Workshop program

Date: Friday, 21st April **Venue:** Faculty of Computer Science, TU Dresden Room # 1004, Andreas-Pfitzmann-Bau (APB)	
0730 hrs - 0800 hrs	**Registration**
0800 hrs - 0830 hrs	**Resilience path overview** **Leaders:** Thorsten Strufe and Akash Kumar
Session I: Software systems (Chair: Pramod Bhatotia)	
0830 hrs - 0915 hrs	**Keynote # 1:** Baris Kasikci (Microsoft Research) *Title: Stamping out concurrency bugs*
0915 hrs - 1015 hrs	**Student talks** ● Dmitrii Kuvaiskii *Title: Dependable Systems Leveraging new ISA extensions* ● Matthias Hille *Title: A Scalable and Resilient OS for Heterogeneous Architectures* ● Till Kolditz *Title: Detecting Multi-Bit Flips In Databases*
1015 hrs - 1100 hrs	**Poster session # 1** (and coffee break)
Session II: Hardware architecture (Chair: Akash Kumar)	
1100 hrs - 1145 hrs	**Keynote # 2:** David Atienza (EPFL) *Title: Design of Energy-Efficient and Reliable Wearable Systems for the Internet-of-Things Era*
1145 hrs - 1230 hrs	**Keynote # 3:** Ahmad-Reza Sadeghi (TU Darmstadt) *Title: Everything You Code Can and Will be Re-used Against You: On the Challenges of Mitigating Code-Reuse Exploits*
1230 hrs - 1400 hrs	**Lunch**
Session III: Embedded systems (Chair: Marco Zimmerling)	
1400 hrs - 1445 hrs	**Keynote # 4:** Kay Roemer (TU Graz) *Title: Dependable Internet of Things*
1445 hrs - 1545 hrs	**Student talks** ● Sadia Moriam *Title: Fault-Resilient Network-on-Chip (NoC) for Many Core Systems* ● Fabian Mager *Title: Exploiting Network Coding for Resilient, Low-latency Communication in Multi-hop Low-power Wireless Networks* ● Andreas Dixius *Title: On-Chip Timing-Detection*

1545 hrs - 1630 hrs	**Poster session # 2** (and coffee break)
Session IV: System security (Chair: Thorsten Strufe)	
1630 hrs - 1715 hrs	**Keynote # 5:** Onur Mutlu (ETH Zurich) *Title: The RowHammer Problem and Other Issues We May Face as Memory Becomes Denser*
1715 hrs - 1800 hrs	**Concluding remarks and discussion**

Keynote talks

Speaker	Title and abstract
 **David Atienza** **(EPFL)** **Webpage:** https://people.epfl.ch/david.atienza **Email:** david.atienza@epfl.ch **Bio:** David Atienza is Associate Professor of Electrical and Computer Engineering and Director of the Embedded Systems Laboratory (ESL) at EPFL, Switzerland. He received his MSc and PhD degrees in Computer Science and Engineering from UCM (Spain) and IMEC (Belgium). His research interests focus on system-level design methodologies for energy-efficient multi-processor system-on-chip architectures (MPSoC) and next-generation embedded systems. In these fields, he is co-author of more than 250 publications, seven patents, and received several best paper awards in top conferences. He also was the Technical Program Chair of DATE 2015 and General Chair of DATE 2017. He received an ERC Consolidator Grant in 2016, the IEEE CEDA Early Career Award in 2013, the ACM SIGDA Outstanding New Faculty Award in 2012, and a Faculty Award from Sun Labs at Oracle in 2011. He was Distinguished Lecturer of IEEE CASS in 2014 and 2015. He is a senior member of ACM and an IEEE Fellow.	**Title:** Design of Energy-Efficient and Reliable Wearable Systems for the Internet-of-Things Era **Abstract:** The evolution of semiconductor process technologies has enabled the design of low cost, compact and high-performance wearable embedded systems. These new wearable systems are computing platforms with multi-processor system-on-chip (MPSoC) architectures that can be deployed ubiquitously, and can potentially provide computing capacity for real-time analysis of human bio-signals to continue the progress of our society in the new era of Internet-of-Things (IoT). However, the inherent resource-constrained nature of wearable embedded systems, coupled with the power requirements of MPSoC architectures, can result in degraded performance and unreliable behavior, or a global energy crisis if they are massively deployed in the IoT era. Therefore, in this talk I will show the impact of potential hardware misbehavior induced by reliability issues and scaled voltages in MPSoC wearables nodes. Then, I will advocate that the inherent resilience of latest algorithms in wearable bio-signals monitoring, as well as a better understanding how living organisms operate, can allow us to conceive new cross-layer design paradigms for the next-generation of energy-efficient and reliable wearable systems in the IoT era. This new approach exploits more on-board intelligence, hardware specialization and the selective application of different robust techniques to gracefully scale the energy consumption of wearable MPSoC architectures according to the required output quality for the target biomedical application.

