JOHANNES KEPLER
UNIVERSITY LINZ

Ph.D. Position

Engineering and Composing Safe and Secure Cyber Physical Systems

Institute of Software Systems Engineering
Johannes Kepler University, Linz, Austria

The big picture:

In the era of Internet of Things (IoT) and Cyber Physical Systems (CPS), systems are composed of parts and these parts need to communicate with each other – even if these parts were developed by different companies and for different purposes. On the one hand, composing parts into systems has the chance to greatly simplify the building of such systems. On the other hand, more complexity has to go into the engineering of their parts. How the composing of parts affects the safety, security, and correctness of such systems remains an unsolved problem. After all, systems can be safe, secure, and correct only if its parts are safe, secure, and correct. However, safe, secure, and correct parts do not guarantee safe, secure, and correct systems because the manner in which the parts are composed affects this.

The goal and research questions:

The goal of this thesis is to better understand safety, security, and correctness implications of parts vs. the whole system[1]. This is complicated by the fact that parts are often based on legacy code and need to be understood and enhanced. The focus is on safety and security primarily and correctness by implication. We want to develop methods and techniques for detecting and consequently removing safety concerns and security vulnerabilities in code. Since, concerns and vulnerabilities in code can lead to huge damages when exploited (e.g., through XSS attacks to obtain confidential information or injuries in case of machinery), it is important that software parts are bug-free and correctly implement safety and security considerations. Apart from vulnerabilities, we also need to consider possible threats or attacks (e.g., buffer overflows and canonicalization attacks) and have to come up with some countermeasures to deal with such situations.

Another challenge is that CPS are built by many stakeholders collaborating with each other through diverse engineering (e.g., requirements models, design documents and code). This is where the DesignSpace[2] helps as it allows the artifacts from different engineering tools[2] to be connected. In this context, we also want to extend the notion of safety and security. For example, how to detect and fix vulnerabilities in code while making sure that all the related artifacts remain harmonious after the changes. Or how to resolve vulnerabilities if the information needed for detecting them is spread across multiple engineering tools?

Research methods:

Techniques that this position could focus on include program analysis (e.g., static analysis), verification (e.g., dynamic analysis), software testing, model learning, etc. Among the goals is to significantly extend

[1] Miklós Biró, Atif Mashkoor, Johannes Sametinger, Remzi Seker: Software Safety and Security Risk Mitigation in Cyber-physical Systems. IEEE Software 35(1): 24-29 (2018)

[2] Andreas Demuth, Markus Riedl-Ehrenleitner, Alexander Nöhrer, Peter Hehenberger, Klaus Zeman, Alexander Egyed: DesignSpace: An Infrastructure for Multi-user/multi-tool Engineering. SAC 2015: 1486-1491

[2] Andreas Demuth, Roland Kretschmer, Alexander Egyed, Davy Maes: Introducing Traceability and Consistency Checking for Change Impact Analysis across Engineering Tools in an Automation Solution Company: An Experience Report. ICSME 2016: 529-538

the power and scalability of such techniques to real-world code bases; in particular, we will exploit the DesignSpace as an underlying collaborative engineering platform since we believe that safety and security analysis is also a collaborative effort that may involve multiple engineers.

Required expertise:

- A Master's degree in computer science or a closely related discipline
- Strong programming skills (for example in Java, C++, or C#)
- Ability to work on own initiative and also as a part of a team
- English language proficiency, written and spoken

Application Instructions:

Applications should include a cover letter, CV, preferably also letters of reference, and a brief statement describing the applicant's research motivation in relationship to this topic. Electronic submissions are required. Review of applications will begin immediately and continue until suitable candidates are appointed.

Contact:

- Prof. Dr. Alexander Egyed (alexander.egyed@jku.at)
- Dr. Atif Mashkoor (atif.mashkoor@jku.at)

About the Institution:

The JKU Institute for Software Systems Engineering is a 30+ people strong research institute that is ranked among the best in the world (e.g., recently Microsoft ranked JKU 16th in the world in software engineering). Research at the institute covers a wide area of software engineering from requirements to capture software, systems architecture, design and testing, to maintenance. Engineering is an inherently creative process that requires rigorous attention to details. However, engineering is also a collaborative, human centric process with adhoc activities. Engineering automations are few and rare – not just during programming but also during modeling, testing or maintenance.

About the Advisor:

Prof. Dr. Egyed received his Doctorate from the University of Southern California, USA and previously worked at Teknowledge Corporation, USA and the University College London, UK. He is most recognized

for his work on software and systems design – particularly on variability, consistency, and traceability. Dr. Egyed has published over 200 refereed scientific books, journals, and conferences with over 6000 citations to date. He was recognized a Top 1% scholar in software engineering in Communications of the ACM, Springer Scientometrics, and Microsoft Academic Search. He was also named an IBM Research Faculty Fellow in recognition to his contributions to consistency checking.

Location: Linz, Austria
Website: http://isse.jku.at/