NTNU CCIS
Center for Cyber and
Information Security

m

Årsrapport 2019

NTNU Center for Cyber and Information Security

Gjøvik, 1. april 2020

Innholdsfortegnelse

NTNU CCIS
Center for Cyber and Information Security

1 Innledning

NTNUs Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for forskning, utdanning og kompetansebygging innen cyber- og informa-sjonssikkerhet. 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 akademia. 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 2019 følgende 26 partnere i tillegg til vertsinstitusjonen NTNU: Cyberforsvaret (CYFOR), Datatilsynet, Eidsiva, Forsvarets forskningsinstitutt (FFI), Høgskolen i Innlandet, IBM, Innlandet politidistrikt, 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 sikkerhetstjeneste (PST), Politihøgskolen (PHS), PwC, Sykehuset Innlandet HF, Statkraft, Statnett, Telenor, Watchcom Security Group og Økokrim.

2 Årsberetning

2.1 Styrets arbeid og generalforsamling

Styret i NTNU CCIS består ved inngangen til 2020 av:

- Ingrid Schjølberg, Norges teknisk-naturvitenskapelige universitet (NTNU), styreleder – (2018-2019)
- Mona Strøm Arnøy, Nasjonal sikkerhetsmyndighet (NSM), nestleder – (2017-2019)
- Hanne Tangen Nilsen, Telenor – (2017-2019)
- Kristin Ottesen Kvigne, Politidirektoratet (POD) – (2017-2019)
- Knut Ivar Rønning, Cyberforsvaret (CYFOR) – (2017-2019)
- Ingeborg Dårflot, Statkraft – (2018-2020)
- Siw Hansen Thokle, Politihøgskolen (PHS) – (2018-2020)
- Tønnes Ingebrigtsen, mnemonic AS – (2018-2020)
- Staal Vinterbo, NTNU CCIS ansattrepresentant – (2018-2020).

I parentes indikeres perioden som medlemmene opprinnelig var valgt for. For å holde kontinuiteten i styrearbeidet og kunne forbedre de formelle prosessene i NTNU CCIS har styrets representanter blitt forespurt om å kunne utvide sin periode i styret slik at de som var valgt for perioden 2017-2019 sitter til 2021 og de som var valgt for perioden 2018-2020 sitter til 2022. Dette forslaget støttes av alle styremedlemmer, med unntak av Ingeborg Dårflot (Statkraft) som ikke lenger ønsker å være representert i NTNU CCIS sitt styre. Forslaget om utvidede styreperioder vil bli fremmet for generalforsamlingen i 2020.

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 110 ansatte på tvers av NTNUs campus i Trondheim og Gjøvik.

I 2019 har Nils Kalstad, instituttleder for IIK, også fungert som leder av og koordinator for aktiviteten i NTNU CCIS. Senteret videreført ordningen med en konstituert vitenskapelig styringsgruppe som i 2019 har bestående av førsteamanuensis Bian Yang, førsteamanuensis Geir Olav Dyrkolbotn, professor Katrin Franke, professor Patrick Bours, professor Sokratis Katsikas og professor Stewart Kowalski (frem til 30.06.2019). Seniorrådgiver Inge Øystein Moen har i 2019 administrativt understøttet aktiviteten i NTNU CCIS i tillegg til at senteret har bred administrativ støtte fra vertsinstitutt og -fakultet.

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 and Privacy Management.

I 2019 har IIK gjennomført en prosess med gjennomgang og gruppering av forskningsaktiviteten ved instituttet. Dette har resultert i to nye grupper som er av særlig interesse for NTNU CCIS:

- Applied Cryptography
- Systems Security.

Styret i NTNU CCIS vedtok i 2019 at man ønsker å invitere disse gruppene inn i senteret. Et annet resultat av gjennomgangen er at gruppen Information Security and Privacy Management har noe mindre oppslutning. I 2020 vil det derfor være nødvendig å se på fremtiden til dette fokusområdet i CCIS. Ellers gjelder det fortsatt at 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 konsortiebygging, 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:

- CyberSec4Europe (H2020)
  En av fire piloter for et fremtidig Europeisk kompetansenettverk for cybersikkerhet
- SDN-microSENSE (H2020)
  Prosjektet kal etablere og demonstrere et desentralisert system for produksjon og distribusjon av elektrisk energi som er sikkert, motstandsdyktig mot cyber-angrep, beskytter personvernet og robust mot datainnbrudd.
- Veikart med prosedyre for sikkerhet når industrien digitaliseres (Norsk Industri)
  Prosjektet skal etablere retningslinjer for god praksis for sikker digitalisering av industrien
- Privacy Matters Innovative Training Network (PriMa, H2020)
  Skal bringe sammen forskertalenter til å utvikle løsninger for å bevare personvernet gjennom digitaliseringen.
- Digital technologies for post-operative remote care and rehabilitation of thoracic and cardiac surgery patients (NFR)

Gjennom statsbudsjettet for 2018 og revidert statsbudsjett 2018 fikk NTNU finansiering til 12 nye Ph.D. stillinger i informasjonssikkerhet fra Kunnskapsdepartementet. Av disse gikk tre stillinger til kryptologi, 1 stilling til didaktikk, 1 til samarbeid med NSM i lys av Nasjonal strategi for digital sikkerhet, 1 til samarbeid med NC_3, 1 til sikkerhet i cyber-fysiske systemer, 1 til biometri og 1 til personvern. Ansettelse skjer i 2020, og alle disse vil ha en tilknytning til NTNU CCIS.

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

2.4 Utdanning

NTNU CCIS har i tillegg til vertsinstitusjonen NTNU flere utdanningsinstitusjoner i partnerskapet. Forsvarets ingeniørhøgskole, Høgskolen i Innlandet og Politihøgskolen 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 kommunikasjonsteknologi
- 5-årig masterstudium i teknologi/sivilingeniør i kommunikasjonsteknologi
- 2-årig engelskspråklig masterstudium «Information Security»
- 2-årig engelskspråklig masterstudium «Communication Technology»

- 1.5-årig erfaringsbasert masterstudium «Information Security»
- 3-årig bachelorstudium i Digital infrastruktur og cybersikkerhet

Erfaringsbasert mastergrad i informasjonssikkerhet tilbys i samarbeid med Politihøgskolen, 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. Den erfaringsbaserte masteren hadde i 2019 gode søkertall, noe som tyder på at denne utdanningen er i ferd med å etablere seg i markedet.

Bachelorutdanningen som tidligere het IT-drift og informasjonssikkerhet ble lansert i en ny versjon i 2019 med navnet Digital infrastruktur og cybersikkerhet. I tillegg til nytt navn og ny struktur så ble utdanningen for første gang også tilbudt i Trondheim. De 90 studieplassene i Gjøvik og 50 i Trondheim ble svært godt mottatt i markedet med henholdsvis 5 og 10 primærsøkere pr studieplass i 2019.

I 2019 har det vært avholdt fire Ph.D. disputaser innen informasjonssikkerhet ved IIK:

- Pankaj Shivdayal Wasnik: *Robust Biometrics on Smartphones – Using Quality Assessment, Presentation Attack Detection and Biometric Fusion*
- Patrick Schuch: *Deep Learning for Fingerprint Recognition Systems*
- Ambika Shresta Chitrakar: *Constrained Approximate Search and Data Reduction Techniques in Cybersecurity and Digital Forensics*
- Christopher Alan Carr: *Towards Fairness and Decentralisation in Modern Cryptology*

Videre har 27 studenter har presentert sine masteroppgaver på Master i informasjonssikkerhet, 43 studenter har presentert sine bacheloroppgaver på Bachelor i IT-drift og informasjonssikkerhet og 37 studenter leverte sine masteroppgaver ved siv.ing. i kommunikasjonsteknologi i 2019.

2.5 En synlig samfunnsaktør

NTNU CCIS skal være en synlig samfunnsaktør. Dette avsnittet gir en oversikt over de mer profilerte aktivitetene i 2019.

2.5.1 NISlectures ble til CCIS lecture

Foredragsserien NISlectures fortsatte i 2019, men omdøpt til CCIS lecture, med temaene:

- *Nammos erfaringer med cybersikkerhet*
  Ole Ingarth Karlsen, Vice President Information Technology and Security, Nammo AS
- *ABC Security – fra forskning til forretning*
  Bian Yang, førsteamanuensis IIK, NTNU
  Ragnhild Skarpen, CEO, ABC Security
- *Praktisk informasjonssikkerhet; NT6 som arena for lokale synergier og innovasjon*
  Mats Thorvaldsen, daglig leder IOPS
  Terje Krogstad, prosjektleder Escio
- *Politiets Avsnitt for digitalt politiarbeid*
  Eyvind Grytting, leder digitalt politiarbeid, Innlandet politidistrikt
- *Informasjonssikkerhetsforskning i Sykehuset Innlandet*
  Ingeborg Hartz, Forskningsdirektør Sykehuset Innlandet HF
  Grethe Østby, PhD-stipendiat, NTNU
- *Graphchain – graph is the new block!*
  Hege Tokerud, Innovation Manager, NTNU TTO
- *Using Behavioural Biometrics Beyond Gaining Access*
  Patrick Bours, Professor IIK, NTNU
- *Reconstruction of the Clock Control Sequence in Pseudorandom Sequence Generators Employing Irregular Clocking by Means of Constrained Bit-Parallel Search*
  Slobodan Petrovic, Professor IIK, NTNU
- *Deep Learning based Malware Detection and Classification*
  Ferhat Ozgur Catak, post-doctoral researcher IIK, NTNU

2.5.2 Nasjonal strategi for digital sikkerhet

Den 30. januar ble Nasjonal strategi for digital sikkerhet lansert av statsminister Erna Solberg, samfunnssikkerhetsminister Ingvild Smines Tybring-Gjedde, justis- og innvandringsminister Tor Mikkel Wara, forsvarsminister Frank Bakke-Jensen og forsknings- og høyere utdanningsminister Iselin Nybø. NTNU CCIS er nevnt fem ganger i strategien og dens tiltaksplaner. Norwegian Cyber Range prosjektet er definert som tiltak 27 i hovedstrategien og med NTNU som ansvarlig virksomhet. Videre nevnes følgende prosjekter i kunnskapsstrategien:

- NTNU CCISs basisbevilgning fra JD og HOD til å utvikle områder som personvern, digital etterforskning, biometri og digital sikkerhet i helsesektoren.
- CyberSmart: En pilot for opplæring av barn og ungdom som kjøres av NTNU CCIS i samarbeid med NSM, NVE, NorSIS, UiO, Forsvaret Høgskole Cyberingeniørskolen og Abelia.
- CyberSec4Europe: Et pilotprosjekt som del av den fremtidige etableringen av et felles europeisk kompetansenettverk for digital sikkerhet, NTNU CCIS og SINTEF er norske partnere
- European Cyber Security Challenge: En nasjonal og internasjonal konkurranse for å synliggjøre unge talenter.

2.5.3 NBL annual workshop

Den 7. mars gjennomførte Norwegian Biometrics Laboratory sitt niende 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 2019 fokuserte på blockchain og 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).

2.5.4 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 25. og 26. 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. I 2019 stilte vi 3 lag, hvor et var ett samarbeidslag med West Point og ett var i samarbeid med Forsvaret høgskole - Cyberingeniørskolen.

