IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Past, Present, and Future

Domenic Forte, Swarup Bhunia, Ramesh Karri, Jim Plusquellic, Mark Tehranipoor

***Abstract*—Hardware plays an integral role in system security with many emerging vulnerabilities and defense mechanisms targeting hardware. The IEEE International Symposium on Hardware Oriented Security and Trust (HOST) aims to facilitate the rapid growth of hardware-based security research and development. Since 2008, HOST has provided an environment to present cutting-edge developments in hardware security and trust. With the recent expansion of its scope to include all areas of overlap between hardware and security, HOST has become a premier event in the field of cybersecurity, and is one of the few to bridge the gap between computer security, microelectronics, and electronic design automation (EDA) communities.**

I. Introduction

Owing to advances in the semiconductor industry and popularity of the Internet, electronic computing and communication systems are ubiquitous today. As society's reliance on them continues to grow, risks to security, privacy, and safety associated with their compromise become more disastrous. Designated as the "root-of-trust", hardware (i.e., ICs, PCBs, and firmware) is the most critical layer to cybersecurity. Unfortunately, countless recent stories highlight that security weaknesses in hardware are pervasive, can be exploited remotely (through software), and are challenging to mitigate.

In January 2018, researchers found two hardware exploits [1], [2] affecting microprocessors from Intel, IBM, and ARM, which allowed adversaries to obtain access to protected memory. Since the issues were related to a microarchitectural feature (speculative execution), they were either un-patchable or patchable with severe impacts on performance. Similar exploits dubbed "microarchitectural data sampling" side channel vulnerabilites are still being uncovered as well as remote fault injection vulnerabilites. The latter abuse physical characteristics of hardware, e.g., DRAM density [3], energy management mechanisms [4], and power distribution networks [5] to escalate privilege, bypass trusted execution environments and secure boots, and recover cryptographic keys.

In parallel, increases in design complexity and changes in economics have forced the electronics industry to rely more heavily on untrusted third parties. Today, 3PIP and commercial-off-the-shelf (COTS) components are regularly integrated into chips and systems. IC and PCB fabrication, testing, and assembly are predominantly performed offshore. Besides semiconductor intellectual property (IP) theft, fears about the integrity of hardware roots-of-trust are mounting. Multiple sources have insinuated that nation states are implanting kill switches and backdoors in ICs and PCBs [6], [7]. Further, counterfeit electronics are a longstanding concern for system safety and the global economy [8].

To address these issues, security must be recognized as a fundamental element to be incorporated into the design, manufacturing, validation, maintenance, and upgrade of hardware for all types of systems. New processes that integrate security and trust into design flows, and add hardware features to enable trusted execution are complex and require a concerted, multidisciplinary effort. To this end, the mission of IEEE Symposium on Hardware Oriented Security and Trust (HOST) [9] is as follows:

- To be a leading and globally recognized forum that unites researchers, practitioners, and users from the computer security, microelectronics, and EDA communities.
- To disseminate cutting-edge ideas, technologies, and results in areas of overlap between hardware and security.
- To provide a platform for leaders in industry, government, and academia to share their unique perspectives and to help shape the direction and priorities of the community.
- To address shortages in the security workforce by recruiting and training students from a diverse group for productive careers with prospective employers.

This paper discusses HOST and how it has evolved into a premiere event in the field of cybersecurity, with significant participation from all sectors of society including academia (50%), industry (30%) and government (20%). Section II describes the history of HOST. Section III summarizes HOST's accomplishments and impacts. Section IV describes the future of HOST, and Section V concludes the paper.

II. History of HOST

A. Workshop Era (2008–2009)

The motivation to start a forum in hardware security and trust began with a collaborative National Science Foundation (NSF) project by co-founders, M. Tehranipoor and J. Plusquellic, in 2007. A government directed Defense Science Report [10] described a serious concern that offshore migration of microelectronic design and fabrication was making it difficult to assure that devices and systems were constructed as specified by their designers. Both co-founders were deeply embedded in the manufacturing test community, and were well positioned to tackle these challenges. Although the DARPA program manager at the time, Dr. D. Collins, referred to the problem as 'change detection', 'hardware Trojan detection' became more widely accepted.

