UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

OBERÖSTERREICH

Special track

AISMS: Adaptivity in Intelligent and Secure Mobile Systems

Marc Kurz, Erik Sonnleitner

Adaptive 2022 | April 2022

marc.kurz@fh-hagenberg.at | erik.sonnleitner@fh-hagenberg.at

HAGENBERG | LINZ | STEYR | WELS

IARIA

Contact

Prof. Dr. Marc Kurz
Professor for Mobile Software Systems
Univ. of Applied Sciences Upper Austria
Department of Mobility & Energy
Campus Hagenberg, Austria
marc.kurz@fh-hagenberg.at

Research Interests
- Distributed & Autonomic Computing
- Mobile Software Systems & Frameworks
- Adaptive & Self-Adaptive Systems
- Activity & Context Recognition
- Internet of Things

Prof. Dr. Erik Sonnleitner
Professor for Secure Mobile Systems
Univ. of Applied Sciences Upper Austria
Department of Mobility & Energy
Campus Hagenberg, Austria
erik.sonnleitner@fh-hagenberg.at

Research Interests
- Mobile device security
- System security & exploitation
- Blockchains & distributed ledger technology
- Web security
- Steganography & information hiding
- Forensics

@MC.AC.ENI.fhooe

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

AISMS Special Track :: Summary

*By applying approaches that can be classified within the topic "**artificial intelligence**", mobile systems strive to provide some kind of "**intelligent behavior**" adapting to the **current user's contextual state**. Additionally, security aspects concerning **personal and sensitive data** are becoming more and more relevant.*

*These two important factors might be diametrically opposed, since usually "intelligence" needs a lot of data to sense the current context of users, but data might be sensitive in terms of privacy and security concerns. Nevertheless, **security in mobile systems** needs to be considered as a critical factor.*

*Therefore, this special track aims at **discussing the hybridity of intelligence and security** with respect to the (self-) adaptation of mobile systems according to the actual contextual state.*

AISMS Special Track :: Topics of Interests

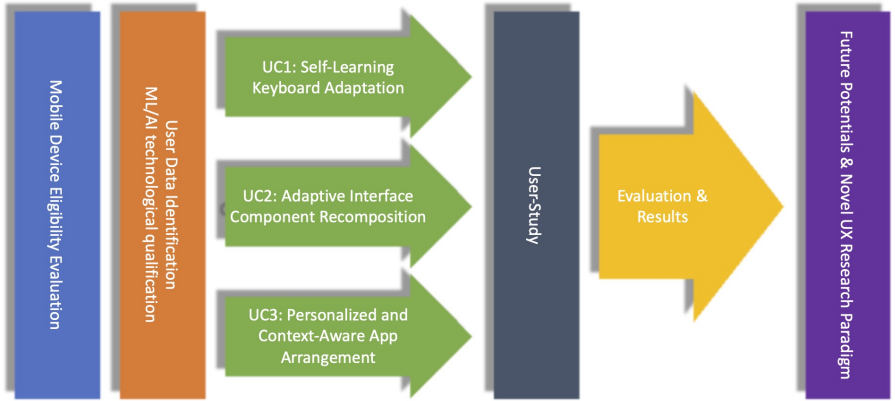
- Artificial Intelligence
- Ambient Intelligence
- Security aspects for mobile systems
- Internet of Things (IoT)
- Adaptive behavior of mobile systems
- Adaptive behavior of mobile sports & health systems
- Adaptive and self-adaptive behavior
- Adaptivity in wearable and mobile systems
- Self-adaptation in mobile environments
- Context-awareness and context-aware adaptation
- Adaptive artificial intelligence
- Privacy and Security in mobile adaptive systems

Summary of Contributions 1/3

Title MeUI - Machine Learning Enhanced Adaptive User Interaction
Authors Marc Kurz, Erik Sonnleitner

- reverse the core principle of device utilization by providing a distinct, personalized and dynamically self-adaptive foundation towards modern **human computer interaction**