Baris Kasikci
(Microsoft Research & University of Michigan)

Webpage: http://www.bariskasikci.org/
Email: barisk@microsoft.com

Bio: Baris Kasikci is a researcher at the Systems and Networking Group at Microsoft Research Cambridge, and he will start as an assistant professor of Computer Science and Engineering at the University of Michigan this Fall. His research is centered around developing techniques, tools, and environments that help developers build more reliable and secure software. He is interested in finding solutions that allow programmers to better reason about their code, and that efficiently detect bugs, classify them, and diagnose their root cause. He is also interested in in system support for emerging hardware platforms, efficient runtime instrumentation, hardware and runtime support for enhancing system security, and program analysis.

Baris completed his PhD in computer science at EPFL under the supervision of George Candea. He is the recipient of the 2016 Roger Needham PhD Award for the best PhD thesis in computer systems in Europe and the 2016 Patrick Denantes Memorial Prize for best PhD thesis in the Department of Information and Communication Sciences at EPFL. He is also one of the recipients of the VMware 2014-2015 Graduate Fellowship. He previously held roles at VMware, Intel, and Siemens. More details can be found at http://www.bariskasikci.org/.

Title: *Stamping Out Concurrency Bugs*

Abstract: The shift to multi-core architectures in the past ten years pushed developers to write concurrent software to leverage hardware parallelism. The transition to multi-core hardware happened at a more rapid pace than the evolution of associated programming techniques and tools, which made it difficult to write concurrent programs that are both efficient and correct. Failures due to concurrency bugs are often hard to reproduce and fix, and can cause significant losses.

In this talk, I will first give an overview of the techniques we developed for the detection, root cause diagnosis, and classification of concurrency bugs. Then, I will discuss how the techniques we developed have been adopted at Microsoft and Intel. I will then discuss in detail Gist, a technique for the root cause diagnosis of failures. Gist uses hybrid static-dynamic program analysis and gathers information from real user executions to isolate root causes of failures. Gist is highly accurate and efficient, even for failures that rarely occur in production. Finally, I will close by describing some ongoing work we are doing to solve key reliability and performance problems of emerging software systems.

Onur Mutlu
(ETH Zurich)

Webpage: https://people.inf.ethz.ch/omutlu
Email: onur.mutlu@inf.ethz.ch

Bio: Onur Mutlu is a Professor of Computer Science at ETH Zurich. He is also a faculty member at Carnegie Mellon University, where he previously held the William D. and Nancy W. Strecker Early Career Professorship. His current broader research interests are in computer architecture, systems, and bioinformatics. He is especially interested in interactions across domains and between applications, system software, compilers, and microarchitecture, with a major current focus on memory and storage systems. He obtained his PhD and MS in ECE from the University of Texas at Austin and BS degrees in Computer Engineering and Psychology from the University of Michigan, Ann Arbor. His industrial experience spans starting the Computer Architecture Group at Microsoft Research (2006-2009), and various product and research positions at Intel Corporation, Advanced Micro Devices, VMware and Google. He received the inaugural IEEE Computer Society Young Computer Architect Award, the inaugural Intel Early Career Faculty Award, faculty partnership awards from various companies, and a healthy number of best paper or "Top Pick" paper recognitions at various computer systems and architecture venues. His computer architecture course lectures and materials are freely available on YouTube, and his research group makes software artifacts freely available online. For more information, please see his webpage at https://people.inf.ethz.ch/omutlu.

