AKADEEMIKUTE VALIMINE 2022

Arvuti- ja tehnikateadused

Link ETISes: Dan Bogdanov

DAN BOGDANOV

Sündinud 28.02.1983

Esitajad

1. Teadus-arendusasutuse Cybernetica AS nõukogu
2. Akadeemikute grupp koosseisus Ülo Jaaksoo ning Jaak Vilo

Haridus, teaduskraad

2007–2013 Tartu Ülikool, doktorikraad (informaatika doktorantuur)
2005–2007 Tartu Ülikool, MSc informaatika (4+2 süsteemi järgi)
2001–2005 Tartu Ülikool, BSc informaatika (4+2 süsteemi järgi)

Teenistuskäik (ETIS)

01.04.2021–… Cybernetica AS, Infoturbeinstituudi direktor (1,00)
01.06.2019–31.03.2021 Cybernetica AS, Infoturbesüsteemide osakonna juhataja (1,00)
01.03.2017–31.05.2019 Cybernetica AS, Privaatsustehnoloogiate osakonna juhataja (1,00)
01.05.2013–28.02.2017 Cybernetica AS, teadusprojektide juht (1,00)
01.10.2007–30.06.2008 Tartu Ülikool, Matemaatika-informaatikateaduskond, Arvutiteaduse instituut, info- ja kommunikatsioonitehnoloogia doktorikooli erakorraline teadur (0,10)
01.09.2006–31.08.2007 OÜ Quretec, analüütik (0,50)
2006–30.04.2013 Cybernetica AS, Teadur (1,00)
01.01.2005–31.12.2006 AS EGeen, analüütik
01.01.2003–31.12.2005 OÜ Web Expert, tarkvaraarendaja
01.01.2000–31.12.2001 OÜ Maripuu Meedia, tarkvaraarendaja

Teadustöö põhisuunad (ETIS)
ETIS VALDKOND: 4. Loodusteadused ja tehnika; 4.7. Info- ja kommunikatsioonitehnoloogia; TÄPSUSTUS: privaatsust säilitav andmetöötlus
ETIS VALDKOND: 4. Loodusteadused ja tehnika; 4.7. Info- ja kommunikatsioonitehnoloogia; TÄPSUSTUS: turvalised hajussüsteemid

Kuni viis käimasolevat teadusprojekti (roll, pealkiri, rahastaja) (konkursikeskkond)

1. Projekt: PROVENANCE (PROofs and Verifications between governmENts ANd CitizEns)
   Rahastaja: DARPA (Defense Advanced Research Projects Agency), Ameerika Ühendriigid
   Roll: projekti kaasjuht (Co-Principal Investigator)
   Periood: 1. aprill 2020 - 30. märts 2024
   Lühikokkuvõte: DARPA SIEVE (Securing Information for Encrypted Verification and Evaluation) programmist rahastatav PROVENANCE projektis uurime nullteadmustõestuste (Zero Knowledge Proofs) rakendamist isikute, ettevõtete ja riikide vahelistes tõendite väljastamises.
   Veebiaadress: https://www.darpa.mil/program/securing-information-for-encrypted-verification-and-evaluation
2. Projekt: CoNurse

Rahastaja: Ettevõtluse Arendamise Sihtasutuse Rakendusuuringute programm (RUP)
Roll: projekti kaasjuht (Co-Principal Investigator)
Periood: 1. jaanuar 2022 - 31. detsember 2023
Lühikokkuvõte: CoNurse projektis uuritakse koos Cognuse OÜga usaldatavate käivituskeskkondade (Trusted Execution Environments) tehnoloogiate kasutamist tervishoiuandmete lõimprivaatsel (Privacy-by-Design) töötlemiseks.
Veebiaadress: https://eas.ee/en/estonia-supports-30-applied-research-and-product-development-projects-with-19-4-million-euros/

3. Projekt: FAMOUS
   Rahastaja: European Defence Industrial Development Programme (EDIDP)
   Roll: Projekti juht
   Periood: 1. detsember 2021 – 30. november 2023
   Lühikokkuvõte: FAMOUS projektis uurime, kas ründepindade ja ründepuude põhised turvaanalüüsimeetodid on kohandatavad keerukamatele küberfüüsilistele süsteemidele nagu sõidukid.
   Veebiaadress: https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP2020_factsheet_GCC_FAMOUS.pdf
4. Projekt: LAGO
   Rahastaja: Horizon Europe
   Roll: projekti kaasjuht (Co-Principal Investigator)
   Periood: 2022-2024
   Lühikokkuvõte: LAGO (Lessen Data Access And Governance Obstacles) projekti eesmärgiks on uurida viise, kuidas kuritegevuse ja terrorismivastases võitluses õnnestuks rakendada eetiliselt ja turvaliselt ettevõtete ja isikute andmeid.

