

MART ORUAAS

KONTAKTANDMED

Sündinud 16.novembril 1976

e-post mart.oruaas@gmail.com

telefon (M) +372 5100227

HARIDUS

1995-2001 Tallinna Tehnikaülikool

*Tehnikateaduste
bakalaureus* Informaatika

ERIALASED OSKUSED

Hajussüsteemid Protokollide disain, hajussüsteemide töökindlus, jõudlus ja turvalisus. Süsteemide formaalne spetsifitseerimine ja verifitseerimine.

Andmeturve Infosüsteemide formaalne turvaanalüüs. Turvaprotokollide disain ja realiseerimine. Tarkvaratehniliste meetmete rakendamine tarkvara ründekindluste tõstmiseks.

*Programmeerimis-
keeled* C, C++, Java, Scala, Ruby, Python, Rust, Go, SQL, JavaScript.

*Formaalsed spetsi-
fitseerimiskeeled* TLA+/PlusCal, Coq, Tamarin, ProVerif.

TÖÖKOGEMUS

Cybernetica AS 2014–Present Süsteemiarhitekt, CYBERNETICA AS — Tallinn

Mitmesugused andmeturbe-alased arendusprojektid. Krüptograafiliste protokollide projekteerimine ja realiseerimine. Infosüsteemide turvaanalüüs. Rakendusuuringud krüptograafia ja infoturbe valdkonnast.
Kompetents: C++, Java, Python, hajussüsteemide arendus

2013–2014 Vabakutseline tarkvaraarendaja

Spetsiifilised allhanketööd mitmele startup-firmale.
Kompetents: C++, Python, algoritmide disain

GrabCAD 2012–2013 Tarkvaraarhitekt, GRABCAD — Tallinn

Tarkvaraarhitekt GrabCADi Tallinna arenduskontoris. Vastutav grabcad.com teenusserverite tarkvaraarhitektuuri, skaleeruvuse ja turvalisuse eest.
Kompetents: Veebiteenuste arendus, skaleerimine ja turvalisus. Mastaapsete rakenduste haldamine pilveteenuse pakkuja keskkonnas. Arendusmeeskonna juhtimine DevOps heade tavade alusel.

2008–2012 Senior Core Library Developer, SKYPE — Tallinn

*Skype Engineering
Ltd.* Skype Core Library ehk Skype tuumiteenuste C++ teegi arhitekt ja arendaja. Tegelesin madala taseme klient-server ning P2P protokollidega, s.h. kõne ja video voogedastuse protokollidega. Viimased kolm kuud sellest ajast olin Microsoft Corporationi Principal Software Development Engineer.
Kompetents: C++, Python, TCP/IP võrguprotokollid, hajus ning paralleelne programmeerimine, pehme reaalaaja tarkvarasüsteemid, algoritmide ja protokollide disain

Skype Engineering Ltd.	2005–2008	Senior Backend Developer, SKYPE — Tallinn	Skype keskteenuste arhitekt ja arendaja. Tegelesin põhiliselt kõnehalduse ning kõne voogedastuse komponentidega. Põhiosa tööst seisnes suure koodimahu ning kõrgete jõudlus- ja käideldavusnõuetega C++ rakenduste loomises ning nende opereerimise toetamises. Kompetents: C++, Python, TCP/IP võrguprotokollid, hajus ning paralleelne programmeerimine, pehme reaalaaja tarkvarasüsteemid, algoritmide ja protokollide disain
Pankade Kaardikeskuse AS	1998–2005	Süsteemiinsener, PANKADE KAARDIKESKUS — Tallinn	Erinevad ametikohustused UNIXi serveri administraatorist kaardimakseprotokollide disainimise ja standardiseerimiseni. Firma tänane nimi on Nets Estonia. Kompetents: UNIX/Linux, C/C++, Java, Windows, protokollide disain, andmeturve
Spin TEK AS	1992–1998	Arvutiinsener, SPIN TEK — Tallinn	Arvutite remont, arvutivõrkude ehitus ja hooldus Kompetents: Windows, Linux, Novell Netware, IP ja IPX arvutivõrgud

PUBLIKATSIOONID

Riigi Infosüsteemi Amet, 2021	Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides. Autorid: Mart Oruaas, Aivo Kalu, Jaak Pruulmann-Vengerfeldt, Kristjan Krips, Jan Willemson
Keynote paper at Baltic DB&IS 2020	Developing requirements for the new encryption mechanisms in the Estonian eID infrastructure. Autorid: Mart Oruaas, Jan Willemson
Cybernetica AS, 2018	European Patent EP3529948B1 – Composite Digital Signatures. Autorid: Ahto Buldas, Aivo Kalu, Peeter Laud, Mart Oruaas
ESORICS 2017	Server-Supported RSA Signatures for Mobile Devices. Autorid: Ahto Buldas, Aivo Kalu, Peeter Laud, Mart Oruaas
Vabariigi Valimiskomisjon, 2003	E-hääletamise turvaanalüüs E-hääletamise kontseptsiooni turve: analüüs ja meetmed, EH-02-01. Autorid: Arne Ansper, Ahto Buldas, Mart Oruaas, Jaan Priisalu, Anto Veldre, Jan Willemson, Kaur Virunurm

MUU INFORMATSIOON

Auhinnad	2018 · Aasta tegija, Cybernetica AS 2015 · Aasta üllataja, Cybernetica AS 2005-2012 · Mitmed Skype sisemised auhinnad edukate projektide eest
Keeleoskus	EESTI · Emakeel INGLISE · Väga hea VENE · Põhitase

7. aprill 2021. a.