2.5.5 Digital Forensics Research Workshop

Digital Forensics Research Workshop EU 2019 (https://dfrws.org/conferences/dfrws-eu-2019/) ble arrangert hos KRIPOS 24.-26. april. Dette er en workshop som har vært arrangert 18 ganger i USA mens arrangementet på KRIPOS var det sjette arrangementet i Europa. DFRWS samler forskere, utviklere og ansatte i politisektoren fra hele verden for å adressere tverrfaglige utfordringer i digital etterforskning. Det var 300 deltagere fra alle kontinenter på arrangementet, og svært gledelig var det høye antallet deltagere fra politisektoren.

2.5.6 Cyber Symposiet og Paranoia

Det fjerde Cyber Symposiet ble organisert som en halvdags konferanse i forkant av Paranoia den 22. mai. 130 representanter fra partnerne i CCIS og andre virksomheter samlet seg for å høre innlegg fra Telenor, Huawei, Forsvarets logistikkorganisasjon, Cyberforsvaret og NTNU. Cyber Symposiet ble også i 2019 arrangert i samarbeid med SIMULA MET. Etter symposiet var NTNU CCIS representert med stand på Paranoia. Et nytt tiltak fra vår side og det var hyggelig å observere at standen hadde en jevn strøm av besøkende.

2.5.7 Malware forum

Den 5. juni 2019 arrangerte NTNU Malware Lab det tredje Malware Forum, i tett samarbeid med NSM/NorCERT. Nok en gang et fullbooket arrangement med foredragsholdere fra FireEye, Google, Symantec, TU Munchen og NorCERT. Førsteamanuensis Geir Olav Dyrkolbotn leder programkomiteen for Malware Forum som i 2019 hadde ca 90 deltagere.

2.5.8 COINS Finse Winter School

Den 5.–10. mai ble COINS Finse Winter School avhold. Vinterskolen på Finse har etablert seg som en møteplass for det norske forskingsmiljøet i informasjonssikkerhet, og tiltrekker seg også gode, internasjonale foredragsholdere. De inviterte foredragsholderne spente over tematikk fra økonomien i standardisering og sertifisering av sikkerhet til symmetrisk

kryptografi. Blant innlederne i 2019 fant vi Dietmar Bremser (German Federal Office for Information Security), Joan Daemen (Radboud University in Nijmegen), Part Preneel (University of Leuven) og Adi Sharmir (Wizmann Institute of Science). Studentpresentasjonene ga en mulighet for doktorandene til å få tverrfaglige tilbakemeldinger på deres forskning fra eksperter.

2.5.9 Sikkerhetsfestivalen 2019

Sikkerhetsfestivalen ble arrangert for første gang på Lillehammer 26. – 30. august. Norsk informasjonssikkerhetsforum var hovedarrangør med god støtte fra bl.a. mange av partnerne i CCIS inkludert. NSM, Oppland Fylkeskommune, NorSIS, Cyberforsvaret og NTNU. NTNU CCIS arrangerte et eget spor over to dager med fokus på FoU utfordringer i tilknytning til Nasjonal strategi for digital sikkerhet. I tillegg arrangerte NTNU CCIS et Megagame med 80 deltagende ungdommer og studenter i Eidsiva Arena. Her fikk kjenne på noen av utfordringene knyttet til å håndtere cyber sikkerhetshendelser på globalt nivå. Gjennom hele uka arrangerte også NTNU Digital Forensics Group 1st International Summer School on Computational Forensics som en del av Sikkerhetsfestivalen. Sommer skolen ble arrangert som en del av samarbeidet COST Action CA17124 "Digital forensics: evidence analysis via intelligent systems and practices" og International Association of Pattern Recognition (IAPR) sin TC6 på Computational Forensics og samlet nesten 30 deltagere på Lillehammer.

2.5.10 Immatrikulering og møte med samfunnssikkerhetsministeren

Samfunnssikkerhetsminister Ingvild Smines Tybring-Gjedde deltok på immatrikuleringen 2019 ved NTNU i Gjøvik. Som en del av arrangementet ble det gjennomført et møte mellom Justis- og beredskapsdepartementet og NTNU ved rektor, IIK og NTNU CCIS. Temaet for møtet var gjensidig samarbeid med særlig fokus på oppfølging av handlingsplanen til Nasjonal strategi for digital sikkerhet og et pågående initiativ for å etablere nasjonal kapasitet innen reverse engineering i samarbeid med kraftsektoren (NVE, KraftCERT, NSM m.fl.).

2.5.11 SikkertNOK

SikkertNOK ble i 2019 arrangert for niende gang på Gjøvik som en åpen og fritt tilgjengelig avslutningskonferanse for Nasjonal sikkerhetsmåned i samarbeid med NorSIS. I 2019 var temaet «Information Security in the Norwegian Health Care Sector» tema, med foredragsholdere fra akademia og virksomheter. Seminaret ble innledet av Bjørn Astad fra Helse- og omsorgsdepartementet etterfulgt av innlegg fra Sykehuset Innlandet, NTNU, ABC Security AS, CGI Norge AS og NorSIS.

2.5.12 CyberSmart rapport overlevert JD

18. oktober leverte CyberSmart prosjektet rapporten etter gjennomført pilot til Justis- og beredskapsdepartementet. Rapporten som ble overlevert til samfunnssikkerhetsministeren beskriver erfaringer som prosjektet sitter igjen med etter bl.a. befaring i Tulsa (USA), gjennomføring av kurs for lærere på ungdomstrinnet i Oslo, pilot gjennomføring ved Godalen VGS og lærerkurs med undervisere fra USA. Prosjektet ser behovet som finnes blant undervisere i grunnskolen og anbefaler en videreføring av satsningen fra departementene. Prosjektet foreslo en organisering med tilknytning til Nasjonalt senter for realfagsrekruttering. Det ble sendt en søknad til JD i etterkant av overleveringen.

2.5.13 Samarbeidsavtale om øving og trening i cyberdomenet

Cyberforsvaret, Telenor Norge AS, Politidirektoratet og NTNU inngikk høsten 2019 en samarbeidsavtale med intensjon om å 1) Utvikle et grunnlag for øving og trening i cyberdomenet, tett knyttet til Norwegian Cyber Range 2) Utvikling av felles kapasitet for gjennomføring av gradert eller særlig skjermet øving og trening. Kapasiteten har arbeidstittel «cyber stabs- og ledertrener» (CSLT) med målsetning om å dekke helheten i aktørenes behov for trening og øving i cyberdomenet 3) Bidra til etablering av et kommersielt tilgjengelig tilbud om øving og trening i cyberdomenet og 4) Utvikle et koordineringsforum for sertifisering og utdanning.

2.5.14 SFI søknaden NORCICS

Sammen med gode partnere i Hafslund Nett AS, Norsk Hydro ASA, Kongsberg Gruppen ASA, mnemonic, Yara Internationa ASA, Sykehuset Innlandet HF, Equinor ASA, Momoscale AS, Norsk Regnesentral, Lyse Elnett AS, Helgeland Kraft AS, Siemens AS, Oslo Politidistrikt, NC-Spektrum, NorSIS, Sintef Digital, Sintef Energi, Sintef Manufacturing og Universitetet i Agder sendte vi 23.10 inn en søknad til Norges forskningsråd om etablering av et Senter for forskningsdrevet innovasjon (SFI). Norwegian Center for Cybersecurity in Critical Sectors vil, hvis finansiert, bidra til å utvikle relevante private og offentlige aktørers evne til å bedre respondere til dagens og fremtidens cybersikkerhetsrisiko. Sokratis Katsikas er foreslått som senterleder, med Katrin Franke som nestleder. Svar på søknaden forventes i 2020.

2.5.15 Norwegian and European Cyber Security Challenge

På oppdrag fra Justis- og beredskapsdepartementet arrangerte IIK gjennom samarbeidet i NTNU CCIS Norwegian Cyber Security Challenge i 2019 og Norges deltagelse i European Cyber Security Challenge fra 8.10 til 12.10 i Bucuresti, Romania. 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 capture the flag konkurranse og en nasjonal finale organisert på Gjøvik den 27. april ble følgende deltagere med på landslaget i cyber sikkerhet: Martin Ingesen (kaptein), Sturla Bae, Simen Lybekk, Bendik Hagen, Henritte Garder, Birk Tjelmeland, Sander Godard, Silje Stadheim, Harald Aarseth, Anders Felde og reservene Anders Engeroen og Johan Åsbakk . Disse ble trent av Nikolai Magnussen og Anders B. Wilhelmsen. For mer informasjon se https://www.ntnu.no/ncsc.

2.5.16 KommuneCSIRT

24. oktober ble etableringen av KommuneCSIRT annonsert med en orientering til Kommunalminister Monica Mæland. KommuneCSIRT er et IKS som etableres av Lillehammer og Gjøvik kommune. NTNU CCIS er ikke direkte involvert i prosessene knyttet til KommuneCSIRT, men etableringen er et tegn på den posisjon som NTNUs campus på Gjøvik har fått innen anvendt informasjonssikkerhet og et tegne på den interesse som Lillehammer og Gjøvik region har for å satse på å skape næring knyttet til fagområdene som NTNU CCIS fronter. NTNU CCIS vil være representert med en styrerepresentant i KommuneCSIRT.

2.5.17 Annen eksponering og arrangementer

En ikke uttømmende liste av andre arrangementer og organisasjoner hvor NTNU CCIS har vært representert i 2019 er:

- Arrangement i samarbeid med Telenor og BI under Arendalsuka
- Deltagelse i Transport 21
- Etablerte et felles emne i informasjonssikkerhetsledelse i samarbeid med BI
- Deltar i Forum for nasjonal IKT-sikkerhet organisert av Justis- og beredskapsdepartementet
- Er norsk node i nettverket North European Cybersecurity Cluster
- Er representert i European Cyber Security Organisation
- Deltagelse på Lock Shields start dag ved NATO CCDCOE i Tallin og på besøksdagen ved den norske noden
- Organiserte forelesningsserie om Sikker digital transformasjon for Sparebank 1 Østlandet som pilot for bedriftsintern EVU
- Representert på den amerikanske ambassaden i Oslo sitt næringsdelegasjonsbesøk høsten 2019
- Deltagelse på frokostmøter ved den britiske ambassaden i Oslo
- Deltagelse på Økokrim sitt 30-års jubileum
- Deltagelse på POD workshop: Fremtidens kompetansebehov i politisektoren
- Er representert i referansegruppen til Nasjonalt Cybersikkerhetssenter (NCSC)
- Er observatør i Oppland fylkeskommune sitt prosjekt CyberLand.

2.6 Regnskapsrapport

Regnskapsrapporten under viser totaløkonomien for NTNU CCIS. Dette inkluderer bevilgninger, partnerbidrag og NTNU sine bidrag som vertsinstitusjon. Senteret har i 2019 økt sin aktivitet og vi ser at flere ansettelser har kommet på plass og at gruppene er aktive og i produksjon. Selv om det ved utgangen av 2019 er noen udisponerte midler, så er dette betydelig lavere enn overføringen av udisponerte midler fra 2018. Underforbruket på bevilgningen fra HOD skyldes i hovedsak at en oppsigelse tidlig i 2019 hvor ny resurs ikke forventes å være på plass før tidlig i 2020. Ut over dette ser vi at aktiviteten finansiert fra JD i 2019 var i henhold til bevilgning og driftsmidler. Oversikten for 2019 viser at CCIS økonomisk nå er inne i en stabil driftsfase. Udisponerte midler fra 2019 er budsjettert inn i aktiviteten for 2020.

