Advancing cybersecurity education through learning analytics = Küberkaitsealase hariduse parendamine õpianalüütika abil
Maennel, Kaie 2021 https://doi.org/10.23658/taltech.29/2021 https://www.ester.ee/record=b5434228*est https://digikogu.taltech.ee/et/Item/d01c0b17-3b4b-41c5-ae24-e75b6128a183

An enhanced lightweight authentication scheme for secure access to cloud data
Hammami, Hamza; Obaidat, Mohammad S.; **Ben Yahia, Sadok** Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 3: ICE-B, Lieusaint, Paris, France, July 8-10, 2020 2020 / p. 110-117 https://doi.org/10.5220/0009824301100117

An expectation-based approach to policy-based security of the Border Gateway Protocol
Li, Jun; Stein, Josh; Zhang, Mingwei; **Maennel, Olaf Manuel** 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) : GI 2016 : IEEE Global Internet Symposium : April 10-14, 2016, San Francisco, CA, USA 2016 / p. 340-345 : ill https://doi.org/10.1109/INFCOMW.2016.7562098 Conference Proceedings at Scopus Article at Scopus Article at WOS

Are the current system engineering practices sufficient to meet cyber crime?
Buldas, Ahto; Saarepera, Märt Human Aspects of Information Security, Privacy and Trust : 5th International Conference, HAS 2017 : held as part of HCI International 2017, Vancouver, BC, Canada, July 9–14, 2017 : proceedings 2017 / p. 451-463 https://doi.org/10.1007/978-3-319-58460-7_31 Conference proceedings at Scopus Article at Scopus Article at WOS

Assessing safety of object pushing using the principle of reversibility
Gavšin, Juri; **Kruusmaa, Maarja** Hybrid Artificial Intelligent Systems : 6th International Conference : HAIS 2011 : Wroclaw, Poland, May 23-25, 2011 : proceedings. Part I 2011 / p. 313-320 : ill https://link.springer.com/chapter/10.1007/978-3-642-21219-2_40

Attacker profiling in quantitative security assessment based on attack trees
Lenin, Aleksandr; Willemson, Jan; **Sari, Dyan Permata** Secure IT Systems : 19th Nordic Conference, NordSec 2014, Tromsø, Norway, October 15–17, 2014, Proceedings 2014 https://doi.org/10.1007/978-3-319-11599-3_12 Article collection metrics at Scopus Article at Scopus

Automating defences against cyber operations in computer networks = Arvutivõrkude kaitse automatiseerimine küberoperatsioonide vastu
Pihelgas, Mauno 2021 https://doi.org/10.23658/taltech.36/2021 https://www.ester.ee/record=b5449710*est https://digikogu.taltech.ee/et/Item/beb3e841-9c6e-4496-a73a-17148bc941ef

Bandwidth Reduction DoS attacks in Multi-Tenant NoC-based MPSoCs : detection and avoidance strategies = Ribalaiuse vähendamise DoS-rünnakud mitme rentnikuga NoC-põhiste MPSoC-de puhul : tuvastamise ja vältimise strateegiad
Chaves Arroyave, Cesar Giovanni 2023 https://doi.org/10.23658/taltech.8/2023 https://digikogu.taltech.ee/et/Item/60b3f5ee-3a53-43c6-b79e-d6a8cbbc3489 https://www.ester.ee/record=b5548907*est

Black-box separations and their adaptability to the non-uniform model
Buldas, Ahto; Niitsoo, Margus Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 152-167 https://doi.org/10.1007/978-3-642-39059-3_11 Conference Proceedings at Scopus Article at Scopus

Bounded pre-image awareness and the security of hash-tree keyless signatures
Buldas, Ahto; **Laanoja, Risto**; Laud, Peeter; Truu, Ahto Provable security : 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014 : proceedings 2014 / p. 130-145 : ill https://doi.org/10.1007/978-3-319-12475-9_10 Conference proceeding at Scopus Article at Scopus Conference proceeding at WOS Article at WOS

Comparative analysis of pattern mining algorithms for event logs
Gasimov, Orkhan; **Vaarandi, Risto**; **Pihelgas, Mauno** 2023 IEEE International Conference on Cyber Security and Resilience (CSR) : Venice, Italy, 2023 2023 / 7 p https://doi.org//10.1109/CSR57506.2023.10224996