Juhendamine (kaitstud väitekirjade arv) (ETIS)

Magistrikraad – 10
Doktorikraad – 1

Ühiskondlik tegevus, sh tegevus oma teadusvaldkonna populariseerimisel (konkursikeskkond)

1) Teaduspõhiste e-riigi turvalahenduste populariseerimine Eestis ja rahvusvaheliselt

Valik tele-esinemistest:

Viirusekandjate jälgimine, ETV Ringvaade 16.04.2020, https://etv.err.ee/1078602/viirusekandjate-jalgimine
Vaktsineerimise korraldus, ETV Suud puhtaks 13.04.2021, https://etv.err.ee/1608163573/suud-puhtaks

Valik konverentsiesinemistest:

- RIA veebikonverents „Olukorrast digiriigis“ 2021 – Debatt: Kuidas riik tagab valimiste turvalisuse? https://www.youtube.com/watch?v=YrujDMakK8U
- Breakout session: Safety and security in the age of artificial intelligence I #TallinnDigitalSummit https://www.youtube.com/watch?v=ZZEcW_ri-i0

Valik ajakirjanduses ilmunud artiklitest:

- https://www.err.ee/617803/intervjuu-id-kaardi-turvarisk-e-riigi-kasutusse-suuri-mojutusi-ei-too
- https://ekspress.delfi.ee/artikkel/120029802/dan-bogdanov-igauks-peab-noudma-oma-andmete-kaitsmist
- https://ekspress.delfi.ee/artikkel/90870915/peame-talitsema-ihalust-kohustusliku-ule-eestilise-jalgimissusteemi-jarele

- https://digi.geenius.ee/rubriik/uudis/dan-bogdanov-kui-asukohaandmed-ara-anda-siis-tagasi-saada-on-neid-raske/
- https://digi.geenius.ee/rubriik/uudis/andmeteadlane-kuidas-ehitada-taiesti-anonuumset-elektroonset-majutuskaarti/

2) Arvutiteaduse populariseerimine teistes valdkondades
Valik esinemistest:

36. Eesti õigusteadlaste päevad: PÕHISEADUS 100. Plenaaristung. Kas põhiõiguste kaitsega on liiale mindud?, https://www.uttv.ee/naita?id=30535
TDS 2019 Parallel Breakout Sessions I: AI in Healthcare, https://www.youtube.com/watch?v=atOnB1dW0OA

Valik artiklitest:

Arvutiteadus ja juura - https://juridica.ee/article.php?uri=2020_6_infotehnoloogilised_v_imalused_p_hi_iguste_kaitsel
Arvutiteadus ja meditsiin - https://www.aripaev.ee/saated/2020/08/19/ekspert-selgitab-koroonaapi-parast-muret-tundma-ei-pea

3) Komisjonides ja nõukogudes osalemine

ETAGi hindamisnõukogu nimetamiskogu - https://www.etag.ee/eesti-teadusagentuur-sai-uue-hindamisnoukogu-3/
EAS Ettevõtjate rakendusuuringute ja tootearenduse meetme hindamiskomisjon - https://eas.ee/eas/hindamiskomisjonid/
Tartu Ülikooli IT Akadeemia programmi nõukogu liige

Teadusorganisatsiooniline ja -administratiivne tegevus (ETIS)

Tartu Ülikooli IT Akadeemia programmi nõukogu liige
2020–... EAS, Ettevõtjate rakendusuuringute ja tootearenduse meetme hindamiskomisjon
2019–... Eesti Teadusagentuuri nimetamiskogu liige
2009–... ISO/IEC JTC1 SC27 tööst osavõtt, privaatsusstandardite arendamine
2015–2016 Programmikomitee liige, Workshop on Encrypted Computing and Applied Homomorphic Cryptography
2014–2014 Programmikomitee liige, International Baltic Conference on Databases and Information Systems
2014–2014 Programmikomitee liige, International Workshop on Genome Privacy and Security
2013–2017 ISO/IEC standardiprojekti 19592 (Ühissalastus) toimetaja
2010–2013 ISO/IEC standardiprojekti 29101 (Privaatsete rakenduste arhitektuur) toimetaja
2008–2012 Tartu Ülikooli Matemaatika-informaatikateaduskonna arvutiteaduse instituudi informaatika erialade programminõukogu liige
2007–2009 Tartu Ülikooli Matemaatika-informaatikateaduskonna nõukogu liige

Teaduspreemiad ja tunnustused (ETIS)

2016, Dan Bogdanov, Eesti Vabariigi Presidendi Noore IT-teadlase eripreemia
2015, Dan Bogdanov, Valgetähe teenetemärk, IV klass
2014, Dan Bogdanov, Eesti Vabariigi Kaitseministeeriumi teaduspreemia
2013, Dan Bogdanov, Silmapaistev Noor Eestlane (teadlane)
2010, Dan Bogdanov, ITL-i Ustus Aguri doktorandistipendiumi laureaat
2007, Dan Bogdanov, Eesti üliõpilaste teadustööde riiklik konkurss 2007. aastal - III preemia magistritööde arvestuses loodusteaduste ja tehnika valdkonnas töö „Kuidas teha turvaliselt arvutusi ühissalastatud andmetega“ eest