Finansieringskilde	Sum	HOD	JD	NTNU	PARTNER
Inntekter					
Øverføring udisponerte midler 2018	3 773 320	1 996 597	1 776 723		
Bevilgning statsbudsjettet – JD	5 000 000		5 000 000		
Bevilgning statsbudsjettet – HOD	2 100 000	2 100 000			
Bidrag partnere	8 072 616				8 072 616
Bidrag NTNU	5 671 687			5 671 687	
Totale inntekter 2019	**24 617 623**	**4 096 597**	**6 776 723**	**5 671 687**	**8 072 616**
Utgifter					
Administrasjon	2 045 578			1 363 768	681 810
Lønn	0				
Reiser	44 357	6 654	37 703		
Utstyr	0				
Utvikling	0				
Partner- og avtaleoppfølging	0				
Forskning, utdanning og formidling	11 698 725			4 307 919	7 390 806
Lønn	4 998 341	1 696 113	3 302 228		
Reiser	948 738	160 362	788 376		
Utstyr	378 974	41 213	337 761		
FoU aktiviteter	850 899	255 270	595 629		
Publikasjoner, trykking, annonser	189 404		189 404		
Møter og arrangementer	286 911	23 041	263 870		
Formidling og markedsføring	320 405	75 065	245 340		
Utvikling	870 572	261 171	609 401		
Totale utgifter 2019	**22 632 904**	**2 518 889**	**6 369 712**	**5 671 687**	**8 072 616**
Udisponerte midler for 2019	**1 984 719**	**1 577 708**	**407 011**	**0**	**0**

NTNU CCIS
Center for Cyber and Information Security

3 Faggrupper

I det følgende presenteres faggruppenes årsrapporter.

3.1 Norwegian Biometrics Laboratory (NBL)

3.1.1 Group webpage

https://www.ntnu.edu/nbl

3.1.2 Group leadership

Group leader: Professor Christoph Busch

3.1.3 Members of the group

Core permanent IIK academic staff

- Christoph Busch
- Patrick Bours
- Raghavendra Ramachandra,

Affiliated IIK staff

- Guoqiang Li
- Loic Bergeron

ERCIM PostDocs

- Kishorkumar Upla
- Mudasir Ahmad Wani
- Nancy Agrawal

Further affiliated IIK staff

- Bian Yang
- Katrin Franke

Adjunct staff

- Lars Erik Pedersen

Non-IIK staff with affiliation to NBL

- Kiran Raja (NTNU-IDI)
- Mohammad Derawi (NTNU-IES)
- Marta Gomez-Barrero (HDA)
- Patrick Schuch (Nect)
- Pankaj Wasnik (Rakuten Institute of Technology)
- Martin Stokkenes (mobai)

Temporary staff (PhD-students)

- Parisa Rezaee Borj
- Pawel Drozdowski
- Ali Khodabakhsh
- Alexander Nikolaus Kirfel
- Hareesh Mandalapu, Edlira Martiri
- Tobias Scheer
- Jag Mohan Singh

- Sushma Venkatesh

3.1.4 Collaboration partners

National: NBF, Mobai, Politiet, NID, Telenor, NR, Zwipe,

European: EAB, EU-JRC, FRONTEX, BSI, University of Twente, Idiap, Idemia, AGB, ATHENE, Hochschule Darmstadt, Fraunhofer IGD, University Bologna, UAM, KUL, EUROCOM, GenKey, secunet, Cognitec, Dermalog, Neurotechnology

Intercontinental: NIST, HID, Hitachi, Fujitsu, NEC

3.1.5 Research activities

Ongoing

- SOTAMD: State of the Art Morphing Detection
  https://www.christoph-busch.de/projects-mad.html
  Sponsor: EU-ISF Borders and Visa
- SWAN: Secure Access Control over Wide Area Network
  https://www.ntnu.edu/iik/swan/
  Sponsor: NRC-IKTPLUSS
- BATL: Biometric Authentication with a Timeless Learner
  https://www.christoph-busch.de/projects-batl.html
  Sponsor: IARPA-ODIN
- Awesome Possum
  https://www.nr.no/nb/projects/awesome-possum
  Sponsor: NRC-InnovationProject

Submitted proposals

- iMARS: image Manipulation Attack Resolving Solutions (accepted 2020)
  Sponsor: EU H2020
- UFAPAROPP: Unconstrained Facial Presentation Attack and Robust Privacy (under evaluation)
  Sponsor: EU H2020
- VasCoDe: Vascular Biometrics Competence Development (under evaluation)
  Sponsor: EU H2020 – ITN
- RETRAK: REliable mulTi-media SeRvices for trustworthy social networKs (rejected)
  Sponsor: RCN

Publications

See: https://www.ntnu.edu/nbl#/view/publications for full list of publications. Some selected publications from 2019:

1. K. Raja, R. Raghavendra, M. Stokkenes, C. Busch: "Biometric Template Protection on Smartphones Using the Manifold-Structure Preserving Feature Representation ", in Handbook of Selfie Biometrics, Springer, pp 299-312, (2019)
2. K. Raja, R. Raghavendra, C. Busch: "Morton Filters for Iris Template Protection - An Incremental and Superior Approach Over Bloom Filters", in Proceedings of the 10th International Conference on Biometrics: Theory, Applications and Systems (BTAS 2019), Tampa, US, September 23-26, (2019)
3. P. Drozdowski, C. Rathgeb, C. Busch: "Computational Workload in Biometric Identification Systems: An Overview", in IET Biometrics, (2019)
4. C. Galdi, V. Chiesa, C. Busch, P. Correia, J.-L. Dugelay, C. Guillemot: "Light Fields for Face Analysis", in IEEE Sensor journal, (2019)
5. K. Raja, R. Raghavendra, E. Auksorius, C. Boccara, C. Busch: "Robust Verification With Subsurface Fingerprint Using Full Field Optical Coherence Tomography", in Proceedings of IEEE Computer Society Workshop on Biometrics (CVPRW 2019), Long Beach, U.S., June 16-17, (2019)
6. A. Khodabakhsh, R. Raghavendra, C. Busch: "Subjective Evaluation of Media Consumer Vulnerability to Fake Audiovisual Content", in Proceedings of the 11th International Conference onQuality of Multimedia Experience (QoMEX 2019), Berlin, DE, June 5-7, (2019)

7. P. Drozdowski, C. Rathgeb, C. Busch: "Turning a Vulnerability into an Asset: Accelerating Facial Identification with Morphing", in Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP 2019), Brighton, U.K., May 12-17, (2019)
8. C. Busch: "Standards for Presentation Attack Detection", in Handbook of Biometric Anti-Spoofing – Presentation Attack Detection, second Edition, Springer, pp 503-214, (2019)
9. K. Raja, R. Raghavendra, C. Busch: "Towards Reducing the Error Rates in Template Protection for Iris Recognition Using Custom Cuckoo Filters", in Proceedings of the International Conference on Identity, Security and Behavior Analysis (ISBA), Hyderabad, India, January 22-24, (2019)
10. P. Bours, H. Kulsrud: "Detection of Cyber Grooming in Online Conversations", in Proceedings of the IEEE Workshop on Information Forensics and Security (WIFS), Delft, the Netherlands, December 9-12, (2019)
11. G. Li, P.R. Borj, L. Bergeron, P. Bours: "Exploring Keystroke Dynamics and Stylometry Features for Gender Prediction on Chat Data", in Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, May 20-24, (2019).

Awards

- Best paper award at ISBA-2019
- Best paper award at IWBF-2019
- EAB industry award 2019

3.1.6 Innovation

The NBL members participate in numerous projects and publishes about the achieved findings at various conferences and in journals.

3.1.7 Education

Overview of graduated PhD candidates

- Pankaj Wasnik: "Robust Biometrics on Smartphones – Using Quality Assessment, Presentation Attack Detection, and Biometric Fusion" on May 8th of 2019.
- Patrick Schuch: "Deep Learning for Fingerprint Recognition Systems" on October 16th of 2019

Overview of supervised MSc and BSc theses

- Thor Aleksander Buan: "In depth analysis of Long-Short-Term-Memory Neural Networks with the purpose of detecting cyberbullying", Msc, 2019
- Carly Grace Allen: "The Usability of Biometric Authentication in Mobile Phones", MSc, 2019
- Halvor Kulsrud: "Detection of cyber grooming during an online conversation", MSc, 2019
- Eirik Holbæk: "Using Author Profiling to Determine the Age Group of an Author", MSc, 2019
- Magnus Rolfsøn: "An evaluation of authentication methods for solutions that require a high degree of both security and user-friendliness on mobile phones", MSc, 2019
- Jørgen Bendiksen: "Automated detection of perpetrators in grooming conversations in Norwegian", MSc, 2019

Lifelong learning activities

- Norsk Biometri Forum
- EAB autum training event (in preparation)

List of courses:

- MSc courses
  - IMT4113 Introduction to Cyber and Information Security Technology (pb)
  - IMT4126 Biometrics (pb, cb)
  - IMT 4206 Research project planning (rr)
  - IMT 4881/2 Specialization course (rr)
  - IMT 4215 Specialization course (rr)
- PhD courses
  - IMT6071 Biometrics (cb)
  - IMT6121 Behavioural Biometrics (pb)

3.1.8 Dissemination activities

- SC37 WG3 conference, Iquique, CL, January 2019
- NBLAW-2019, Gjøvik, NO, March, 2019
- NBF, Oslo, May, 2019
- SC37 WG3 conference, Darmstadt, DE, July 2019
- EAB-RPC conference, Darmstadt, DE, September 2019
- BIOSIG conference, Darmstadt, DE, September 2019
- FRONTEX conference, Warshaw, PL, October 2019
- NBF, Oslo, NO, October 2019
- SecurityPrinters conference, Copenhagen, DK, October 2019

3.1.9 Updated plans and roadmaps for the following year

Rationale, strategy, and goal

Norwegian Biometrics Laboratory is more than just a physical room at the campus. It is a discussion forum to brainstorm, to generate new ideas and projects and to present intermediate results. Thus it is an essential part of the Department of Information Security and Communication at the Norwegian University of Science and Technology (NTNU) and represents an active focus point with many international research projects.

Further, it is the intention of NBL to increase the awareness of biometrics in Norway via the Norwegian Biometric Forum and its potential involvement in the Norwegian legislation and to contribute to the international standardization in the field.

Furthermore, we focus on privacy enhancing technologies, such as biometric template protection and integration in physical and logical access control. Our group serves also as independent testing institution for biometric performance evaluations based on our in-house biometric databases. The Biometrics lab is an active member in the European Association for Biometrics and co-organizer of the international BIOSIG conference as well as many other conferences and workshops.

Important dates of upcoming events

- NBLAW-2020: 2020-03-04
- NBL-Retreat: 2020-03-05 to 2020-03-06
- NBL-IWSBB: 2020-03-06 to 2020-03-08
- NBF: 2020-05-07
- SC37: 2020-07-13 to 2020-07-17
- EAB-RPC: 2020-09-14 to 2020-09-16
- BIOSIG: 2020-09-16 to 2020-09-18
- NIST-IFPC: 2020-10-27 to 2020-10-29

3.2 Critical Infrastructure Security and Resilience

3.2.1 Samarbeid og samarbeidspartnere

Collaboration with partners listed in section "Collaborating partners" below towards project work; proposal writing and submission; and joint publications.