Title: *The RowHammer Problem and Other Issues We May Face as Memory Becomes Denser*

Abstract: We will discuss the RowHammer problem in DRAM and how it poses a new system-wide security vulnerability. RowHammer is the phenomenon that repeatedly accessing a row in a modern DRAM chip causes errors in physically-adjacent rows. It is caused by a hardware failure mechanism called read disturb errors. The Google Zero Project recently demonstrated that this hardware phenomenon can be exploited by user-level programs to gain kernel privileges. Several other recent works work demonstrated other attacks exploiting RowHammer, including remote takeover of a server vulnerable to RowHammer. We will analyze the root causes of the problem and examine solution directions. We will also discuss what other problems may be lurking in DRAM and other types of memories, e.g., NAND flash and Phase Change Memory, which can potentially threaten the foundations of reliable and secure systems, as the memory technologies scale to higher densities.

Kay Roemer
(TU Graz)

Webpage:
https://www.tugraz.at/en/institutes/iti/institute/team/prof-kay-roemer/
Email: roemer@tugraz.at

Bio: Kay Römer is professor at and director of the Institute for Technical Informatics, head of the Field of Expertise "Information, Communication & Computing", and vice dean of the Faculty of Electrical and Information Engineering at TU Graz. He obtained his doctorate in computer science from ETH Zurich in 2005 with a thesis on wireless sensor networks. As a senior researcher, he led the sensor network-related research activities of the Distributed Systems Group at ETH Zurich between 2005 and 2009. From 2009 to 2013 he held a professorship at University of Lübeck in Germany. Kay Römer is an internationally recognized expert on networked embedded systems, with research focus on wireless networking, fundamental services, operating systems, programming models, dependability, testbeds, and deployment methodology. He was the scientific coordinator of the EU FP7 FIRE project RELYonIT on dependable networking in the Internet of Things. He is currently the coordinator of the TU Graz Research Center "Dependable Internet of Things".

Title: *Dependable Internet of Things*

Abstract: Wireless networked embedded systems are increasingly used for safety-critical applications, where even under harsh environmental conditions dependability requirements must be met. In this talk we introduce the Dependable Things research center at TU Graz and present recent results on improving the dependability of wireless communication and localization, embedded computing, and networked control for the Internet of Things.

Ahmad-Reza Sadeghi
(TU Darmstadt)

Webpage:
https://www.trust.informatik.tu-darmstadt.de/people/ahmad-reza-sadeghi/

Email: ahmad.sadeghi@trust.tu-darmstadt.de

Bio: Ahmad-Reza Sadeghi is a full professor of Computer Science at the TU Darmstadt, Germany. He is the head of the Systems Security Lab at the Cybersecurity Research Center of TU Darmstadt. Since January 2012 he is also the director of the Intel Collaborative Research Institute for Secure Computing (ICRI-SC) at TU Darmstadt. He holds a Ph.D. in Computer Science from the University of Saarland, Germany. Prior to academia, he worked in R&D of Telecommunications enterprises, amongst others Ericsson Telecommunications. He has been continuously contributing to security and privacy research. For his influential research on Trusted and Trustworthy Computing he received the renowned German “Karl Heinz Beckurts” award. This award honors excellent scientific achievements with high impact on industrial innovations in Germany.
He is Editor-In-Chief of IEEE Security and Privacy Magazine, and on the editorial board of ACM Books. He served 5 years on the editorial board of the ACM Transactions on Information and System Security (TISSEC), and was guest editor of the IEEE Transactions on Computer-Aided Design (Special Issue on Hardware Security and Trust).

Title: *Everything You Code Can and Will be Re-used Against You: On the Challenges of Mitigating Code-Reuse Exploits*

Abstract: Memory corruption and memory disclosure vulnerabilities are still a persistent source of threats against software systems, although known for over two decades. The main problem is that modern software still contains vast amount of unsafe, legacy code. Moreover, exploitation techniques are rapidly evolving and often incorporate increasingly sophisticated techniques, which can be used to bypass all widely deployed countermeasures such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR). This has recently motivated many researchers in academia and industry to make considerable efforts on improving defenses against modern code-reuse exploits. It seems that there is a strong desire in our community to build secure systems from unsafe code! Hence, many software-hardening solutions have been proposed, some of which are based on hardware support. Recently Intel has released new specification on Control-Flow Enforcement Technology (CET) for x86/x64 to mitigate code-reuse techniques.

However, even though these solutions significantly raise the bar for exploitation, new attacks are continually discovered, and no ultimate solution seems to be in sight.

This talk gives an overview of the continuing arms race between code-reuse attacks and mitigation techniques and their nuances, particularly the hardware-based defenses. We then highlight and discuss the effectiveness and usefulness of recent approaches. The game is not over yet.