978-1-7281-4823-6/19/$31.00 ©2019 IEEE

In 2008 and 2009, HOST was a 1-day workshop with M. Tehranipoor as General Chair and J. Plusquellic as Program Chair, and was co-located with the Design Automation Conference (DAC). Both workshops consisted of a keynote, several paper sessions, a panel, and a poster session. Dr. D. Collins and P. Kocher from Cryptography Research, Inc. (CRI) served as keynote speakers in 2008 and 2009, resp. Topics of the accepted papers in order of popularity were hardware Trojans, side-channel attacks and countermeasures, physical unlonable functions (PUFs) and cryptography. Both events were successful, and it became clear that HOST should expand into a major venue for professionals and academics to interact on hardware security and trust.

B. DAC Symposium Era (2010–2013)

To accommodate expanding participation and interest, the General Chair, J. Plusquellic, and Program Chair, K. Mai, worked with the sponsors and organizing committee (OC) to convert the 1-day workshop into a 2-day symposium in 2010. The OC, number of submitted papers, and attendees grew significantly, along with the scope of topics covered. The 2-day program allowed 18 papers along with a panel, a poster session, and invited talks by R. Torrance from Chipworks and P. Rohatgi from CRI. The quality of the program improved with the acceptance rate for full papers at approximately 35%.

In 2011 and 2012, K. Mai served as the General Chair. A Vice-Program chair position was created to help with the larger number of submitted papers (48). HOST also reinforced the review process with an online discussion phase. In 2011, P. Schaumont and R. Karri served as Program and Vice Program Chair, respectively. The HOST program consisted of 15 papers and 11 posters across a range of topics, including true random number generation, IP security, run-time security and trust monitors, and architecture level security. The General Chair and OC recruited two industrial sponsors for the first time, and sponsorship of HOST expanded to include the IEEE Computer Society's Test Technology Technical Council (TTTC) and Technical Committee on Security and Privacy (TCSP). In 2012, R. Karri and F. Koushanfar acted as Program and Vice-Program Chairs, respectively. HOST received 52 submissions, of which 16 were accepted as regular papers and 9 as posters. The 2-day program included a keynote speaker, paper sessions, a panel and an industrial paper session for the first time. Topic areas expanded again to include reverse engineering, FIB-based probing attacks, and fault injection.

In 2013, R. Karri was the General Chair, with F. Koushanfar and M. Hsiao as the Program and Vice-Program Chairs. HOST received 62 submissions. 19 were accepted as regular papers and 7 as posters. HOST 2013 continued to expand with three keynote presentations and new topics including obfuscation, trusted boot and CAD tool security. Additional rigor was applied in the review phase.

C. Early Independent Symposium Era (2014–2016)

This era began when HOST separated from DAC to become its own independent event. In 2014, General Chair F. Koushanfar led a move to the DC metropolitan area in order to facilitate interaction with local government agencies. HOST received 65 regular submissions with 18 and 14 accepted as regular and poster papers, resp., with new topics such as split manufacturing, active shield design, and security opportunities of emerging devices. Keynotes were given by K. Bernstein (DARPA) and J. Roddy (Intelligent Decisions, Inc.).

In 2015 and 2016, General Chair W. Robinson led HOST's expansion to 2.5 days and then 3 days allowing for additional keynotes, visionary talks panels, networking, and other activities. In 2015, HOST pursued and received student travel support from NSF, which led to a substantial increase in student attendance. J. Plusquellic introduced a new activity in HOST 2016 that provided students with the opportunity to demonstrate new hardware attacks and protections to HOST attendees, and to compete for a Best Demo Award. Given its popularity, future HOSTs have continued to offer hardware demo sessions. In 2016, industrial liaisons, M. Tehranipoor and G. Qu, increased number of industry sponsors to 10. HOST 2016 also received a record number of submissions (106) with the top five topics being hardware-based security primitives (crypto, PUFs, TRNGs), hardware design techniques for software and/or system security, architecture support for security, side-channel attacks and countermeasures, and secure and efficient implementation of crypto algorithms.