3.2.2 Forskning

Ongoing research activities

- H2020 Project GHOST (https://www.ghost-iot.eu/)
  The main objective set forth by GHOST is to develop a user-friendly application to improve security and privacy in a Digital Home connected to the Internet of Things (IoT), using the most advanced technologies available for this purpose. GHOST envisions a transparent cybersecurity environment for all Europeans living in a connected world: with minimal effort consumers will become aware and understand the cybersecurity risks (threats and vulnerabilities), and will take informative decisions affecting their cyber-physical security and privacy. The work of the CISaR group focuses on three aspects of the project, namely on low level network analysis by means of deep packet inspection; dynamic risk assessment; and the development of a complete distributed communication and

decision making framework by means of blockchain technology. Prof. Katsikas, Dr Spathoulas and Dr Anagnostopoulos worked in the project throughout 2019.

- H2020 Project DELTA (https://www.delta-h2020.eu/)
  DELTA proposes a Demand-Response (DR) management platform that distributes parts of the Aggregator's intelligence into a novel architecture based on Virtual Power Plant (VPP) principles. It establishes a more easily manageable and computationally efficient DR solution and delivers scalability and adaptiveness into the Aggregator's DR toolkits. DELTA also delivers a fully autonomous architectural design which enables end-users to escape the hassle of responding to complex market signals. Two pilots in the UK and Cyprus are being used to prove the DELTA concept. The pilots cover a wide variety of residential/tertiary loads (>11GWh), RES generation (>14GWh) & energy storage systems (>9MWh) (average annual measurements). The CISaR group leads the workpackage on "Secure Data Handling and Exchange in future DR Ecosystems". Our work focuses on two aspects of the project, namely on the security of the DELTA data exchange, including by means of blockchain technology and smart contracts; and the cyber and physical security of the DELTA DR framework. Prof. Katsikas, Dr Spathoulas and Dr Baiocco worked in the project throughout 2019.
- H2020 Project CyberSec4Europe (https://cybersec4europe.eu/)
  CyberSec4Europe is a pilot for a future European Cybersecurity Competence Network – a new digital ecosystem built of a network of centres of cybersecurity expertise, with a central hub. CyberSec4Europe designs, tests and demonstrates potential governance structures for a future European Cybersecurity Competence Network using best practice examples derived from concepts like CERN as well the expertise and experience of partners. The work carried out by the CyberSec4Europe contains four interconnected pillars: Governance, design and pilot (WP2); From research and innovation to industry (WP3-WP4-WP5); Education, training and standardisation (WP6-WP7-WP8); Communication and community building. The work of CISaR focuses on cybersecurity education and security awareness; open tools and infrastructure for certification and validation; dissemination, spreading of competence, and policy recommendations. Prof. Katsikas and Dr Gkioulos worked in the project throughout 2019. Contributions were also made by Dr Rooney, and PhD candidates G. Kavallieratos and A. Amro.
- H2020 Project SDN-microSENSE (https://www.sdnmicrosense.eu/)
  SDN-microSENSE aims at providing and demonstrating a secure, resilient to cyber-attacks, privacy-enabled, and protected against data breaches solution for decentralised Electrical Power and Energy Systems (EPES). Six Use Cases (UC) are being used to demonstrate the results of the project: UC1 - Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES (Norway); Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control (Bulgaria); Large-scale Islanding Scenario Using Real-life Infrastructure (Greece); EPES Cyber-defence against Coordinated Attacks (Spain); Distribution Grid Restoration in Real-world PM Microgrids (Greece); Realising Private and Efficient Energy Trading among PV Prosumers (Sweden). The work of CISaR focuses on UC1; extraction of user, security and privacy requirements, the corresponding architectural specification of the target system with focus on the SDNbased microgrid, and its holistic vulnerability and threat assessment; and the analysis and specification of novel SDN-based IDS systems. Prof. Katsikas, Prof. Wolthusen, and Dr Gkioulos worked in the project throughout 2019. Contributions were also made by Dr Weldehawaryat. Dr Nehra joined the project team in November 2019.
- H2020 Project LOCARD (https://locard.eu/)
- LOCARD aspires to automate the collection and documentation of every digital form of evidence in every format and medium. LOCARD proposes a comprehensive framework to make far-flung, variously captured and disparate data resources into court-ready, forensically sound evidence that complies with all the special requirements demanded for the forensic capture, preservation and presentment of these data, by allowing the storage of digital evidence metadata in a blockchain. The work of CISaR focuses on novel methods on mobile forensics, particularly for Android devices, streaming services, apps and devices, cloud forensics; identity management and blockchain technologies; and Chain of Custody / Continuity of Evidence management techniques. Prof. Katsikas and Dr Spathoulas worked in the project throughout 2019.
- H2020 Project +CityxChange (https://cityxchange.eu/)
  +CityxChange aims at enabling the co-creation of the future we want to live in by developing a framework and supporting tools to enable a common energy market supported by a connected community. This leads to recommendations for new policy intervention, market (de)regulation and business models that deliver positive energy communities integrating e-Mobility as a Service (eMaaS). Two *Lighthouse Cities*, Trondheim Kommune and Limerick City and County Council are developing feasible and realistic demonstration projects in climate-friendly and sustainable urban environments.

- IKTPluss Project CPSEC
  CPSEC (Cyber-Physical Security in Energy Infrastructure of Smart Cities) aims to develop a comprehensive and systemic approach combining cyber and physical security solutions to protect energy installations from cyber, physical and combined cyber-physical threats. The main technical output of the project will be the Integrated Security, Safety and Site Management platform which will cover a wide variety of concepts, including, systemic risk management, prevention by design, monitoring and detection, response and mitigation, and information sharing. The CISaR group leads the project. Our work focuses on the requirements and the definition of the system architecture; systemic Risk Management; and monitoring and detection. Prof. Katsikas and Dr Pandey worked in the project throughout 2019. in the project throughout 2019. PhD candidate A. Akbarzadeh joined the project team in May 2019. Dr Pandey Dr Pandey was awarded a grant by the Research Council of Norway to move to India for 6 months (starting in October 2019) to work on the project.
- IKTPluss Project Cybwin (https://ife.no/en/project/cybwin-cybersecurity-platform-for-assessment-and-training-for-critical-infrastructures-legacy-to-digital-twin/)
  CybWin (Cybersecurity Platform for Assessment and Training for Critical Infrastructures: Legacy to Digital Twin) develops knowledge of applicable digital vulnerabilities and threats to the Norwegian Critical Infrastructure (CI). CybWin is a cybersecurity platform with physical, replicated and simulated components of real-world CIs, empowered with tools for RAMS (reliability, availability, maintainability, safety) assessment, vulnerability assessment, attack simulation, incident prediction and response. CISaR leads the "Dissemination and networking" workpackage of the project. Our work focuses on Industrial Control Systems (ICS) architecture and interdependencies; ICS threat landscape for Norwegian CI; ICS RAMS- and Cybersecurity- risk models; simulations for RAMS- and cybersecurity- incident prediction and response; human performance evaluation during cybersecurity incident response; and cybersecurity risk visualisation for operational safety. Prof. Katsikas and Dr Gkioulos worked in the project throughout 2019. PhD candidate Nabin Chowdhury joined the project team in November 2019.
- MAROFF Project Marcy
  The goal of Marcy (Maritime Cyber Resilience) is to investigate and develop means for increasing the cyber resilience of maritime digitized systems and operations. The project will address both human and technological means. Methodologically, the project will employ demonstrators and simulation, utilizing operational installations of maritime systems, as well as the operational vessels, bridge simulators and cyber ranges. CISaR leads the "Resilient Digital Maritime Systems" workpackage. Our work focuses on Interconnections and Interdependencies; Assessment of cyber risk; and Mitigation and transfer of cyber risk. The start of the research work has been postponed due to delays in hiring PhD candidates. Prof. Katsikas and Dr Gkioulos did preparatory work for the project throughout 2019.
- IKTPluss Project SAINTGrid
  SAINTGrid studies the security of HVDC integrated transmission and distribution networks.
- NFR Project eX3 (https://www.ex3.simula.no/)
  eX3 (Experimental Infrastructure for Exploration of Exascale Computing) aims to allow for exploration and research on the computational backbone infrastructures critical to tomorrow's society, infrastructures that need to be inherently secure and reliable. Assoc. Prof. Gran acts as the Scientific Leader of Communication Technologies in eX3.
- Norwegian Cyber Range (https://www.ntnu.no/ncr)
  The Norwegian Cyber Range is an arena for cyber security testing and training. Dr Gkioulos worked in the project throughout 2019.
- Veikart med prosedyre for sikkerhet når industrien digitaliserer
  The study will deliver a set of guidelines and recommendations on best practices for the secure adoption of the aforementioned technologies by Norwegian industries that have adopted or plan to adopt, distinguishing and focusing on solutions suitable for large groups but also small and medium-sized enterprises. These will form the foundation for the design of a training course aiming at key stakeholders of the process of adoption of Industry 4.0. In addition, the study will aim to support discussions at the policy making and regulatory levels.
- PhD research project "Cyber Power Praxis: a study of ways to improve understanding and governance in the cyber domain"
  The aim of this PhD research project is to answer the question "How to improve performance among novice cyber operators and better prepare them for governing the effects of cyberpower?" PhD candidate Benjamin James Knox

worked on the project throughout 2019, under the supervision of Prof. Katsikas (main supervisor), Prof. Kirsi Helkala, and Prof. Stefan Sütterlin.

- PhD research project "Security of the cyber-enabled ship"
  The aim of this PhD research project is to contribute to improving the security and safety of Cyber-Enabled Ships (C-ES) by delivering security requirements and a security architecture for the C-ES, through identifying, assessing and managing the attendant combined cyber security and safety risks, and by identifying and modelling threats and attacks against the C-Es to analyze their impact. PhD candidate Georgios Kavallieratos worked on the project throughout 2019, under the supervision of Prof. Katsikas (main supervisor), Prof. Slobodan Petrovic, Prof. Edmund Førland Brekke, and Prof. Hao Wang. Dr Gkioulos has been assisting with the candidate's supervision.
- PhD research project "Communication and Cybersecurity for autonomous passenger ferry"
  The city of Trondheim is considering the application of an autonomous ferry (Autoferry) to carry passengers across the city canal as an alternative to a higher cost bridge. Such a ferry, being constructed of new all-electric components, carrying passengers without a pilot on board, is expected to require unique communication requirements and raise new types of cybersecurity risks. The aim of this PhD research project is to define a reliable and secure communication architecture for the Autoferry system, in addition to developing an Integrated Security, Safety and Ship Management System (IS3MS) to ensure the security and safety of the ferry and of its passengers. PhD candidate Ahmed Walid Amro worked on the project throughout 2019, under the supervision of Prof. Katsikas (main supervisor), Prof. Nadezda Sokolova, and Prof. Kimmo Kansanen. Dr Gkioulos has been assisting with the candidate's supervision.
- PhD research project "Cyber-physical security of power plants within the smart grid"
  The overall objective of this PhD research project is to contribute to improving the security of the power plant systems within the smart grid, seen as vital Cyber Physical Systems, by proposing a risk management framework, and by delivering security requirements through identifying, assessing and managing security risks of the system when considering its combined cyber-physical features. PhD candidate Aida Akbarzadeh started working on the project in August 2019, under the supervision of Prof. Katsikas (main supervisor), Prof. Katina Kralevska, and Dr Pandey.
- PhD research project "Cyber-security training for critical infrastructure protection"
  This PhD research project aims to contribute to the current landscape of critical infrastructure protection measures. An evaluation of the key features needed for successful critical infrastructure cyber-security training will be conducted. The data collected will be used to develop a new training framework targeting
  Critical Infrasructure personnel and cyber-security experts. The goal of the framework is to raise human preparedness for incident prevention and incident handling. The framework will be later validated through case studies run in simulated digital environments, which will be replicated after real-world Critical Infrastructure. PhD candidate Nabin Chowdhury started working on the project in November 2019, under the supervision of Prof. Katsikas (main supervisor) and Dr Gkioulos.