2002, Dan Bogdanov, Expo Science Europe 2002 – peaauhind inseneriteaduste kategoorias töö „Meetod kahe punkti vahelise lühima tee leidmiseks etteantud kolmemõõtmelisel maastikul“

Varasem kandideerimine – ei

BIBLIOMEETRILISED ANDMED

Otsingutulemused seisuga 04.10.2022

Publikatsioonide arv, viidete arv, h-indeks (esildise alusel)	***Web of Science*** 1990–2022 –––––––––––––– ***Google Scholar*** (kõik)			***Web of Science*** 2012–2022	
	Publ. arv	Viidete arv	h-indeks	Publ. arv	Viidete arv
Kokku 48 (ETIS)	13 60	554 2356	9 21	12	290

Kümme tähtsamat publikatsiooni

Publikatsioonide üldarv: 48 (ETIS)

1) Troncoso, Carmela; Bogdanov, Dan; Bugnion, Edouard; Chatel, Sylvain; Cremers, Cas; Gürses, Seda; Hubaux, Jean-Pierre; Jackson, Dennis; Larus, James R.; Lueks, Wouter; Oliveira, Rui; Payer, Mathias; Preneel, Bart; Pyrgelis, Apostolos; Salathé, Marcel; Stadler, Theresa; Veale, Michael (2022). Deploying decentralized, privacy-preserving proximity tracing. Communications of the ACM, 65 (9), 48−57. DOI: 10.1145/3524107.

2) Archer, David W.; Bogdanov, Dan; Lindell, Yehuda; Kamm, Liina; Nielsen, Kurt; Pagter, Jakob Illeborg; Smart, Nigel P.; Wright, Rebecca N. (2018). From Keys to Databases -- Real-World Applications of Secure Multi-Party Computation. The Computer Journal, 61 (12), 1749−1771. DOI: 10.1093/comjnl/bxy090.

3) Bogdanov, Dan; Kamm, Liina; Laur, Sven; Sokk, Ville (2018). Rmind: a tool for cryptographically secure statistical analysis. IEEE Transactions on Dependable and Secure Computing, 15 (3), 481−495. DOI: 10.1109/TDSC.2016.2587623.

4) Pullonen, P.; Matulevičius, R.; Bogdanov, D. (2017). PE-BPMN: Privacy-Enhanced Business Process Model and Notation. International Conference on Business Process Management (BPM 2017), 10445: International Conference on Business Process Management (BPM 2017), Barcelona. Ed. Carmona J., Engels G., Kumar A. Springer, 40−56. DOI: 10.1007/978-3-319-65000-5_3.

5) Bogdanov, Dan; Kamm, Liina; Kubo, Baldur; Rebane, Reimo; Sokk, Ville; Talviste, Riivo (2016). Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation. Proceedings on Privacy Enhancing Technologies, 2016 (3), 117−135. DOI: 10.1515/popets-2016-0019.

6) Bogdanov, Dan; Jõemets, Marko; Siim, Sander; Vaht, Meril (2015). How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation (Short Paper). Financial Cryptography and Data Security 2015, 19th International Conference, San Juan, Puerto Rico, 26.-29.01.2015. Ed. Rainer Böhme, Tatsuaki Okamoto. Springer Heidelberg, 227−234. (Lecture Notes in Computer Science; 8975). DOI: 10.1007/978-3-662-47854-7_14.

7) Kamm, Liina; Bogdanov, Dan; Laur, Sven; Vilo, Jaak (2013). A new way to protect privacy in large-scale genome-wide association studies. Bioinformatics, 29 (7), 886−893. DOI: 10.1093/bioinformatics/btt066.

8) Bogdanov, Dan; Talviste, Riivo; Villemson, Jan (2012). Deploying secure multi-party computation for financial data analysis. In: Angelos D. Keromytis (Ed.). Proceedings of the Sixteenth International Conference on Financial Cryptography and Data Security (57−64). . Springer. (Lecture Notes in Computer Science).

9) Bogdanov, Dan; Niitsoo, Margus; Toft, Tomas; Willemson, Jan (2012). High-performance secure multi-party computation for data mining applications. International Journal of Information Security, 11 (6), 403−418. DOI: 10.1007/s10207-012-0177-2.

10) Bogdanov, Dan; Laur, Sven; Willemson, Jan (2008). Sharemind: a framework for fast privacy-preserving computations. Computer Security – ESORICS 2008: 13th European Symposium on Research in Computer Security Málaga, Spain, October 6-8, 2008. Ed. Jajodia, Sushil; Lopez, Javier. Heidelberg: Springer, 192−206. (Lecture Notes in Computer Science; 5283). DOI: 10.1007/978-3-540-88313-5_13.