D. Present Symposium Era (2017–2020)

The present era has been characterized by an aggressive expansion of the HOST event size, scope, and outreach activities. HOST also made significant efforts to improve the diversity of its program, the quality of its review process, and more. During this era, HOST attendance increased by over 90% with HOST 2019 having over 350 attendees.

HOST 2017 marked the 10th anniversary for this event – a significant and important milestone – and the OC, led by S. Bhunia, developed a program to recognize this accomplishment and commemorate it through many special activities. Several firsts occurred at HOST 2017. It was a 5-day event with tutorial sessions on the first day. 4 tutorials were delivered by leading experts from academia and industry (including 2 women) on topics in hardware and systems security: Internet of Things (IoT), supply chain, trusted platform modules, and analog/mixed signal circuits. The tutorials were very well attended (about 100 attendees with 30% students) and received positive feedback. HOST 2017 had two co-located events for the first time: WISE and IASW. The Workshop for Women in Hardware and Systems Security (WISE) advocated for, encouraged, and grow the participation of women in hardware and systems security. The IoT and Automotive Security Workshop (IASW) included invited talks and a panel. WISE and IASW had over 40 attendees each. Since 2017, HOST has continued to offer tutorials and workshops with success.

In 2018, General Chair R. Kastner began an overhaul to HOST's submission and review processes along with Program Chairs G. Qu and D. Forte. The page limit was increased from 6 pages to 8 pages in order to provide more space

for experiments, in-depth analysis, and proofs. HOST added a rebuttal phase so that authors could make clarifications to the program committee – this addition was popular with the authors and had a noteworthy impact on the decision making process. HOST 2018 introduced the HOST Hall of Fame to honor contributions to HOST and hardware security. Its 4 inaugural members were M. Tehranipoor, J. Plusquellic, S. Fazzari, and F. Koushanfar. In addition to a half-day WISE, HOST included a one-day co-located event, the Trusted and Assured MicroElectronics (TAME) Forum, with over 100 attendees. HOST 2018 offered 6 tutorials, half of them being presented by individuals from underrepresented groups.

In 2019, G. Qu was the General Chair. HOST expanded its scope to include *all* areas of overlap between hardware and security – from device to architecture to system levels. HOST 2019 increased its page count from 8 to 10 pages. To accommodate these changes, D. Forte led an effort to define new policies and procedures in consultation with the OC [11]. First, similar to other highly regarded venues, term limits were added to the program committee (PC) to homogenize decision-making each year and to reinvigorate the process. Second, a unique optimization program was developed to select PC members according to multiple criteria: area of expertise (esp. to meet wider scope), past performance on the PC, and diversity (gender, race, academic rank, etc.). Besides WISE and TAME, HOST 2019 added the Workshop on Energy-Secure System Architectures (ESSA), and offered 7 tutorials.

HOST 2020 is in-process with D. Forte as the General Chair. One of its main themes is industry engagement, which is evident in several ways. First, HOST 2020 will take place in Silicon Valley[1], the global center for technology and innovation. Second, HOST will offer its first large-scale exhibition for companies to increase brand exposure and visibility of their technologies, identify leads, network and establish collaborations, and recruit from HOST's large talent base. Third, HOST revamped its sponsorship packages to align with the needs of sponsors and attendees. HOST 2020 further improved the submission and review processes and now offers multiple submission deadlines, similar to other top venues. Multiple deadlines allow authors to submit their research results in a more timely fashion. The HOST review process was revised to have multiple rounds, allowing for the entire process to be more efficient for authors and TPC members. It also requires reviewers to submit reviews using an NSF-style review template to inform authors on both the positive and negative aspects of their submissions. To accommodate the workload associated with the two submission deadlines, the OC expanded to three Program Chairs. Y. Iskander and S. Fazzari are managing the first deadline, and J. Plusquellic and S. Fazzari are in charge of the second.

