Research Program 8 in 2014: Overview

Lukáš Sekanina
Brno University of Technology
Faculty of Information Technology
sekanina@fit.vutbr.cz

Secure and Safe Architectures, Networks and Protocols

We are focusing on reliability and enhancing security of the information technology. The research is mainly focused on secure and reliable computing architectures, networks and protocols for both regular and embedded systems.

Secure and Safe Architectures, Networks and Protocols

Information services
Supercomputing services
Research programs
About us
Contact

From our portfolio —
RP8: Secure and safe architectures, networks and protocols

- Develop and apply new methods of modeling, design, optimization, diagnostics, validation and verification for modern secure and reliable HW-SW systems (including networks and protocols).

**Theorem 2.** For all $q, r \in Q$, we have $q \preceq_b r$ if and only if $q^O \preceq r^O$.

**Proof.** (If) We define $\preceq$ to be a binary relation on $Q$ such that $q \preceq r$ if and only if $q^O \preceq r^O$. We immediately imply the result.

Suppose that $p \preceq r$ and $p' \xrightarrow{a} (p) \cup P$ where $p \notin P$ is since $p' \xrightarrow{a} (p) \cup P$ is a transition of $A$, we know that $\preceq$ is a binary relation on $A^O$. Since $\preceq$ is a simulation, we can find two $(p', a, P)^O \preceq (r', a, R)^O$ and $p'^O \preceq r'^O$. From $p'^O \preceq r'^O$, $(p', r')$, we have $p' \preceq r'$ and $P \preceq R$. It follows that $\preceq$ is in fact a binary relation on $A^O$.

(Only if) Define $\preceq$ as a binary relation on $Q^O$ such that $p \preceq r$. By definition, $\preceq \subseteq I$. We show that $\preceq$ is a simulation.

Suppose that $p'^O \preceq r'^O$ and the transition $p'^O \xrightarrow{(p', a, P)} r'^O$ and by definition of $A^O$, a transition $r'^O \xrightarrow{a} (r', a, R)^O$ in $A$ such that $(p', a, P)^O \preceq (r', a, R)^O$.

Suppose that $(p, a, P)^O \preceq (r, a, R)^O$ and the transition know that $P \preceq R$ and $p \preceq r$. By definition of $A^O$, the $p'^O \preceq r'^O$. Together we have there exists a transition $(r, a, P)^O$. By definition of $Q^O$, $p'^O \preceq r'^O$. □
Security of multi-agent systems, wireless networks and biometric systems (doc. Hanáček)

Embedded systems, networks and protocols (prof. Švéda)
- 17:10 Ryšavý O.: Fast RTP Detection and Codecs Classification in Internet Traffic

Computer architectures and diagnostics (doc. Kotásek)

HW/SW co-design (prof. Hruška)

Evolvable hardware (prof. Sekanina)

Modelling and simulations of systems (doc. Janoušek)
- 17:30 Janoušek V.: Enabling Dynamic Reconfigurability of Distributed Control Systems Using Reference Nets

Automatic verification (prof. Vojnar)
New journal papers (JIF)


- Dobai R., Sekanina L.: Low-Level Flexible Architecture with Hybrid Reconfiguration for Evolvable Hardware. *ACM Transactions on Reconfigurable Technology and Systems*. in press (IF = 0.408)
New technology

- FPGA-based platform enabling monitoring (e.g. precise packet filtering) of 100 Gbs networks (RP8 Milestone)

- Tools for rapid development of application-specific processors
  - processor
  - compiler (RP8 Milestone)
  - decompiler
Milestones 2014

- Implementation and verification of countermeasures against attacks on multi-agent systems, wireless networks, and biometric systems. (6/2014)
- Method and implementation of software for automated creation of a compiler of higher programming language for usage in reliable HW-SW systems. (6/2014)
- Completion of a platform on the basis of FPGA for networks up to the speed of 100 Gb/s, which will enable realization of various security applications. (11/2014)
Awards and Recognition

- Kurt Gödel Medal from the FLoC Olympic Games 2014 (Vienna)
  - Dudka K., Peringer P., Vojnar T.
  - The Predator tool for automated shape analysis of programs with dynamic linked data structures has been awarded for its successes in three consecutive years of the international competition in software verification SV-COMP.

- Best Paper Award at KTTO 2014 (Ostrava)
  - Basel M., Kmeť M., Matoušek P.: On-line Monitoring of VoIP Quality Using IPFIX

- Best PhD student award at Int. Joint Conf. on e-Business and Telecommunications (ICETE 2014 Doctoral Consortium)
  - POLČÁK Libor. Challenges in Identification in Future Computer Networks
New research projects starting in 2014

- **FP7**

- **COST, Aktion, Tempus**
  - New solutions for multimodal biometrics - enhancement of security and reliability of biometric technologies (COST, doc. Drahanský)
  - Automatic Analysis and Verification of Transactional Memories (COST, Prof. Vojnar)
  - Centers of Excellence for young RESearchers (TEMPUS, doc. Drahanský)

- **Czech Science Foundation**
  - Automatic Formal Analysis and Verification of Programs with Complex Unbounded Data and Control Structures (prof. Vojnar)
  - Advanced Methods for Evolutionary Design of Complex Digital Circuits (prof. Sekanina)
## Selected indicators for 2014

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Promised</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>J with IF</td>
<td>3</td>
<td>1 + 3 in press</td>
</tr>
<tr>
<td>Other publications</td>
<td>15</td>
<td>&gt;20</td>
</tr>
<tr>
<td>Patents</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SW</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Contractual research</td>
<td>3.5 M CZK</td>
<td>3.159 M CZK + RP7</td>
</tr>
<tr>
<td>National grants</td>
<td>10 M CZK</td>
<td>6.54 M CZK + RP7</td>
</tr>
<tr>
<td>International grants</td>
<td>8.1 M CZK</td>
<td>2.131 M CZK + RP7</td>
</tr>
</tbody>
</table>
Thank you for your attention!

Lukáš Sekanina
Brno University of Technology
Faculty of Information Technology
sekanina@fit.vutbr.cz