







Impact of Emerging Hardware on Security and Privacy

Trent Jaeger  | The Pennsylvania State University
Brent ByungHoon Kang  | Korea Advanced Institute of Science and Technology
Nele Mentens  | KU Leuven and Leiden University
Cynthia Sturton  | University of North Carolina

The articles in this special issue focus on ongoing research efforts in the development, use, and evaluation of emerging hardware features and techniques to improve system security. We have seen the emergence of new hardware features to improve software security by limiting memory access within an address space, such as Intel's memory protection keys (MPKs) and extended page table (EPT) switching, among others. Researchers have also proposed hardware-assisted roots of trust using trusted execution environments (TEEs), such as Intel's software guard extensions (SGXs), so some questions are what the utility is of such techniques and what limitations they still face. The papers in this special issue provide guidance in these areas, which can be helpful in examining future research directions and future applications of such techniques.

Recently, we have seen a variety of hardware features released that are designed to improve software security. In the 30 years since the Morris worm, we have found that software-only solutions to prevent memory errors

from being exploited are either too expensive to be deployed broadly or too prone to being circumvented.

This situation has motivated the use of hardware to implement key defensive features more reliably and efficiently. For example, several hardware features have been introduced that provide fine-grained control of access to memory, such as Intel's MPKs and EPT switching. In addition, other hardware features provide TEEs to reduce dependence on complex systems software that may be prone to memory errors, limiting the trusted computing base of systems. Finally, hardware components often provide a fundamental root of trust (RoT) for

systems, but the complexity of such components may result in flaws that would prevent an RoT from achieving its goals.

The introduction of these hardware features is a potential boon for improving system security, but several challenges remain. One challenge is to develop software that utilizes such features effectively to achieve the desired security goals with low overhead. Only then will we be able to see the wide adoption of such hardware necessary to reduce the exploitation of memory errors broadly. However, another challenge is that

We must ensure that the proposed solutions do not also present new vulnerabilities that adversaries can exploit to circumvent security enforcement.

these hardware features may have blind spots that create new exploitable attack surfaces that may require yet more additional defenses. We must ensure that the proposed solutions do not also present new vulnerabilities that adversaries can exploit to circumvent security enforcement.

This special issue collects relevant ongoing research efforts in the security and privacy field concerning the development, use, and evaluation of new hardware features to improve software security.

The first two articles examine the effectiveness of fine-grained memory access control mechanisms. The first article, by Park et al.,^{A1} assesses the MPK hardware feature, identifying challenges in the MPK design and mitigations of several challenges to enable broader usage. The second article, by Narayanan and Burtsev,^{A2} examines EPT switching and the design decisions necessary to ensure isolation is enforced correctly.

The next two articles explore issues in the design and use of hardware roots of trust. First, Meza et al.^{A3} show how to employ information flow analysis on root-of-trust hardware designs to detect and fix real flaws, providing an experience-based discussion of this approach. Second, Lacoste and Lefebvre^{A4} describe the application of TEEs in the telecommunications industry, showing how TEEs may be employed and further challenges to be addressed.

We hope that these articles help inform practitioners how to use these new hardware features and analysis techniques and provide researchers with insights into current capabilities and limitations to investigate future improvements. ■

Trent Jaeger is a professor of computer science and engineering at The Pennsylvania State University, University Park, PA 16802 USA. His research interests include operating systems security, software security, and distributed systems security for a wide variety of application areas. Jaeger received a Ph.D. in computer science and engineering from the University of Michigan. He is a Senior Member of IEEE. Contact him at trj1@psu.edu.

Brent ByungHoon Kang is a professor at the School of Computing, Graduate School of Information

Security, at Korea Advanced Institute of Science and Technology, Daejeon, South Korea. His research interests include systems security, kernel monitoring, hardware-anchored security, dialect computing, and disaggregated system. Kang received a Ph.D. in computer science from University of California at Berkeley. He is a Member of IEEE. Contact him at brentkang@kaist.ac.kr.

Nele Mentens is a professor at Leiden University, 2333 CA Leiden, The Netherlands, and KU Leuven, 3001 Leuven, Belgium. Her research interests include embedded security, hardware security, and configurable computing. Mentens received a Ph.D. in electrical engineering from KU Leuven. She is a Senior Member of IEEE. Contact her at nele.mentens@kuleuven.be.

Cynthia Sturton is an associate professor and Peter Thacher Grauer Scholar at the University of North Carolina at Chapel Hill, Chapel Hill, NC 27599 USA. Her interests include hardware security, formal verification, and hardware design. Sturton received a Ph.D. in computer science from the University of California at Berkeley. She is a Member of IEEE. Contact her at csturton@cs.unc.edu.

Appendix: Related Articles

- A1. S. Park, S. Lee, and T. Kim, "Memory protection keys: Facts, key extension perspectives, and discussions," *IEEE Security Privacy*, vol. 21, no. 3, pp. 8–15, May/June. 2023, doi: 10.1109/MSEC.2023.3250601.
- A2. V. Narayanan and A. Burtsev, "The opportunities and limitations of extended page table switching for fine-grained isolation," *IEEE Security Privacy*, vol. 21, no. 3, pp. 16–26, May/June. 2023, doi: 10.1109/MSEC.2023.3251385.
- A3. A. Meza, F. Restuccia, J. Oberg, D. Rizzo, and R. Kastner, "Security verification of the OpenTitan hardware root of trust," *IEEE Security Privacy*, vol. 21, no. 3, pp. 27–36, May/June. 2023, doi: 10.1109/MSEC.2023.3251954.
- A4. M. Lacoste and V. Lefebvre, "Trusted execution environments for telecoms: Strengths, weaknesses, opportunities, and threats," *IEEE Security Privacy*, vol. 21, no. 3, pp. 37–46, May/June. 2023, doi: 10.1109/MSEC.2023.3259801.