III. Summary of Achievements

In its short 12 year history, HOST has made a considerable impact on the field of hardware security, trust, and assurance. Following are some of HOST's notable achievements.

1) Significant Growth and Expansion: HOST began as a 1-day workshop co-located with DAC and consisted of approximately 50 attendees and 30 submissions. Today, HOST is a 3-4 day independent event with over 300 attendees and 100 submissions. Its scope has expanded from IC security to all areas of overlap between hardware and security across multiple domains (i.e., microarchitecture, IoT/CpS, cloud, vehicle, smart grid, etc.). In addition to its technical program, HOST now offers tutorials, co-located workshops, exhibition, hardware demos, and more. These activities are increasing awareness of hardware security challenges and solutions, while providing valuable education and contributing to the workforce development in an area of national importance.

2) High Impact Research: HOST publications are well-cited and have had a significant influence on the field. For example, [12] introduced the first PUF that could be implemented on *any* FPGA. [13] was the first paper to ever *clone* a PUF. [14] proposed the first hardware Trojan taxonomies. [15] and [16] proposed the first delay-based techniques for detecting hardware Trojans. [12], [13] and [14]–[16] are among the most cited PUF and hardware Trojan papers in the literature. More, recently, [17] and [18] proposed satisfiability (SAT) attacks against logic locking that have significantly altered the way such techniques are developed and analyzed.

As of this writing, HOST has over 50 papers with 50+ citations and over 20 papers with 100+ citations. In July 2019, HOST had an h5-index[2] of 25 and h5-median[3] of 44 according to Google Scholar Metrics [19]. For comparison, IEEE S&P had h5-index and h5-median of 72 and 128 resp. While this gap may seem large, IEEE S&P is 3 × older than HOST and receives over 500 submissions annually (4× more than HOST). HOST's numbers are impressive for a young conference with a growing community, and we expect substantial gains over the next decade. HOST's acceptance rate is extremely competitive at 25%.

3) Spinoffs: The HOST steering committee and organizers have been involved in the launch of various events across the world. In 2016, HOST produced its first direct spin-off event – the IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST). Other examples of HOST outreach include TAME, a national forum on trusted and assured microelectronics [20] and PAINE, a conference on Physical Attack and Inspection on Electronics [21]. Women in Hardware and Systems Security (WISE) was co-located with HOST [22] from 2017–2019. The Workshop on Attacks and Solutions in Hardware Security (ASHES) is another offshoot [23]. International Verification and Security Workshop (IVSW) is part of the IEEE Federated Event on Design for Robustness. Top Picks in Hardware Security [24] is celebrating impactful papers in hardware and embedded cybersecurity. In addition, HOST engendered hardware and embedded security tracks at

[1]This will be the first HOST on the west coast since 2012 and the first HOST outside of the DC area since 2013.

[2]h5-index is the largest h such that h articles published in the last 5 years have at least h citations each.

[3]h5-median is the median # of citations for the articles of h5-index.

established IEEE/ACM conferences such as DAC, ICCAD, ITC, ICCD, VTS, and ETS. Through these activities, HOST has raised awareness about government/defense/industry concerns, and brought hardware and embedded security into failure analysis, verification, computer security, VLSI testing, and EDA communities.

4) High Profile Speakers: HOST has provided a platform to address new challenges facing the community. HOST has consistently drawn leaders and decision-makers from government, industry, and academia for keynotes, visionary talks, and panels to highlight the hot topics. Program managers (PMs), VPs, CTOs, directors, and fellows, offered their unique perspectives on hardware and system security. DARPA PMs used HOST as a forum to announce new programs (e.g., TRUST, IRIS, SHIELD, OMG, and AISS).