- Hypothesis: *ML/AI technologies allow for a significant change in the (mobile) device interaction in terms of usability. The classic approach of one-size-fits-all approach can be reversed towards a personalized experienced and a self-learning adaptation of interaction increasing the user experience.*



Summary of Contributions 2/3

Title Tree-Based Regressors for Predicting Energy Expenditure from Heart Rate in Wearable Devices

Authors Stephan Selinger, Luka Dimitrijevic

- estimate energy expenditure from heart rate with a higher coefficient of determination using tree-based regressors than commonly used linear models
- data from 892 graded exercise tests; trained various models and selected one which not only performed better than the linear model

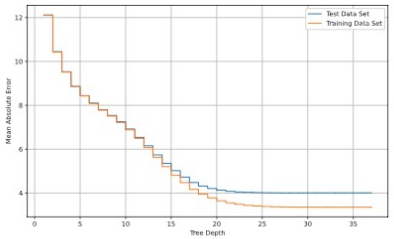


Figure 1. Tree depth vs. mean absolute error.

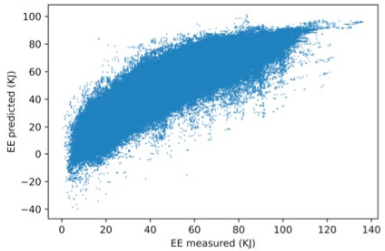


Figure 2. EE vs. predicted EE by LM_2.

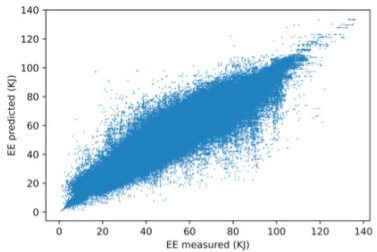


Figure 3. EE vs. predicted EE by DT_1.

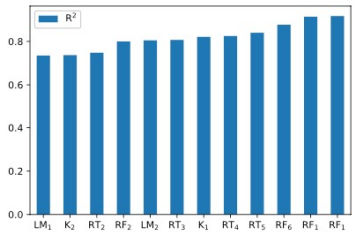


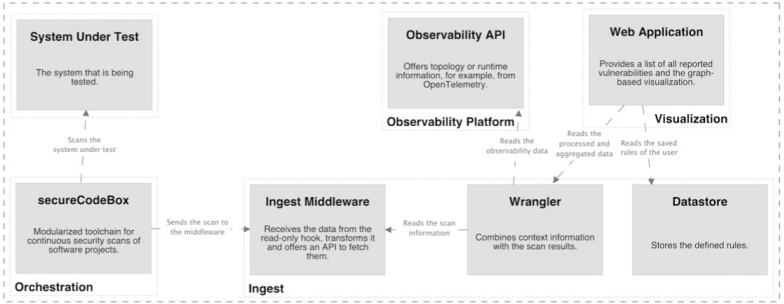
Figure 4. Coefficients of determination.

Summary of Contributions 3/3

Title Context-Aware Security Intelligence of Vulnerability Scanners in Cloud-native Environments

Authors Simon Ammer, Jens Krösche, Markus Gierlinger, Mario Kahlhofer

- reduce false positives of scanners in a cloud environment by utilizing contextual information
- an architecture to combine scanner results and topology information is proposed, and a prototype called **Themis** with a rule-based filtering approach and graph-based visualization of found vulnerabilities is presented.



Future Challenges

- Focusing more on the aspect regarding **“intelligence” vs “security”**
  - > Are those two aspects really diametrically opposed?

- Discussing different machine learning models in terms of data, security and adaptivity
  - > Also considering “**deep learning**”, “**neural networks**” and other novel approaches

- Developing/collecting comprehensive **datasets**
  - > How much data needed?
  - > How should this data be efficiently annotated?

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

OBERÖSTERREICH

Special track

AISMS: Adaptivity in Intelligent and Secure Mobile Systems

Marc Kurz, Erik Sonnleitner

Adaptive 2022 | April 2022

marc.kurz@fh-hagenberg.at | erik.sonnleitner@fh-hagenberg.at

HAGENBERG | LINZ | STEYR | WELS

IARIA