Proposals submitted

1. ANGEL - Securing Europe's offshore critical infrastructure. Proposal submitted to the H2020-SU-INFRA-2018-2019-2020 call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Vasileios Gkioulos, Marios Anagnostopoulos, and Georgios Spathoulas.
2. BAHADUR - Trust Enabling Certification Framework for Digital Assets from Manufacturer to Consumer. Proposal submitted to the H2020-SU-ICT-2018-2020 call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Vasileios Gkioulos, Marios Anagnostopoulos, and Georgios Spathoulas.
3. COBWEB - Citizen security and privacy enabler for World-wide safe browsing. Proposal submitted to the H2020-SU-DS-2018-2019-2020 call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Vasileios Gkioulos, and Georgios Spathoulas.
4. DAGGER - Big DatA to fiGht aGainst cybEr crime and terrorism. Proposal submitted to the H2020-SU-SEC-2018-2019-2020 call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Katrin Franke, Vasileios Gkioulos, Marios Anagnostopoulos, and Georgios Spathoulas.
5. SCANNER - Security and privaCy AuditiNg staNdardization and cERtification. Proposal submitted to the H2020-SU-ICT-2018-2020 call. Participants from CISaR: Sokratis Katsikas, Basel Katt, Vasileios Gkioulos, Marios Anagnostopoulos, and Georgios Spathoulas.

6. SecurTEN - Securing Cyber Physical System of Urban Nodes in Trans- European Transport Network. Proposal submitted to the H2020-SU-INFRA-2018-2019-2020 call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Vasileios Gkioulos, Marios Anagnostopoulos, and Georgios Spathoulas.
7. SEC-PREP - Cyber-Security Training Platform for the Digital Natives. Proposal submitted to the Latvia-Norway EEA call for proposals. Status: Not retained. Participants from CISaR: Sokratis Katsikas and Vasileios Gkioulos.
8. CYPEDIA - CYber training Platform for security EDucatIon and Awareness. Proposal submitted to EEA and Norway Grants. Status: Pending. Participants from CISaR: Sokratis Katsikas and Vasileios Gkioulos.
9. PATREO - Process Automation Toolkit: the new Real Estate Ownership paradigm. Proposal submitted to the Greece-Norway EEA Call for Proposals. Status: Pending. Participants from CISaR: Sokratis Katsikas and Pankaj Pandey.
10. ABSOLUTE - Enhancing Societal Security Awareness by Promoting a Security Culture Through Education. Proposal submitted to the Research Council of Norway – FINNUT call. Status: Pending. Participants from CISaR: Sokratis Katsikas and Vasileios Gkioulos
11. ACDICOM - Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations. Proposal submitted to the Research Council of Norway – SAMRISK call. Status: Not retained. Participants from CISaR: Sokratis Katsikas.
12. Digitalization of short-term resource allocation in power markets. Proposal submitted to the NFR - KSPKOMPETANSE19 call. Status: Pending. Participants from CISaR: Sokratis Katsikas and Vasileios Gkioulos.
13. NORCICS - Norwegian Center for Cybersecurity In Critical Sectors. Proposal submitted to the Research Council of Norway – SFI call. Status: Pending. Participants from CISaR: Sokratis Katsikas, Katrin Franke, and Stephen Wolthusen.
14. Cyber-Physical Security and Risk Management in Critical Infrastructure. Proposal submitted to the MHRD Scheme on Global Initiative on Academic Network (GIAN) of the Government of India call. Status: Pending. Participants from CISaR: Sokratis Katsikas and Pankaj Pandey.

Awards

- Sokratis Katsikas was awarded a Doctorate Honoris Causa from the Department of Production and Management Engineering, Democritus University of Thrace, Greece in May 2019.

Selected publications

1. Stefanos Gritzalis, Edgar R. Weippl, **Sokratis K. Katsikas**, Gabriele Anderst-Kotsis, A Min Tjoa, Ismail Khalil (Eds.), Trust, Privacy and Security in Digital Business, Proceedings of the 16th International Conference, TrustBus 2019, Linz, Austria, August 26–29, 2019.
2. **Sokratis Katsikas** and Vasilios Zorkadis (Eds.), E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age, Communications in Computer and Information Science, Springer, 2019
3. Teemu J. Tokola, Thomas Schaberreiter, Gerald Quirchmayr, Ludwig Englbrecht, Günther Pernul, **Sokratis K. Katsikas**, Bart Preneel, Qiang Tang, "A Collaborative Cybersecurity Education Program", in Ismini Vasileiou and Steven Furnell (Eds.), Cybersecurity Education for Awareness and Compliance, IGI Global, 2019.
4. **Georgios Spathoulas** and **Sokratis Katsikas**, "Towards a secure Industrial Internet of Things", in Cristina Alcaraz (Ed.), Security and Privacy Trends in the Industrial Internet of Things, Springer, 2019.
5. V. Anastopoulos and **S. Katsikas**, "A Methodology for the Dynamic Design of Adaptive Log Management Infrastructures", EAI Transactions on Security and Safety, Volume 6, Issue 19, e2, 2019. DOI: 10.4108/eai.25-1-2019.159347.
6. **G. Kavallieratos, N. Chowdhury, S. Katsikas, V. Gkioulos, S. Wolth**usen, "Threat Analysis for Smart Homes", Future Internet, 11(10), 207; https://doi.org/10.3390/fi11100207, 2019.
7. **G. Kavallieratos, S.K. Katsikas, V. Gkioulos**, "Cyber-attacks against the autonomous ship", in Proceedings, 4th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2018), Barcelona, Spain, pp. 20-36, doi: https://doi.org/10.1007/978-3-030-12786-2_2, 2019.
8. **G. Kavallieratos, V. Gkioulos, S.K. Katsikas**, "Threat analysis in dynamic environments: The case of the smart home", in Proceedings, 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, pp. 234-240, doi: 10.1109/DCOSS.2019.00060, 2019.
9. **G. Kavallieratos, S.K. Katsikas, V. Gkioulos**, "Towards a cyber-physical range", in Proceedings, 5th ACM Cyber-Physical System Security Workshop (CPSS 2019), Auckland, New Zealand, pp. 25-34, doi: 10.1145/3327961.3329532, 2019.

10. **P. Pandey**, A. Collen, N. A. Nijdam, **M. Anagnostopoulos, S. Katsikas**, and D. Konstantas, "Towards Automated Threat-based Risk Assessment for Cyber Security in Smarthomes", in Proceedings, European Conference on Cyber Warfare and Security – ECCWS, Coimbra, Portugal, pp. 839-844, 2019.
11. V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester and **S. Katsikas**, "A forensics-by-design management framework for medical devices based on blockchain", in Proceedings 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, pp. 35-40. doi: 10.1109/SERVICES.2019.00021, 2019.
12. **G. Spathoulas**, S. Evangelatos, **M. Anagnostopoulos**, G. Mema, **S. Katsikas**, "Detection of abnormal behavior in smart home environments", in Proceedings 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, pp. 1-6, doi: 10.1109/SEEDA-CECNSM.2019.8908352.
13. Giacomo Assenza, Valerio Cozzani, Francesco Flammini, Nadezhda Gotcheva, Tommy Gustafsson, Anders Hansson, Jouko Heikkila, Matteo Iaiani, **Sokratis Katsikas**, Minna Nissilä, Gabriele Oliva, Eleni Richter, Maaike Roelofs, Mehdi Saman Azari, Roberto Setola, Wouter Stejin, Alessandro Tugnoli, Dolf Vanderbeek, Lars Westerdahl, Marja Ylönen, and Heather Young, "White Paper on Industry Experiences in Critical Information Infrastructure Security: A Special Session at CRITIS 2019, in Proceedings 14th International Conference, CRITIS 2019, Linköping, Sweden, September 23–25, 2019, pp. 197-207.

3.2.3 Collaborating partners

- **GHOST:** TELEVES SA (ES), UNIVERSITE DE GENEVE (CH), ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (GR), IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE (UK), EXUS SOFTWARE LTD (UK), TECHNISCHE UNIVERSITAT DARMSTADT (DE), KALOS AS (NO), CRUZ ROJA ESPANOLA FUNDACION (ES), Obrela Security Industries - Information Security Services S.A. (GR).
- **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)
- **CyberSec4Europe:** Goethe-Universität Frankfurt (DE), TU Delft (NL), University of Murcia (ES), FORTH (GR), NEC Laboratories Europe GmbH (DE), University of Trento (IT), Masaryk University Brno (CZ), Cybernetica (EE), TDL (BE), Conceptivity (CH), Austrian Institute of Technology (AT), ATOS Spain (ES), BBVA - Banco Bilbao Argentaria S.A. (ES), Université Paul Sabatier (FR), Dawex (FR), IBM Zurich (CH), Intesa Sanpaolo Group Services (IT), JAMK University of Applied Sciences (FI), Karlstad University (SE), LERO (IE), POLITO (IT), Siemens AG (DE), SINTEF – Stiftelsen (NO), TU Denmark (DK), University of Cyprus (CY), University of Luxembourg (LU), University of Malaga (SE), University of Maribor (SI), University of Pireaus (GR), University Porto - C3P (PT), VTT Technical Research Centre of Finland (FI), VaF (SK).
- **SDN-microSENSE:** AYESA ADVANCED TECHNOLOGIES SA (ES); PANEPISTIMIO DYTIKIS MAKEDONIAS (EL); ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (EL); PREDUZECE ZA TELEKOMUNIKACIJSKE USLUGE REALAIZ DOO BEOGRAD (SAVSKI VENAC) (RS); ATOS SPAIN SA (ES); SCHNEIDER ELECTRIC FRANCE SAS (FR); PUBLIC POWER CORPORATION S.A. (EL); FUNDACION TECNALIA RESEARCH & INNOVATION (ES); DIMOS AVDIRON (EL); INNOVATIVE ENERGY AND INFORMATION TECHNOLOGIES LTD (BG); ELEKTROENERGIEN SISTEMEN OPERATOR EAD (BG); CEZ DISTRIBUTION BULGARIA AD (BG); UBITECH LIMITED (CY); CYBERLENS LTD (UK); SIDROCO HOLDINGS LIMITED (CY); INFINITY LIMITED (UK); EIGHT BELLS LTD (CY); INCITES CONSULTING SARL (LU); Energynautics GmbH (DE); SIAXAMPANIS E.E. (EL); GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER (DE); RAVNA HYDRO Ltd. (BG); FUNDACIO INSTITUT DE RECERCA DE L'ENERGIA DE CATALUNYA (ES); ESTABANELL Y PAHISA ENERGIA SA (ES); CHECKWATT AB (SE); INDEPENDENT POWER TRANSMISSION OPERATOR SA (EL); SINTEF ENERGI AS (NO); D I L DIEL Ltd. (BG); OPTIMIZACION ORIENTADA A LA SOSTENIBILIDAD SL (ES); GEIE ERCIM (FR).
- **LOCARD:** ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS (EL), GUARINO ALESSANDRO (IT), FUNDACION APWG, EUROPEAN UNION FOUNDATION (ES), MOTIVIAN EOOD (BG), IMC DIACHIRISI PLIROFORION KAI EPIKINONION ANONYMOS ETAIRIA (EL), UNIVERSITA DEGLI STUDI DI PADOVA (IT), TELEFONICA INVESTIGACION Y DESARROLLO SA (ES), EUROPEAN ELECTRONIC MESSAGING ASSOCIATION AISBL (BE), NEUROSOFT CYPRUS LIMITED (CY), VRIJE UNIVERSITEIT BRUSSEL (BE), Vlaamse ICT Organisatie (BE), Infotrend Innovations Co Ltd (CY), ACCENTURE SAS (FR), UNIVERSITA TA MALTA (MT), KENTRO MELETON ASFALEIAS (EL), TECHNISCHE UNIVERSITAT BERLIN (DE), HELLENIC POLICE (EL), Inspectoratul General al Politiei Romane (RO).

