INFOTEHNOLOOGIA TEADUSKOND
ARVUTITEADUSE INSTITUUT
TEADUS- JA ARENDUSTEGEVUSE AASTAARUANNE 2014

1. Struktuur

Arvutiteaduse instituut / Department of Computer Science
Direktor Jüri Vain

- **Õppetoolid**:
  - Üldinformaatika õppetool/ Chair of General Informatics, juhataja Jüri Vain
  - Teoreetilise informaatika õppetool/ Chair of Theoretical Informatics, juhataja Tarmo Uustalu
  - Võrgutarkvara õppetool/ Chair of Network Software, juhataja Tanel Tammet
  - TTÜ küberkriminalistika ja küberjulgeoleku keskus/ TUT Centre for Digital Forensics and Cyber Security, juhataja Rain Ottis

2. Teadus- ja arendustegevuse (edaspidi T&A) iseloomustus

2.1 Struktuuriüksusesse kuuluvad uurimisgrupid

1. Uurimisgrupp:
Formaalmeetodite põhine analüüs, verifitseerimine ja planeerimine
Formal methods based analysis, verification and planning
Uurimisgrupi juht: Jüri Vain

Uurimisgrupi teadustöö kirjeldus

Main research activities of the group are focused on the development and application of formal methods (model checking, SMT constraint solving, abstraction refinement, automated reasoning and semantic data mining) for model-based development of distributed cyber physical systems and also social media and crowd-sourced information systems. The studies of the group involve following problem groups:

Satisfiability Modulo Theories (SMT) based *test generation of reactive planning on-line testers* for non-deterministic systems has been the domain where group has introduced new concepts and shown their practical feasibility. SMT based diagnosis of faults in autonomous underwater vehicles (AUV) is a joint research topic with Birmingham University group. Research on correct-by-construction software development methods using refinement transformations is performed in collaboration with Abo Akademi University group. Specifically, the applicability of model refinement transformations for synthesis of software systems with real-time constraints is studied.

Second group of problems that are related to *model transformations* is aspect-oriented (AO) modelling. The topic that has grown out from the ideas of AO programming recently is new in the formal modelling domain and addresses the main obstacle in the use of formal modelling - complexity. This is joint research with Abo Akademi University group.

Research on *simulation modelling and analysis of time jittering* in cyber physical systems has been started in collaboration with university of Sannio (Italy) and Kharkov University of Avionics. Combining numeric simulation techniques with timing model checking has shown promising results in several industrial case studies (published in IEEE 25th International Symposium on Software Reliability Engineering Workshops ISSREW 2014, 3-6 November 2014, Naples, Italy).

Research on m*odelling and analysis of human motions* is spanned around the application of Motion Mass parameters (set of parameters describing amount and smoothness of the human limbs motions) to the different problems of psychology and medicine. In cooperation with the Psychology Institute of Tallinn University, the influence of the human arousal level on the motor functions has been studied. The recent experimental results have verified that the influence of the arousal level on the motion mass may be described by linear function. It was also demonstrated that magnitude of the influence depends on stimuli type. In cooperation with the neurology clinic of Tartu University Hospital evolution of the motion mass parameters for Parkinson Disease patients is investigated. Initial results here indicate that the motion mass parameters differ significantly between the patients and a control group of healthy individuals of the same age. Results obtained, clearly demonstrate that the notion of Motion Mass, proposed in cooperation with Psychology Institute is applicable to solve problems arising in medicine and psychology and justify further research in those directions

The group is focusing also on the applied research in the field of *semantic web, big data and cyber security.* All these research areas are investigated by combining theoretical investigations with practical experimentation with the implementations: semantic analysis, classification and deduplication of tourism objects worldwide; in-memory databases with an integrated reasoner and applications in impact analysis for database systems; security issues of cyber space and semantic analysis of cyber threats. The research here is relatively new and focuses on two interconnected areas: first, developing algorithms for rule-based analysis of large datasets, with experimental work focusing on building an efficient in-memory database with an integrated reasoning engine: see http://whitedb.org. Second, developing algorithms for analysing data lineage and impact in large real-life database systems: see http://dlineage.org.