Student talks

Student and title	Abstract
• **Dmitrii Kuvaiskii** **Title:** Dependable Systems Leveraging new ISA extensions	**Abstract:** Modern commodity CPUs are equipped with plentiful ISA extensions, e.g., recent Intel processors contain extensions for vector manipulation (AVX), hardware transactional memory (TSX), memory protection (MPX), and secure computation (SGX). Moreover, current CPU microarchitectures provide abundant processing capabilities such as powerful branch predictors, deep pipelines, and out-of-order execution. In this work, we show how to increase software dependability by leveraging CPU extensions, with the focus on software-based fault tolerance and security for legacy C/C++ programs. For fault tolerance, we build techniques to detect CPU faults utilizing unused IPC resources (∆-Encoding project), and Intel TSX (HAFT) and Intel AVX (Elzar) extension sets. For security, we investigate memory safety using Intel MPX and develop a specialized solution for Intel SGX (SGXBounds).
• **Matthias Hille** **Title:** A Scalable and Resilient OS for Heterogeneous Architectures	**Abstract:** Modern architectures are increasingly making use of a large number of heterogeneous computing units such as FPGAs, GPUs, and specialized accelerators. Currently, these computing units are treated as devices without having direct access to OS services such file-systems, networking, memory management, etc. The primary reason for their poor integration is the missing interface to grant them access to system resources while enforcing proper isolation which is done by the MMU on a standard core. In order to manage these computing units we are developing a scalable multikernel based on the M3 operating system. M3 does not require a kernel to be run on computing units, but can control and configure them via a single privileged processing element running a kernel. The goal of our work is to extend the M3 design to a multikernel OS approach to make the OS scalable and resilient against failures. In this talk, I will discuss the extended motivation for our project, and important challenges that we need to address including, resource distribution, naming, load balancing and distributed capability

	management.
• **Till Kolditz** **Title:** Detecting Multi-Bit Flips In Databases	**Abstract:** Modern in-memory database systems leverage the increasing processor performance and memory density of each new hardware generation. Meanwhile, with each technology node, hardware becomes less reliable and database system designers must start considering multi-bit flips as the norm rather than the exception. AN coding has little to moderate impact on the key performance indicators of database systems: query throughput and query latency. In this talk I present the concepts of AN coding and our enhancements, as well as its integration into the query processing layer of database systems.
• **Sadia Moriam** **Title:** Fault-Resilient Network-on-Chip (NoC) for Many Core Systems	**Abstract:** Rapid scaling of transistor gate sizes has significantly increased the density of on-chip integrations and paved the way for many-core systems-on-chip with highly improved performances. The design of the interconnection network for these complex systems is a critical one and the network-on-chip (NoC) is now the predominantly adopted interconnect for such large core arrays. However, the performance enhancements of technology scaling come at the cost of reliability as on-chip components particularly the NoC become increasingly prone to faults. Redundancy is the basic approach to fault tolerance and in this talk, we discuss different approaches toward NoC fault tolerance and their results.
• **Fabian Magar** **Title:** Exploiting Network Coding for Resilient, Low-latency Communication in Multi-hop Low-power Wireless Networks	**Abstract:** Cyber-physical systems (CPS) use distributed feedback loops to control physical processes. Designing practical distributed CPS controllers often benefits from a logically centralized approach, where each node computes the control law locally based on global knowledge of the system state. We present Mixer, an all-to-all communication protocol that enables nodes in a multi-hop low-power wireless network to exchange sizable packets with one another. Mixer harnesses the broadcast nature of the wireless medium and integrates synchronous transmissions with random linear network coding, thereby achieving high resilience against unpredictable packet losses and node failures. Results from real-world experiments demonstrate that Mixer significantly reduces latency compared with the state of the art, while providing similar or higher reliability.

• **Andreas Dixius** **Title:** On-Chip Timing-Detection	**Abstract:** Upcoming technologies will be highly impacted by on-chip device variation, ageing and supply voltage variation. Therefore on-chip timing variations will increase significantly. A full featured set of timing-detection standard cells was designed in a current CMOS technology and can be inserted by a technology independent adapted design flow into any digital design given in a hardware description language during netlist and layout synthesis. Two prototype chips with the developed detector cells in CMOS prove detector functionality and motivate further research.