- **+CityxChange:** University of Limerick; ABB AS; Arup; Avis Budget Group, Inc.; Collaborativa.eu; Energy Agency of Plovdiv; Electricity Supply Board; ESB Networks DAC; FourC AS; Future Analytics Consulting Lth.; GKinetic Energy Ltd; IES; IOTA Foundation; ISOCARP Institute; MPOWER; NHP Eiendom AS; Officinæ Verdi Group; Powel; R2M Solutions srl.; R. Kjeldsberg AS; Space Engagers; Statkraft Varme; TrønderEnergi
- **CPSEC:** Institute for Energy Technology – IFE (NO), Indian Institute of Information Technology (IIITA) Allahabad (IN), Indian Institute of Technology (IITK) Kanpur (IN).
- **CybWin:** IFE (NO), SECURE-NOK AS (NO), Korean Advanced Institute of Science and Tec KAIST (KO), EUROCONTROL (EU), AVINOR FLYSIKRING AS (NO), VTT Technical Research Centre of Finland Ltd (FI).
- **MarCy:** Norges Teknisk- Naturvitenskaplige Universitet Institutt for Havromsoperasjoner og byggteknikk, Norwegi an Defence University College, KONGSBERG DEFENCE & AEROSPACE AS, NORWEGIAN HULL CLUB - GJENSIDIG ASSURANSEFORENING, DNV GL GROUP AS, Chalmers University of Technology (SE), University of Plymouth (UK)
- **SAINTGrid:** SINTEF Energi
- **eX³:** Simula Research Laboratory (NO), University of Bergen (NO), University of Tromsø (NO), Uninett Sigma2 (NO), Fabriscale Technologies (NO), Numascale (NO), Dolphin Interconnect Solutions (NO), and Graphcore (through the acquisition of initial partner Skala Technologies (NO))
- **CYPEDIA:** FOGUS INNOVATIONS & SERVICES (GR), International Cyber Investigation Training Academy (BG), UBITECH LIMITED (CY), RED COMMUNICATIONS OE (GR), CERTSIGN S.A. (RO).
- **RELINK:** OsloMet (NO), SIFO (NO), Teknologirådet (NO), University of the Aegean (GR), University of Helsinki (FI), Rathenau Instituut (NL).

3.2.4 Invited talks

- Sokratis Katsikas, "Towards a secure Industrial Internet of Things: Trends and Challenges", 3rd IEEE Conference on Information and Communication Technology, Allahabad, India, December 6-8 2019.
- Sokratis Katsikas, "Towards a secure Industrial Internet of Things: Trends and Challenges", 12th International Symposium on Foundations & Practice of Security, Toulouse, France, 5-7 November 2019.
- Sokratis Katsikas, "Security and resilience of the crewless ship", 6th International Symposium for ICS & SCADA Cyber Security Research, Piraeus, Greece, 10-12 September 2019.
- Sokratis Katsikas, "Integrating OT with IT: Security challenges in industry 4.0", 5th International Conference - Big Data in Cyber Security, Napier University, Edinburgh, UK, 4-5 June 2019.

3.2.5 Utdanning

No PhD-students graduated in 2019.

Teaching activities

- Prof. Wolthusen has taught IMT 4125 (Network Security) in the spring 2019 term, covering core aspects of network infrastructure protocol security.
- Prof. Katsikas and Prof. Wolthusen taught IMT4203 (Critical Infrastructure Security and Resilience) in the fall 2019 term, covering core aspects of critical infrastructure and cyber physical systems security.

3.2.6 Viktige møter og aktiviteter

- Several EU project meetings
- NFR-funded project meetings
- Meetings with Norsk Industri
- NORCICS SFI proposal writing meetings with several partners

3.2.7 Medlemmer

Akademisk ansatte, fulltid

- Assoc. Prof. Ernst Gunnar Gran
- Assoc. Prof. Katina Kralevska

- Dr Marios Anagnostopoulos
- Dr Alessio Baiocco
- Dr Vasileios Gkioulos
- Dr Ming Chang Lee
- Dr Ajay Nehra
- Dr Pankaj Pandey
- Dr Georgios Spathoulas
- Dr Goitom Kathay Weldehawaryat

Akademisk ansatte, deltid:

- Prof. Bernhardt Hämmerli
- Prof. Sokratis K. Katsikas (Group coordinator)
- Prof. Stephen D. Wolthusen
- Assoc. Prof. Thomas Kemmerich

Tilknyttede akademiske ressurser:

PhD-kandidater:

- Aida Akbarzadeh
- Ahmed Walid Amro
- Nabin Chowdhury
- Håkon Gunleifsen
- Georgios Kavallieratos
- Benjamin James Knox

3.3 Cyber Defence

CCIS faggruppe Cyber Defence fokusere på forskning, trening, øving og kompetansebygging innenfor cyberoperasjoner.

3.3.1 Samarbeid og samarbeidspartnere

Forskningsgruppe Cyberforsvar samarbeider, internt, tett med forskningsgruppe Digital Forensics innen forskning, undervisning og formidling rundt etablering av en CCIS/NTNU malware lab på Gjøvik. Gruppen har tett samarbeid med Cyberforsvaret (bl.a. Cyber Ingeniørhøgskole (CIS), Center for Cybersikkerhet (CCS) og Cyber Våpenskolen (CVS) ved Jørstadmoen). Gruppen har utvidet samarbeidet med NSM, NorCERT, BDO CERT, Telenor Norge AS og Norton LifeLock med fokus på malwareanalyse gjennom gjesteforelesere, master oppgaver og workshop.

Innen etablering av en nasjonal kapasitet for cyber range er gruppen involvert i etableringen av Norwegian Cyber Range (NCR). Gruppen representere både CYFOR og NTNU i arbeidsgruppe "øvelser" som del av samarbeidsavtale om øving og trening i cyberdomenet. Dette er en avtale mellom CYFOR, Politidirektoratet, Telenor Norge AS og NTNU om felles utvikling og bruk av NCR.

Gruppen samarbeider med "Performance and Applied Cognitive Engineering Cyber Operations Research Group (PACECybORG)". Dette er en multidisiplinær gruppe av nasjonale og internasjonale forskere med focus på menneskelige faktorer av cyberforsvar.

3.3.2 Forskning

Gruppens fokuserer på å styrke organisasjoners motstandsdyktighet mot og håndtering av cyberangrep. 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 kombiner dyp teknisk analyse og kontekstinformasjon om hva som er kritiske verdier for individet, organisasjonen eller samfunnet.

Gruppen ser også på antatt, men lite forstått, kognitive aspekter, som økt toleranse mot usikkerhet eller håndtering av kognitiv belastning, som bidrar til hvordan vurderinger og beslutninger tas for å agere og bestemme ytelse i defensive cyberspace operasjoner. I cyber operasjoner er vi i mindre grad direkte konfrontert med utfallet av våre handlinger enn situasjoner med fysisk eller direkte konfrontasjon. Vår forventning om fremtidig utfall er mer abstrakt eller spesifisert

annerledes, mindre detaljert og typiske beslutningsprosesser gjennomføres under mange divergerende og konvergerende press. Effekten av digitalisering og beslutningstaking og bidrag fra "behavioral sciences" er i stor grad ikke undersøkt innen cyber domenet, men kan allikevel ha umiddelbar effekt på cybersikkerhet både nasjonalt og internasjonalt. I kjølvannet av "NATO Cyber Pledge" er det behov for økt innsats på forskning, trening og utdanning av personell på vei inn i eller som allerede opererer i cyberdomenet.

Gruppen deltar (veiledning av PhD student) i R&D project Ars Forensica 248094/O70) med midler fra forskningsrådets IKT-PLUSS program og bidrar i søknadsprosessen til EU H2020 call SU-ICT-03-2018.

Gruppens leder, Geir Olav Dyrkolbotn er grunnlegger av og ansvarlig (chair) for NTNU Malware Forum, en årlig 1 dags konferanse fokusert på malware. Etablert i 2017. Gjennomførte i 2019, for tredje gang, med 7 nasjonale og internasjonale foredragsholdere og ca. 90 deltagere. NTNU Malware Forum gjennomføres i samarbeid med NSM/NorCERT Sikkerhetsforum.

Gruppen bidrar med planlegging og gjennomføring av Norwegian Cyber Security Challenge (NCSC).

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 Øverlier 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 ac CCIS (JBD)

3.3.3 Utdanning

Gruppen har et spesielt fokus på Cyber Operation som del av erfaringsbasert master i informasjonssikkerhet., gjennom tre fag ved NTNU; cyber tactics, cyber intelligence og reverse engineering and malware analysis. Geir Olav Dyrkolbotn er fagansvarlig for fagene i tillegg til å underviser reverse engineering and malware analysis. Alle fagene har fått svært gode tilbakemelding og vil være viktige bidrag i forbindelse med øving og trening i Norwegian Cyber Range.

Norwegian Cyber Range (NCR)

Geir Olav Dyrkolbotn sitter i prosjektledelse og kjernegruppe for prosjektet: Norwegian Cyber Range (NCR) ved NTNU/CCIS. Dette er et 3 års prosjekt med ramme på 50 mil NOK til etablering av en nasjonal øvings og trening arena for cybersikkerhet/cyber operasjoner.

Faggruppe cyber defence ved Geir Olav Dyrkolbotn er initiativtaker til og deltager i arbeidsgruppen til Mulighetsstudie Cyber Range. Formålet med mulighetsstudien var å utrede og konkretisere mulig samarbeid mellom partene (CYFOR, Telenor AS, Politidirektoratet og NTNU) innenfor kapabilitetsbygging, nasjonalt operativt samarbeid og samhandling ved cyberhendelser i fred, krise og krig, og innenfor utdanning, prosedyrer, øving, trening, forskning og testing på IKT- og cyberoperasjoner. Mulighetsstudien er nå avsluttet og forankret hos alle parter. Som resultat er det underskrevet en samarbeidsavtale om øving og trening i cyber domenet.