Detecting and mitigating Low-and-Slow DoS attacks in NoC-based MPSoCs
Chaves Arroyave, Cesar Giovanni; **Azad, Siavoosh Payandeh**; Sepulveda, Johanna; **Hollstein, Thomas** 2019 14th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC) : July 1-3 2019, York - United Kingdom : proceedings 2019 / p. 82-89 : ill https://doi.org/10.1109/ReCoSoC48741.2019.9034934

Does secure time-staming imply collision-free hash functions
Buldas, Ahto; **Jürgenson, Aivo** Info- ja kommunikatsioonitehnoloogia doktorikooli IKTDK kolmanda aastakonverentsi artiklite kogumik : 25.-26. aprill 2008, Voore külalistemaja 2008 / p. 59-63 : ill

Does secure time-stamping imply collision-free hash functions?
Buldas, Ahto; Jürgenson, Aivo Lecture notes in computer science 2007 / p. 138-150

Efficient semantics of parallel and serial models of attack trees = Ründepuude paralleel- ja jadamudelite efektiivsed

semantikad
Jürgenson, Aivo 2010 https://www.ester.ee/record=b2604924*est

802.11 Denial of Service ründed ja nende leevendamine : referaat
Rebane, Andri A & A 2009 / 2, lk. 43-50 : ill https://artiklid.elnet.ee/record=b1451681*est

E-learning environment identification system : error injection and patterns dynamics
Kumlander, Deniss Innovations and advances in computer, information, systems sciences, and engineering 2013 / p. 917-924 https://doi.org/10.1007/978-1-4614-3535-8_76 Conference Proceedings at Scopus Article at Scopus

An experimental study of building blocks of lattice-based NIST post-quantum cryptographic algorithms
Imran, Malik; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** Electronics 2020 / art. 1953, 26 p. : ill https://doi.org/10.3390/electronics9111953 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Frankenstack : real-time cyberattack detection and feedback system for technical cyber exercises
Pihelgas, Mauno; **Kont, Markus** Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), July 26–28, 2021 : Virtual Conference : proceedings 2021 / p. 396-402 https://doi.org/10.1109/CSR51186.2021.9527923

Gone phishin' (but not to jail) [Online resource]
Mäses, Sten; Kikerpill, Kristjan Proceedings of the 3rd Interdisciplinary Cyber Research Workshop 2017 : 8th of July 2017 2017 / p. 29-30 https://www.ttu.ee/public/k/kyberkriminalistika_ja_kyberjulgeoleku_keskus/crw2017_final.pdf

Hardware realization of lattice-based post-quantum cryptography = Võrel põhinev post-kvant-krüptograafia riistvaraline realisatsioon
Imran, Malik 2023 https://www.ester.ee/record=b5571216*est https://doi.org/10.23658/taltech.33/2023 https://digikogu.taltech.ee/et/Item/75aeb070-cb8b-4511-beaf-cbea3fca147d https://www.ester.ee/record=b5571216*est

Hardware trojan insertion in finalized layouts : from methodology to a silicon demonstration
Perez, Tiago Diadami; **Pagliarini, Samuel Nascimento** IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2023 / p. 2094-2107 https://doi.org/10.1109/TCAD.2022.3223846 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Hardware Trojans for confidence reduction and misclassifications on neural networks
Grailoo, Mahdieh; **Leier, Mairo**; **Pagliarini, Samuel Nascimento** Proceedings Of The Twenty Third International Symposium On Quality Electronic Design (ISQED 2022) 2022 / art. 180541, p. 230-235 https://doi.org/10.1109/ISQED54688.2022.9806246

Infosüsteemide turve
Hanson, Vello; **Buldas, Ahto** 1997 https://www.ester.ee/record=b1059903*est

Infotehnoloogia. Sõnastik. Osa 8, Turvalisus
Hanson, Vello; Tavast, Arvi; **Kalja, Ahto**; **Võhandu, Leo** 1999 https://www.ester.ee/record=b1323628*est