Uurimisgrupi aruandeaastal saadud tähtsamad teadustulemused *(inglise keeles)*:

- An aspect-oriented method for modelbased testing using UPPAAL timed automata (UPTA) with the focus on providing a rigorous constructive approach supported by modelling and test automation tool support. Our approach provides two contributions: a) it allows for decoupling the design of different aspects of the system, then it uses a set of explicit composition patterns to weave the aspects together; b) it defines a set of coverage criteria for aspect-oriented UPTA models which allows one to generate tests for testing aspects individually or for testing the interference between aspects. In both cases, we define precise semantics for the composition and, respectively, for the test generation process [1].
- The methodology of proving correctness of tests for remote testing of systems with time constraints has been developed. To demonstrate the feasibility of the approach we show how the abstract conformance tests are generated, verified and made practically executable on distributed modelbased testing platform dTron [2].
- Presence of the linear dependence between the arousal level and state of motor functions has been proven experimentally. Significant difference of the values of motion mass parameters between the PD patients and healthy individuals has been shown [3].
- We proposed to use jitter bounds on Networked automation systems (NAS) and the technical process to study the timing performance. Using the jitter model, the timing performance is verified using tools from model checking. The investigation also proposes a work-flow to study the timing performance of NAS using jitter analysis. Finally, the work-flow is illustrated using suitable industrial examples. Results indicate that the method can be used effectively during the design and verification stage to verify timing performance before deployment [4].
- Semantic analyses has been performed and used for creating popular visualization tools (see http://sightsmap.com) for large crowd-sourced, geotagged world-wide datasets created by a large number of individuals: Panoramio photoset (used for photos on Google maps), Foursquare (recording visits to places) and a geotagged subset of Wikipedia. Also highly efficient prover database infrastructure http://whitedb.org suitable for parallel processing of large data sets in shared memory has been included into mainstream Linux distros like Debian and Ubuntu. A system http://dlineage.com for automatic rule- and semantic-based impact analysis in DB systems for Business Intelligence and Data Warehouse services, planning and change management has been built with industry cooperation (ELIKO,

Mindworks). It is in pilot use in a large bank and a large utilities company [5].

Olulisemad publikatsioonid.

1. D. Truscan, J. Vain, M. Koskinen (2014). Combining aspect-orientation and UPPAAL timed automata. *In: Proceedings of the 9th International Conference on Software Paradigm Trends : 2014. Aug 29, 2014 - Aug 31, 2014 Vienna, Austria: (Toim.) Holzinger, Andreas; Cardoso, Jorge; Cordeiro, José; van Sinderen, Marten; Mellor, Stephen.* SciTePress, 2014, 159 - 164.
2. J. Vain, A. Anier, E. Halling. Provably correct test generation for online testing of timed systems. In H.-M. Haav, A. Kalja, T. Robal, eds. Databases and Information Systems VIII, Frontiers in Artificial Intelligence, IOS Press.
3. Nomm, S.; Kõnnusaar, T.; Toomela, A. (2014). Towards Establishing Relationships Between Human Arousal Level and Motion Mass. In: Neural Information Processing: 21th International Conference, ICONIP 2014, Kuching, Sarawak, Malasya, November 3-6, 2014. (Eds.) Loo, C.K., Keem Siah, Y., Wong, K.K.W., Beng Jin, A.T., Huang, K.. Springer, 2014, (Lecture Notes in Computer Science/Theoretical Computer Science and General Issues; 8834), 19 – 26
4. Srinivasan, Seshadhri; Buonopane, Furio; Ramaswamy, Srini; Vain, Jüri (2014). Verifying response times in networked automation systems using jitter bounds. *In: IEEE 25th International Symposium on Software Reliability Engineering Workshops [ISSREW 2014] : 3-6 November 2014, Naples, Italy, Proceedings:* Piscataway: IEEE, 2014, 47 - 50.
5. Tomingas, K.; Tammet, T.; Kliimask, M. (2014). Rule-Based Impact Analysis for Enterprise Business Intelligence. In: Artificial Intelligence Applications and Innovations; AIAI 2014 Workshops: CoPA, MHDW, IIVC, and MT4BD.: AIAI 2014; Rhodes, Greece, September 19–21, 2014.. Springer, 2014, (IFIP Advances in Information and Communication Technology; 437), 301 - 309.