3.3.4 Viktige møter og aktiviteter

- Malware Forum 2019
- Norwegian Cyber Security Challenge (NCSC)
- Samarbeidsmøter (BDO CERT, NSM/NorCERT, Telenor, CYFOR, Symantec Norge)
- Foredrag ved University of Florida (Nelms institute for the connected world)
- Gjennomført undervisning, veiledning og presentasjoner for NTNU, CYFOR og CIS/FHS
- Deltatt i planlegging og gjennomføring av Cyber Defence Exercise (CDX) ved CIS/FHS
- Deltatt i planlegging og gjennomføring av Telenors Øvelse Bukkesprang (Cyber Defence Øvelse)

3.3.5 Medlemmer

<u>Akademisk ansatte, fulltid:</u>

- Geir Olav Dyrkolbotn, førsteamanuensis

- Benjamin Knox, PhD-kandidat. Ben begynte i oktober 2019 som forsker cyber defence ved CYFOR. Forvanter å fullføre PHD utdanning først kvartal 2020

Tilknyttede akademiske ressurser:

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

PhD-kandidater:

- Sergii Banin

3.4 eHealth and Welfare Security

3.4.1 Samarbeid og samarbeidspartnere

- Direktoratet for e-helse on long-term research and innovation collaboration.
- Sykehuset Innlandet on long-term research and innovation collaboration.
- Centre for Connected Care at Oslo universitetssykehus HF on international research project application
- Total Innovation, Sykehuset Innlandet, JodaCare AS, and Buypass AS in innovation in biometric cryptosystems in local healthcare sector
- NTNU IDI for proposal on healthcare data application
- Oppland fylkeskommune for proposal on healthcare consumer technology platform
- Helsetjenestens Driftsorganisasjon for Nødnett HF on the activity on Nødnett 2.0
- Norsk Helsenett on potential contribution to the national project helseanalyseplattformen
- SFI Raufoss Manufacturing, NTNU industrial economy department, Zhejiang University, and Shandong University of Science and Technology for international collaboration research proposal on AI and machine agent for homecare management with its challenges in security

3.4.2 Forskning

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
  - Security practice survey preparation in hospital
  - Stress management during security incidents
- Dr. Vivek Agrawal
  - The role of an 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 among the healthcare professionals
  - Current challenges in the Norwegian Pre-Hospital services and investigation of the emerging technologies
- Prof. Einar Snekkenes
  - Investigation of the conflict between the information security compliance requirements and the operational requirements of the healthcare.
- Assoc. Prof. Hao Wang
  - Big data analytics for healthcare
  - Secure data analytics
- PhD researcher Prosper Yeng
  - Survey and discussion with inland hospital staffs on health security practice
  - Assistance in managing the IKTPLUSS project HealthDemocratization
- PhD researcher Muhammad A. Fauzi
  - Literature survey on stress and emotion management of healthcare workers anticipating cyber security threats

Proposals

1. PriMa (ITN- H2020-MSCA-ITN-2019) Privacy Matters. (Selected for funding) Bian Yang and Christoph Busch
2. IKTPLUSS International Collaboration Research 2019: Digital technologies for post-operative remote care and rehabilitation of thoracic and cardiac surgery patients (selected for funding). Bian Yang
3. IKTPLUSS International Collaboration Research 2019: Healthcare Agent System (not selected for funding). Bian Yang
4. RFF INNLANDET Research Project 2019: Healthcare Consumer Technology Platform (not selected for funding). Bian Yang
5. 8. RCN-Helsevel 2019. Acute Medical Decision Support System- AMDSS (Innovation Project for the Public Sector - HELSEVEL). (Under Evaluation) Vivek Agrawal and Bian Yang
6. 9. EU Horizon 2020 (H2020-SU-DS05-2018-2019): Predictive, Dynamic and Collaborative Security for Connected Healthcare4.0 Ecosystems. (Under Evaluation) Bian Yang

Projects

- Health Democratization (IKTPLUSS). Bian Yang and Einar Snekkenes
- PriMa (ITN- H2020-MSCA-ITN-2019) Privacy Matters. Bian Yang and Christoph Busch
- NTNU Digital Transformation PhD Project on Blockchain research. Bian Yang
- NTNU Digital Transformation PhD Project on Human Behaviour Analysis for healthcare stress management. Bian Yang and Christoph
- IKTPLUSS International Collaboration Research 2019: Digital technologies for post-operative remote care and rehabilitation of thoracic and cardiac surgery patients. Bian Yang
- ABCHealth (Innovation Norway): privacy-preserving identity management for healthcare services
- Remote video communication for ambulance use (funded by Sykehuset Innlandet). Bian Yang and Hao Wang
- Helse-EU Digital Patient project

Invited talks

- Contract-based identity management, NBL Annual Workshop, March, 2019, Gjøvik, Bian Yang
- Contract-based identity management, Biometric Forum, May, 2019, Oslo, Bian Yang
- eHealth and Welfare Security Research Activities, SikkertNOK 2019, November 2019, Gjøvik, Bian Yang
- Health Security Practice Modelling and Incentivization, Normenkonferanse, November 2019, Oslo, Prosper Yeng

Selected publications

1. Kandabongee Yeng P., Yang B., Arthur Snekkenes E. Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches: A Literature Survey. Studies in health technology and informatics. 2019;261:239-45.
2. Yeng P., Yang B., Snekkenes E., editors. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC); 2019 15-19 July 2019.
3. Yeng P. K., Yang B., Snekkenes E. A., editors. Framework for Healthcare Security Practice Analysis, Modeling and Incentivization International Workshop on Big Data Analytics for Cyber Threat Hunting; 2019 9-12 Dec 2019; Los Angeles: IEEE Big Data.
4. Yeng P. K., Yang B., Weyori B. A., Nimbe P., Solvoll T., editors. Web Vulnerability Measures for SMEs. Norwegian Information Security Conference 2019 20.11.20|9; Narvik: NISK Journal; 2019.
5. M. A. Fauzi, B. Yang, and E. Martiri, "PassGAN-Based Honeywords System," in 2019 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2019.
6. S. Li, H. Xiao, H. Wang, T. Wang, J. Qiao and S. Liu, "Blockchain Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 124-131.
7. Liu, Xiaolei; Du, Xiaojiang; Zhang, Xiaosong; Zhu, Qingxin; Wang, Hao; Guizani, Mohsen. 2019. "Adversarial Samples on Android Malware Detection Systems for IoT Systems." Sensors 19, no. 4: 974.
8. Hao Wang, Chaonian Guo, Shuhan Cheng, LoC — A new financial loan management system based on smart contracts, Future Generation Computer Systems, Volume 100, 2019, Pages 648-655, ISSN 0167-739X
9. Hao Wang, Shenglan Ma, Hong-Ning Dai, Muhammad Imran, Tongsen Wang, Blockchain-based data privacy management with Nudge theory in open banking, Future Generation Computer Systems, 2019, ISSN 0167-739X
10. Q. Wang, H. Dai, H. Wang, G. Xu and A. K. Sangaiah, "UAV-enabled friendly jamming scheme to secure industrial Internet of Things," in Journal of Communications and Networks, vol. 21, no. 5, pp. 481-490, Oct. 2019.

11. Guangquan Xu, Bingjiang Guo, Chunhua Su, Xi Zheng, Kaitai Liang, Duncan S. Wong, Hao Wang, Am I eclipsed? A smart detector of eclipse attacks for Ethereum, Computers & Security, Volume 88, 2020, 101604, ISSN 0167-4048
12. Rang Zhou, Xiaosong Zhang, Xiaofen Wang, Guowu Yang, Hao Wang, Yulei Wu, Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted Internet of Things, Information Sciences, Volume 491, 2019, Pages 251-264, ISSN 0020-0255
13. Ning, Zhenhu, Guangquan Xu, Naixue Xiong, Yongli Yang, Changxiang Shen, Emmanouil Panaousis, Hao Wang, and Kaitai Liang, "TAW: Cost-Effective Threshold Authentication With Weights for Internet of Things," in IEEE Access, vol. 7, pp. 30112-30125, 2019.
14. Xu, Guangquan, Yao Zhang, Litao Jiao, Emmanouil Panaousis, Kaitai Liang, Hao Wang, and Xiaotong Li. "DT-CP: A Double-TTPs-Based Contract-Signing Protocol With Lower Computational Cost," in IEEE Access, vol. 7, pp. 174740-174749, 2019.

3.4.3 Viktige møter og aktiviteter

- Meeting with the employees of Sykehuset Innladnet, Hamar October 2019.
- Meeting with Professor Jeng-Shyang Pan from Shandong University of Science and Technology, Gjøvik, October 2019.
- Meeting with the ambulance department of Sykehuset Innlandet December 2019, Gjøvik, on the topic of better availability and security of the remote video communication
- Visiting and meeting healthcare innovation researchers and industries in Hangzhou, China, June 2019
- Poster presentation and networking in eHIN 2019 on November 2019
- Poster presentation and networking in normenkonferanse 2019 on November 2019

3.4.4 Medlemmer

Akademisk ansatte, fulltid:

- Bian Yang
- Einar Snekkenes
- Vivek Agrawal
- Prosper Yeng
- Muhammad A. Fauzi

Akademisk ansatte, deltid:

- Aud Obstfelder
- Christoph Busch
- Dag Waaler
- Hao Wang
- Katrin Franke
- Laura Georg
- Maren Kristine Raknes Sogstad
- Patrick Bours
- Raghavendra Ramachandra
- Sarita Sunder
- Sokratis Katsikas
- Staal Vinterbo
- Stephen Wolthusen
- Stewart James Kowalski
- Sule Yildirim Yayilgan
- Thomas Kemmerich

3.5 NTNU Digital Forensics research group: TESTIMON

3.5.1 Gruppens hjemmeside:

https://www.ntnu.edu/iik/digital_forensics#/view/about

3.5.2 Gruppens medlemmer:

Kjernemedlemmer:

- Professor Katrin Franke
- Førsteamanuensis Stefan Axelsson
- Førsteamanuensis Mariusz Nowostawski
- Førsteamanuensis Lasse Øverlier

Tilknyttede IIK-medlemmer:

Førsteamanuensis Geir Olav Dyrkolbotn

Eksterne tilknyttede:

Avdelingsdirektør, førsteamanuensis Thomas Walmann, Økokrim

Seniorrådgiver, førsteamanuensis Bente Skattør, Oslo politidistrikt

Professor Inger Marie Sunde, Politihøgskolen

Midlertidige stillinger tilknyttet:

- Post doc Andrii Shalaginov
- Gunnar Alendal, Kripos
- Stig Åsmund Andersen, Oslo politidistrikt
- Jan William Johnson
- Jul Fredrik Kaltenborn, Politihøgskolen
- Martin Karresand, FOI
- Rune Nordvik, Politihøgskolen
- Kyle Porter
- Jens-Petter Skjelvag Sandvik, Kripos
- Abylay Satybaldy
- Rene Pickhardt

3.5.3 Eksterne finansieringskilder:

- Politidirektoratet
- ArsForensica

- ESSENTIAL
- THEUSUS
- Romania Blockchain
- Digital Transformation

3.5.4 Laboratorier som brukes:

- Maskinlæring og kunstig intelligens med forensic fokus
- Blokkjede laboratorium
-

3.5.5 Eksterne samarbeidsparter:

Politidirektoratet

Oslo politidistrikt

3.5.6 Gruppens bakgrunn og hovedmål:

Digital forensics (etterforskning) er voksende grenspesialitet innen informasjons- og cybersikkerhet. Stadig flere lovbrudd inneholder digitale elementer (både vanlige lovbrudd og cyberkriminalitet), noe som gjør forskning innen digital kriminalitet og digital etterforskning økende viktig.

