

MART ORUAAS

PERSONAL INFORMATION

Born in Estonia, 16 November 1976

e-mail mart.oruaas@gmail.com

phone (M) +372 5100227

EDUCATION

1995–2001 Tallinn Technical University

Bachelor of Science Informatics

PROFESSIONAL SKILLS

Distributed systems Protocol design, reliability, performance and security of distributed systems. Formal specification and verification of distributed software systems.

Information security Formal security analysis of information systems. Design and implementation of security protocols. Software hardening through advanced methods in software engineering.

Programming languages C, C++, Java, Scala, Ruby, Python, Rust, Go, SQL, JavaScript.

Formal specification languages TLA+/PlusCal, Coq, Tamarin, ProVerif.

WORK EXPERIENCE

2014–Present System Architect, CYBERNETICA AS — Tallinn

Cybernetica AS Working on information security related software projects. Design and implementation of cryptographic protocols.
Competencies: C++, Java, Python, distributed and concurrent programming, algorithm and protocol design. Cryptographic protocol design and implementation. Formal security analysis of information systems. Applied research in the fields of cryptography and information security.

2013–2014 Freelance software engineer

Worked as software developer for several early-stage startups.
Competencies: C++, Python, algorithm design

2012–2013 Software Architect, GRABCAD — Tallinn

GrabCAD Software Architect in GrabCAD Tallinn development office. Responsible for structuring, scaling and securing GrabCAD backend services.
Competencies: Web application development, scaling and securing. Working with large deployments on cloud infrastructure. Running a team in DevOps mode.

2008–2012 Senior Core Library Developer, SKYPE — Tallinn

Skype Engineering Ltd. Architect and developer of Skype Core Library, the cross-platform C++ runtime that implements most of functionality found in Skype clients. Responsibility areas included low-level networking and P2P media and signalling transport protocols. Took part of design and implementation of transport layer for Group Video Calling feature. For the last three months I was employed as Principal Software Development Engineer in Microsoft Corporation.
Competencies: C++, Python, IP networking, distributed and concurrent programming, semi-realtime software systems, algorithm and protocol design

<i>Skype Engineering Ltd.</i>	2005–2008	Senior Backend Developer, SKYPE — Tallinn	Architect and developer of several Skype serverside components, including the ones responsible for call signalling and media transport. Majority of the work involved writing and maintaining large C++ codebases and supporting operational staff in maintaining applications built from those codebases. Competencies: C++, Python, IP networking, distributed and concurrent programming, semi-realtime software systems, algorithm and protocol design
<i>Pankade Kaardikeskuse AS</i>	1998–2005	Computer Engineer, PANKADE KAARDIKESKUS — Tallinn	Evolved from network manager to lead software engineer over time and got involved in nation-wide payment network redesign efforts. This company is today known as Nets Estonia. Competencies: UNIX/Linux, C/C++, Java, Windows, protocol design, standard development, data security
<i>Spin TEK AS</i>	1992–1998	Computer Technician, SPIN TEK — Tallinn	Part-time job, consisted mostly of computer and network repair and management. Competencies: Windows, Linux, Novell Netware, IP and IPX networking

PUBLICATIONS

<i>Estonian Information System Authority, 2021</i>		Cryptographic algorithms, their lifecycle and software support.	Authors: Mart Oruaas, Aivo Kalu, Jaak Pruulmann-Vengerfeldt, Kristjan Kriips, Jan Willemson
<i>Keynote paper at Baltic DB&IS 2020</i>		Developing requirements for the new encryption mechanisms in the Estonian eID infrastructure.	Authors: Mart Oruaas, Jan Willemson
<i>Cybernetica AS, 2018</i>		European Patent EP3529948B1 – Composite Digital Signatures.	Authors: Ahto Buldas, Aivo Kalu, Peeter Laud, Mart Oruaas
<i>ESORICS 2017</i>		Server-Supported RSA Signatures for Mobile Devices.	Authors: Ahto Buldas, Aivo Kalu, Peeter Laud, Mart Oruaas
<i>Estonian National Electoral Committee, 2003</i>		Security Analysis of a Proposed E-voting System	E-hääletamise kontseptsiooni turve: analüüs ja meetmed, EH-02-01. Authors: Arne Ansper, Ahto Buldas, Mart Oruaas, Jaan Priisalu, Anto Veldre, Jan Willemson, Kaur Virunurm

OTHER INFORMATION

<i>Awards</i>	2018 · Employee of the Year of Cybernetica AS
	2015 · Amazing Newcomer award of Cybernetica AS
	2005-2012 · Multiple collegiate awards of Skype Technologies Ltd.
<i>Languages</i>	ESTONIAN · Mother tongue
	ENGLISH · Fluent in everyday and professional use
	RUSSIAN · Basic

April 7, 2021