Küberturve ja küberkriminalistika
Cyber Security and Digital Forensics
Uurimisgrupi juht: Olaf Maennel

Description of research:
The main effort in 2014 went into establishing the research group and forming the TUT Centre for Digital Forensics and Cyber Security. More specific research has been done on following topics:
Serious games in cyber security. This research stream explores serious games in cyber security education and experimentation. Specifically, we focus on technical cyber security exercises (Locked Shields series) and tabletop exercises.
Network security. This research stream focuses on network monitoring, measuring and situational awareness also on collecting and reporting security metrics from massive event streams in industrial environments. During this research, we experimented with novel noSQL database technologies and combined them with our existing event correlation and anomaly detection frameworks. In the field of network measurements we studied challenges of network routing forensics and developed a tool that is able to assist operators in detecting problematic routing conditions. This tool is pubic as a community service and is being used widely. We also worked with Cisco on a configuration emulation platform named VIRL. This tool uses auto-configuration research to setup medium-scale core-network infrastructure labs. The Cisco made this toolset public at the end of 2014.

Uurimisgrupi aruandeaastal saadud tähtsamad teadustulemused
In 2014, one of the research topics was collecting and reporting security metrics from massive event streams in industrial environments. During this research, we experimented with novel noSQL database technologies and combined them with our existing event correlation and

anomaly detection frameworks. We have published our four-year experience of using tabletop exercises in cyber security Master's education.
Our industrial research results on collecting and reporting security metrics were published as a paper in IEEE MILCOM 2014. We were able to put our research efforts into an official Internet Standard (IETF RFC 7196), as well as assist Cisco to turn our research into a commercial product (Cisco VIRL). The work was published as research work in 2011 in the 12th international Conference on Passive and Active Measurement (PAM). It was then adopted as an official industry recommendation (RIPE ripe-580) in January 2013. In May 2014 it became an official Internet Standard "Cristel Pelsser, Randy Bush, Keyur Patel, Pradosh Mohapatra, Olaf Maennel. "Route Flap Damping Made Usable". Internet Engineering Task Force (IETF) RFC 7196, May 2014.

Publications:

[1] Ottis, Rain. (2014). Light Weight Tabletop Exercise for Cybersecurity Education. Journal of Homeland Security and Emergency Management, 11(4), 579 - 592.
[2] Vaarandi, Risto; Pihelgas, Mauno (2014). Using Security Logs for Collecting and Reporting Technical Security Metrics. *In: Proceedings of the 2014 IEEE Military Communications Conference:* IEEE, 2014, 294 - 299.
[3] Nejc Škoberne, Olaf Maennel, Iain Phillips, Randy Bush, Jan Zorz, and Mojca Ciglaric. 2014. IPv4 address sharing mechanism classification and tradeoff analysis. IEEE/ACM Trans. Netw. 22, 2 (April 2014), 391-404. (DOI: 10.1109/TNET.2013.2256147)
[4] Andra Lutu, Marcelo Bagnulo, Jesus Cid-Sueiro, Olaf Maennel. "Separating Wheat from Chaff: Winnowing Unintended Prefixes using Machine Learning". In Proceedings of IEEE Infocom, Toronto, Canada, April, 2014. (DOI: 10.1109/infocom.2014.6848023)
[5] Andra Lutu, Marcelo Bagnulo, Cristel Pelsser, Olaf Maennel. "Understanding the Reachability of IPv6 Limited Visibility Prefixes". In Proceedings of 15th Passive and Active Measurement Conference (PAM 2014), Los Angeles, USA, March, 2014. (DOI: 10.1007/978-3-319-04918-2_16)