Gruppen utgjør en av forskningsgruppene innenfor NTNU CCIS.

3.5.7 Utdanninger gruppen deltar i:

Vi leverer 2 kurs I digital etterforskning og 1 master-program (erfaringsbasert).

3.5.8 Forskningsaktiviteter:

Pågående forskningsprosjekter:

ArsForensica - (https://www.ntnu.edu/iik/digital_forensics/ars-forensica-rcn-project)

The Ars Forensica project on Computational Forensics for Large-scale Fraud Detection, Crime Investigation & Prevention is funded by the Research Council of Norway for the period 2015-2019.

The overall objective of Ars Forensica is to provide new knowledge that can significantly improve the prevention, preparedness, investigation and prosecution of incidents in ICT environments, without compromising privacy and the rule of law. Ars Forensica addresses topics related to the Research Council of Norway (RCN) IKTPLUSS – programme:

1. Robust and secure (ICT) infrastructures and systems;
2. Privacy-preserving technologies, and
3. Interaction between technology, individuals and communities.

The ESSENTIAL project - (https://www.essentialresearch.eu/) 2017-2020

The ESSENTIAL project is funded by the EU's horizon 2020 grant programme and is a unique programme that brings together academic institutions, governmental organisations and private companies in the field of Security Science. Security is a field of study capable of diverse applications in daily life yet security science is a young discipline which requires much larger inter-disciplinary effort than is dedicated to it to date. ESSENTIAL seeks to address the fundamental problem of developing security science in a way which is theoretically sound and yet maximizes opportunities for applied training in security.

The key challenge in this field and the reason behind building a joint PhD research programme dedicated to Security Science is the need to address security challenges systematically across their life cycle. This requires developing a systematic body of knowledge with strong theoretical and empirical underpinnings, which incorporates both the computer science and information security dimensions and the social, legal and organizational aspects of security.

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 modeling security perception and democratizing intelligence to improving security and privacy in data ecosystems.

ALERT - NFR project (Lothar)

FORMOBILE project and the FREETOOL 3 project, both EU funded projects. In the H2020 FOR MOBILE PHS is the lead of the training package for LEAs, and in the FREETOOL 3 I am contributing developing a new tool. *(Rune)*

Co-Principal Investigator: Project: Digital Forensic Knowledge Integration and Intelligence (DIREKT-Intel), India-Norway collaboration under SPARC scheme, the grant received 6.5 million INR from India & additional funding support from ArsForensica. duration 2 years (April 2019-March 2021). (Vinti)

WP member: Project- Human-oriented Multi-agent cyberSecurity guarding based on resource-aware computational Intelligence for Smart environments (HOMSIS) - IKTPLUSS 2019 (Vinti)

Project: Digital Forensic Knowledge Integration and Intelligence (DIREKT-Intel), India-Norway collaboration under SPARC scheme.

Åpne seminarer:

ArsForensica sammen med politiet

Sendte forskningssøknader:

- **CoDiFI** -
- We targeted SU-DS05-2019 and submitted a H2020 Proposal on **Cybersecurity for Healthcare 4.0 Ecosystems** where NTNU & NR are involved.
- **"Blockchain for the Next Generation Internet ID**: ICT-54-2020" and "Building blocks for resilience in evolving ICT systems ID: SU-ICT-02-2020" calls.
- **Collaboration on the H2020 FINSEC (Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures** - https://www.finsec-project.eu/) project.
- **Collaboration with a cluster of H2020 critical infrastructure protection projects, FINSEC** (https://www.finsec-project.eu/), DEFENDER (http://defender-project.eu/), SAFECARE (https://www.safecare-project.eu/), and RESISTO (http://www.resistoproject.eu/)
- **Human-oriented Multi-agent cyberSecurity guarding based on resource-aware computational Intelligence for Smart environments** (HOMSIS) - IKTPLUSS 2019, *project manager, in processing.*
- **Unveiling caPabilitiy oF deep learning to ensuRe malware detection and respOnse to machine learNing evasion Techniques in Internet Of Things** (UPFRONT-IOT) - FRIPRO 2019, *project manager, in processing*

- **Cyber-Physical Platform for Secure and Optimized NETworked RObotic Systems** (SONETROS) - IKTPLUSS 2019, *co-applicant, in processing.*
- **Cost Action CA17124 Short Term Scientific Mission** (STSM) of Igor Kotsiuba - host researcher.
- **Cost Action CA17124 Short Term Scientific Mission** (STSM) to KTH - visiting researcher.

Publikasjoner

Bok-kapitler med referee:

Gunnar Alendal, Stefan Axelsson, Geir Olav Dyrkolbotn, Exploiting Vendor-Defined Messages in the USB Power Delivery Protocol, Edited book chapter in Advances in Digital Forensics XV, the 15:th IFIP WG 11.9 international conference, January 28-29, 2019. Orlando Florida

Struan Gray, Stefan Axelsson, Forensic Atomic Force Microscopy of Semiconductor Memory Arrays, Edited book chapter in Advances in Digital Forensics XV, the 15:th IFIP WG 11.9 international conference, January 28-29, 2019. Orlando Florida.

Martin Karresand, Åsalena Warnqvist, David Lindahl, Stefan Axelsson and Geir Olav Dyrkolbotn, Creating a Map of User Data in NTFS to Improve File Carving,, Edited book chapter in Advances in Digital Forensics XV, the 15:th IFIP WG 11.9 international conference, January 28-29, 2019. Orlando Florida.

Tidsskriftsartikler:

Abie, Habtamu & Kylänpää, Markku & Savola, Reijo. (2019). Risk-driven Security Metrics for an Android Smartphone Application. International Journal of Information and Computer Security. 11. 1. 10.1504/IJICS.2019.10021820.

M. A. Azad, S. Bag, F. Hao and A. Shalaginov, "Decentralized Self-enforcing Trust Management System for Social Internet of Things," in IEEE Internet of Things Journal, in press.

Mohamed Falah Faiz, Junaid Arshad, Mamoun Alazab, Andrii Shalaginov; Predicting Likelihood of Legitimate Data Loss in Email DLP, Elsevier Future Generation Computer System, 2019. ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.11.004. (http://www.sciencedirect.com/science/article/pii/S0167739X19314943)

Martin Karresand, Stefan Axelsson and Geir Olav Dyrkolbotn, Using NTFS Cluster Allocation Behavior to Find the Location of User Data, Journal article in Digital Investigation 29, 2019.

Martin Karresand, Stefan Axelsson and Geir Olav Dyrkolbotn, Disk Cluster Allocation Behavior in Windows and NTFS, Journal article accepted for publication in Mobile Networks and Applications, 2019.

N. Momen, M. Hatamian and L. Fritsch, "Did App Privacy Improve After the GDPR?," in IEEE Security & Privacy. doi: 10.1109/MSEC.2019.2938445, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8845749&isnumber=5210089

Rune Nordvik, Henry Georges, Fergus Toolan, Stefan Axelsson, Digital Investigation, Reverse Engineering of ReFS, Volume 30, Pages 127-147, September 2019.

Rune Nordvik, Fergus Toolan, Stefan Axelsson, Using the object ID index as an investigative approach for NTFS file systems,, Digital Investigation , Volume 28, Supplement, Pages s30-s147, April 2019.

Nowostawski, Mariusz; Tøn, Jardar. (2019) Evaluating Methods for the Identification of Off-Chain Transactions in the Lightning Network. Applied Sciences. vol. 9 (12).

Konferanser/workshops med referee:

H. Abie, "Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems," 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 2019, pp. 1-6.

Vinti Agarwal, Neminath Huballi, Katrin Franke, Ambika Shreshta. Identifying Anomalous HTTP Traffic with Association Rule Mining. IEEE forum on advanced networking and telecommunications ANTS 2019

Banin, Sergii; Dyrkolbotn, Geir Olav. Correlating High- and Low-Level Features: Increased Understanding of Malware Classification. Lecture Notes in Computer Science 2019 ;Volum 11689. S.149-167. IWSEC 2019, August 28-30, 2019, Tokyo, Japan

S. Boudko and H. Abie, "Adaptive Cybersecurity Framework for Healthcare Internet of Things," 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 2019, pp. 1-6.

Thilo Denzer, Andrii Shalaginov and Geir Olav Dyrkolbotn, Intelligent Windows Malware Type Detection based on Multiple Sources of Dynamic Characteristics, NISK 2019

Gunleifsen, Håkon; Gkioulos, Vasileios; Wangen, Gaute; Shalaginov, Andrii; Kianpour, Mazaher; Abomhara, Mohamed Ali Saleh. (2019) Cybersecurity Awareness and Culture in Rural Norway. Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019).

Hatamian, M., Momen, N., Fritsch, L., & Rannenberg, K. (2019, June). A Multilateral Privacy Impact Analysis Method for Android Apps. In Annual Privacy Forum (pp. 87-106). Springer, Cham.

Nowostawski, Mariusz; Frantz, Christopher. (2019). Quasi-Social: Software as the 'Social' in Socio-Technical Design. In Proceedings of the 5th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2019), Stockholm, Sweden, June 10. Pp.42-53.

Shalaginov, Andrii & Semeniuta, Oleksandr & Alazab, Mamoun. (2019). MEML: Resource-aware MQTT-based Machine Learning for Network Attacks Detection on IoT Edge Devices. 123-128. 10.1145/3368235.3368876.

Ambika Shrestha, Slobodan Petrović, Efficient k-means Using Triangle Inequality on Spark for Cyber Security Analytics, Proceedings of the ACM International Workshop on Security and Privacy Analytics, IWSPA '19, pp. 37-45, March 27, 2019. Dallas, Texas, USA.

Ambika Shrestha, Slobodan Petrović, Analyzing Digital Evidence Using Parallel k-means with Triangle Inequality on Spark, Proceedings of 2018 IEEE International Conference on Big Data, pp. 3049-3058, December 10-13, 2018. Seattle, Washington, USA.

Ambika Shrestha, Slobodan Petrović, Parallel k means clustering with triangle inequality on Spark, Poster presented at Swedish Data Science workshop, SweDS 2018, November 20-21, 2018, Umeå, Sweden. (*POSTER*)

Annet:

Sundberg, S., Blomqvist, A., & Bromander, A. (2019). KAUdroid - Project Report : Visualizing how Android apps utilize permissions. Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-70784

Technical Report: A preliminary Process Model for Investigation., Andersen, Stig, Preprint published at SocArXiv. (Not peer reviewed)

3.6 Andre forskningsgrupper i NTNU CCIS

Forskningsgruppene Systems Security Group og Applied Cryptography er i prosess med å bli innlemmet i NTNU CCIS og vil rapportere på sin aktivitet i 2020. Forskningsgruppen Information Security and Privacy Management har hatt et år med omstilling og redusert aktivitet. Det vil i løpet av 2020 bli avklart i hvilken form denne forskningsgruppen eventuelt kan videreføres.

På neste side følger navn og logoer for våre partnere i 2019:

Information Security