Keyless signature infrastructure and PKI : hash-tree signatures in pre- and post-quantum world
Buldas, Ahto; **Laanoja, Risto**; **Truu, Ahto** International journal of services technology and management 2017 / p. 117-130 : ill https://doi.org/10.1504/IJSTM.2017.10002708 Journal metrics at Scopus Article at Scopus

Kübermaailmas on oluline probleeme ennetada
Sõmer, Tiia Mente et Manu 2017 / lk. 30-33 : fot http://www.ttu.ee/public/m/mente-et-manu/MM_01_2017/index.html https://artiklid.elnet.ee/record=b2811469*est

Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta [Võrguväljaanne]
digipro.geenius.ee 2022 Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta

Leveraging layout-based effects for locking analog ICs
Aljafar, Muayad J.; Azais, Florence; Flottes, Marie-Lise; **Pagliarini, Samuel Nascimento** ASHES'22: Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security 2022 / p. 5-13 https://doi.org/10.1145/3560834.3563826

Long-term secure time-stamping using preimage-aware hash functions : (short version)
Buldas, Ahto; Geihs, Matthias; Buchmann, Johannes Provable Security : 11th International Conference, ProvSec 2017, Xi'an, China, October 23–25, 2017 : proceedings 2017 / p. 251-260 : ill http://doi.org/10.1007/978-3-319-68637-0_15 Conference proceedings at Scopus Article at Scopus Article at WOS

Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance
Leiding, Benjamin; **Norta, Alexander** Future Data and Security Engineering : 4th International Conference, FDSE 2017, Ho Chi Minh City, Vietnam, November 29 - December 1, 2017 : proceedings 2017 / p. 181-196 : ill https://doi.org/10.1007/978-3-319-70004-5_13

Conference proceedings at Scopus Article at Scopus Article at WOS

MedBIoT : generation of an IoT Botnet Dataset in a medium-sized IoT network
Guerra Manzanares, Alejandro; **Medina-Galindo, Jorge**; **Bahsi, Hayretdin**; **Nõmm, Sven** Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP : February 25-27, 2020, La Valletta, Malta. Vol. 1 2020 / p. 207-218 : ill https://doi.org/10.5220/0009187802070218

Mikrokontrollerite riistvara turbest
Toomsalu, Arvo Arvutustehnika ja Andmetöötlus 1997 / 7/8, lk. 7-12

Mikrokontrollerite turve
Toomsalu, Arvo Arvutustehnika ja Andmetöötlus 1997 / 5, lk. 12-13; 6, lk. 10-15

Mobiilse pahavara plahvatusele võib pakkuda leevendust masinõpe [Võrguväljaanne]
Oidermaa, Jaan-Juhan novaator.err.ee 2022 Mobiilse pahavara plahvatusele võib pakkuda leevendust masinõpe

New efficient utility upper bounds for the fully adaptive model of attack trees
Buldas, Ahto; **Lenin, Aleksandr** Decision and game theory for security : 4th International Conference, GameSec 2013, Fort Worth, TX, USA, November 11-12, 2013 : proceedings 2013 / p. 192-205 : ill https://doi.org/10.1007/978-3-319-02786-9_12 Computer Proceedings metrics at Scopus Article at Scopus

A novel anonymous authentication and key agreement scheme for smart grid
Hammami, Hamza; Obaidat, Mohammad S.; **Ben Yahia, Sadok** Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 3: ICE-B, Lieusaint, Paris, France, July 8-10, 2020 2020 / p. 357-362 https://doi.org/10.5220/0009824203570362

Password attacks and generation strategies
Tasevski, Predrag TTÜ üliõpilaste teadustööde konkursi kokkuvõtted : Tipika teaduskonverents, 24. november 2011, Tallinn 2011 / p. 14

Proceedings of the 1st Interdisciplinary Cyber Research Workshop 2015 : 18th of July 2015, Tallinn University of Technology [Online resource]
2015 http://cybercentre.cs.ttu.ee/en/icr2015/

Proceedings of the 2nd Interdisciplinary Cyber Research Workshop 2016 [Online resource]
2016 http://cybercentre.cs.ttu.ee/wp/wp-content/uploads/2016/03/CRW_2016_lingitud.pdf http://www.ester.ee/record=b4579694*est

