group at the CCIS Spring Symposium.
- Cooperated with NORSIS to in the organization and execution of the Security Top Leader Forum in May.

3.6.2 Forskning

Information about ongoing research and perhaps research proposal that are in development or just sent in

3.6.2.1 Ongoing Projects

UnRizkNow: A community of practice for cyber risk practitioners:

The objective of this project is to establish an online-based community of practice for cyber security risk practitioners. The online community of practice should be the target's group preferred venue for gathering and sharing information and knowledge in the community domain. The main target group will be cyber risk practitioners in small and medium-sized business. The project will start from the cyber security risk practitioners in Norway, but it will gradually involve practitioners from across the globe to bring it into International arena

3.6.2.2 Proposal submitted to NordForsk

The **Secure Eco-system Learning Hub (SEECOLE-HUB)** will establish a mobile Nordic community of university cyber security educators, researchers and doctoral students the share case based and challenges based teaching and research methods to cover aspects of law, policy and human factors, ethics and risk management for the secure adoption of Internet of Things technology in Urban and Rural environments in the Nordic countries. This Nordic community will interact with the local governments, innovators and end-users by establishing and coordinating regional advisor boards, in Norway, Sweden, Denmark and Finland.

3.6.2.3 Proposals under development

Assurance for system-of-systems security: modeling measuring, managing

- Problem: Systematics and General systems theory have a long academic tradition that can be traced back to the ancient Greeks and Pythagoras. The basic research approach and theories has not change much in 3000 years and is to either discover or create patterns that can be used to understand and predict past, present and future events of an artifact in focus. Security assurance and systems assurance are defined as the degree of confidence that the security needs and requirement of a system are meet. Consequently, research into assurance for systems-of-systems security is about finding and creating models and measurements to predict with different degrees of confidence that that the systems-of-systems that is in focus will be secure enough.

3.6.2.4 Selected publications

- Agrawal, V., & Szekeres, A. (2017, June). CIRA Perspective on Risks Within UnRiskNow - A Case Study. In Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on (pp. 121-126). IEEE. 10.1109/CSCloud.2017.14
- Wen, Shao-Fang; Kowalski, Stewart James. (2017) A Case Study: Heartbleed Vulnerability Management and Swedish Municipalities. Human Aspects of Information Security, Privacy and Trust.
- Agrawal, Vivek; Snekkenes, Einar Arthur. (2017) An Investigation of Knowledge Sharing Behaviors of Students on an Online Community of Practice. Proceedings of the 5th International Conference on Information and Education Technology, ICIET, Jan 10-12 2017, Tokyo, Japan.

3.6.2.5 Awards

December 2017 Stewart Kowalski receive the Association of Information Systems prize for Innovation in Teching.

3.6.3 Utdanning

PhD-students that are finished so far in 2017:

- Gaute Wangen
 - Cyber Security Risk Assessment Practices: Core Unified Risk Framework. Norges teknisk-naturvitenskapelige universitet 2017 326-2378-5; Volum 2017.185 s. Doktoravhandling ved NTNU(153). NTNU

Master students that are finished so far in 2017:

- Tonje Andreassen: *The role of trust when implementing Network Based Defence in the Norwegian Armed Forces*
- Henrik Tørresby: *Recommendations for Improving Protection of Sensitive Information in Defence Material Procurement*
- Terje Benjaminsen: *The Norwegian Downsizing Approach in Terms of the Insider Threat*
- Henrik Hansen: *Approaching the BYOD trend securely*

3.6.4 Viktige møter og aktiviteter

- Workshop with ISF Norway on 26th April at Noble peace center, Oslo [<https://www.isf.no/isf-varmote-pa-nobels-fredssenter/>]
- Workshop with ISACA Norway on 21st June at Oslo, [https://www.deltager.no/isaca_sommermote_2017]
- Poster presentation at CCIS symposium on 23rd May at Oslo [<https://ccis.no/cyber-information-security-symposium-2017-digital-resilience/>]
- Meeting with Kari Laumann at Datatilsynet on the involvement of Personvernombud in the data collection activity
- NTNU CCIS acted as Platinum Sponsor for the ESORICS conference and the Information Security Management Group at NTNU provided the General and Organization Chair of the conference, Prof. Dr. Einar Snekkenes and Associate Prof. Dr. Laura Georg. Prof. Dr. Sokratis Katsikas from NTNU CCIS, acted as Workshop Chair.
- *Med personopplysninger som valuta*, Op-ed in Oppland Arbeiderblad
- *Protecting personal information is insufficient for privacy*, at Big Data – Energy and Networks (Trondheim)

3.6.5 Medlemmer

Akademisk ansatte, fulltid

- Einar Arthur Snekkenes, Professor
- Staal A. Vinterbo, Professor
- Stewart Kowalski, Professor

Akademisk ansatte, deltid:

- Laura Georg, Associate Professor
- Bernhard Markus Hämmerli, Professor
- Gaute Wagne, Post Doc

Tilknyttede akademiske ressurser:

- Richard McEvoy

PhD-kandidater:

- Adam Szekeres
- Vivek Agrawal
- Shao-Fang Wen