Proceedings of the 3rd Interdisciplinary Cyber Research Workshop 2017 : 8th of July 2017 [Online resource]
2017 http://www.ester.ee/record=b4684355*est https://www.ttu.ee/public/k/kyberkriminalistika_ja_kyberjulgeoleku_keskus/crw2017_final.pdf

Proceedings of the 4th Interdisciplinary Cyber Research Workshop 2018 : 9th of June 2018 [Online resource]
2018 https://www.ttu.ee/public/k/kyberkriminalistika_ja_kyberjulgeoleku_keskus/CRW_2018_lingitud.pdf https://www.ester.ee/record=b5139478*est

Rational choice of security measures via multi-parameter attack trees
Buldas, Ahto; Laud, Peeter; Priisalu, Jaan; Saarepera, Märt; Willemson, Jan 1st International Workshop on Critical Information Infrastructures Security : Samos Island, Greece, August 30 - September 2, 2006 2006 / p. 232-243 https://link.springer.com/chapter/10.1007/11962977_19

Regulatory patterns of the Internet development : expanding the role of private stakeholders through mediatized "self-regulation"
Solarte Vasquez, Maria Claudia Baltic journal of European studies 2013 / p. 84-120 https://artiklid.elnet.ee/record=b2646912*est

Roy, Partha Sarathi ; Dutta, Sabyasachi ; Susilo, Willy ; Safavi-Naini, Reihaneh. Password protected secret sharing from lattices : [review]
Henno, Jaak zbMATH Open 2022 / 1 p. https://zbmath.org/pdf/1492.94193.pdf

Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns
Norta, Alexander; Matulevičius, Raimundas; Leiding, Benjamin Computers & Security 2019 / p. 253−269 https://doi.org/10.1016/j.cose.2019.05.017 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Security and privacy issues in cloud computing : [brief descriptions]
Abbas, Haider; **Maennel, Olaf Manuel**; Assar, Said Annals of telecommunications 2017 / p. 233-235 https://doi.org/10.1007/s12243-017-0578-3 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Security proofs for hash tree time-stamping using hash functions with small output size
Buldas, Ahto; **Laanoja, Risto** Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 235-250 : ill https://doi.org/10.1007/978-3-642-39059-3_16 Conference Proceedings at Scopus Article at Scopus

Security protocols analysis in the computational model - dependency flow graphs-based approach = Turvaprotokollide analüüs arvutuslikul mudelil - sõltuvusgraafidel põhinev lähenemisviis
Tšahhirov, Ilja 2008 https://www.ester.ee/record=b2449152*est

Simple infeasibility certificates for attack trees
Buldas, Ahto; **Lenin, Aleksandr**; Villemson, Jan; **Charnamord, Anton** Advances in Information and Computer Security : 12th International Workshop on Security, IWSEC 2017, Hiroshima, Japan, August 30 – September 1, 2017 : proceedings 2017 / p. 39-55 : ill https://doi.org/10.1007/978-3-319-64200-0_3 Conference proceedings at Scopus Article at Scopus Article at WOS

Specialized cyber red team responsive computer network operations = Vastutegevusele orienteeritud punase meeskonna küberoperatsioonid
Blumbergs, Bernhards 2019 https://digi.lib.ttu.ee/i/?12015

TalTechi arvutisüsteemide professori uudne tehnoloogia raskendab spionaaži [Võrguväljaanne]
Kald, Indrek ituudised.ee 2021 "TalTechi arvutisüsteemide professori uudne tehnoloogia raskendab spionaaži

Towards a healthcare cybersecurity certification scheme
Hovhannisyan, Kristine; Bogacki, Piotr; Colabuono, Consuelo Assunta; Lofu, Domenico; Marabello, Maria Vittoria; **Maxwell, Brady Eugen** 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) 2021 / p. 1-9 https://doi.org/10.1109/CyberSA52016.2021.9478255

Vastupidavus võrgusüsteemides
Viigipuu, Rain A & A 2009 / 1, lk. 22-30 https://artiklid.elnet.ee/record=b1226510*est

Студента TalTech ждал неприятный сюрприз в начале учебного года: как такое могло произойти?
postimees.ee 2023 Студента TalTech ждал неприятный сюрприз в начале учебного года: как такое могло произойти?