5) Strides in Diversity and Inclusion: Equity, diversity, and inclusion have become a priority of HOST. To this end, we have pursued additional funding from NSF and other industry sponsors to provide student travel, lodging, and registration support, thus enabling students to participate in hardware demos, poster competitions, panels, etc. who would otherwise be excluded. More than 40 students are supported annually, and ~35% of them have been women and minorities. Each year, the HOST organizers make a concerted effort to include diverse speakers in the program. HOST also subsidized WISE for several years to encourage and support women in the field.

6) Annual Revitalization: HOST persistently improved itself each and every year. Notable examples include the introduction of the hardware demo competition and tutorial sessions. The hardware demo competition is unique to HOST, and has grown each year since its inception to become one of its most popular activities. HOST has also made significant upgrades to its submission and review processes, including a novel TPC evaluation and selection system, rebuttal phase, multiple rounds and deadlines, and conflict-free awards chair [11].

IV. The Future of HOST

HOST envisions an environment where hardware security and trust can be effectively reasoned, allowing for informed decisions during system design, acceptance, and update. HOST's contributions have culminated and have had several significant impacts on the community. First and foremost, TAME has emerged to enable experts from government, industry, and academia to form working groups and meet regularly for effective coordination on hardware security hot topics. With TAME in its final year, HOST may fill this role. Further, HOST is planning collaborative activities with its peers including CHES and HASP. Second, the success of AsianHOST and the proliferation of dedicated hardware security sessions in other venues demonstrate the demand for year-round dissemination of research in hardware security. This has prompted HOST to introduce multiple submission deadlines and to consider EuroHOST as a third annual event in Europe. HOST also plans to disseminate videos of its technical presentations and hardware demos via social media. Lastly, improvements to HOST submission and review processes have profoundly impacted author satisfaction, the number of submissions, and its reputation. HOST is considering in-person TPC meetings as its next upgrade.

V. Conclusion

HOST has come a long way in a decade – what started out as a niche workshop on hardware Trojans has blossomed into a symposium with a broad scope that interests multiple communities. HOST has significantly impacted hardware and embedded cybersecurity through technical papers, invited talks, spinoffs, tutorials, demos, and achievements in diversity/inclusion. Just as security is a moving target, HOST will continue to evolve in support of the community and society.

References

[1] M. Lipp *et al.*, "Meltdown: Reading kernel memory from user space," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018.

[2] P. Kocher *et al.*, "Spectre attacks: Exploiting speculative execution," in *40th IEEE Symposium on Security and Privacy (S&P'19)*, 2019.

[3] D. Gruss *et al.*, "Rowhammer. js: A remote software-induced fault attack in javascript," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2016, pp. 300–321.

[4] A. Tang *et al.*, "Clkscrew: exposing the perils of security-oblivious energy management," in *26th USENIX Security Symposium*, 2017, pp. 1057–1074.

[5] J. Krautter *et al.*, "Fpgahammer: remote voltage fault attacks on shared fpgas, suitable for dfa on aes," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 44–68, 2018.

[6] S. Adee, "The hunt for the kill switch," *iEEE SpEctrum*, vol. 45, no. 5, pp. 34–39, 2008.

[7] J. Robertson and M. Riley, "The big hack: how china used a tiny chip to infiltrate us companies," *Bloomberg Businessweek*, vol. 4, 2018.

[8] M. M. Tehranipoor *et al.*, "Counterfeit integrated circuits," in *Counterfeit Integrated Circuits*. Springer, 2015, pp. 15–36.

[9] "IEEE International Symposium on Hardware Oriented Security and Trust," http://www.hostsymposium.org.

[10] T. Force, "High performance microchip supply," *Annual Report. Defense Technical Information Center (DTIC), USA*, 2005.

[11] "HOST Organizing Policies," http://www.hostsymposium.org/policy.php.

[12] S. S. Kumar *et al.*, "The butterfly puf protecting ip on every fpga," in *HOST*. IEEE, 2008, pp. 67–70.

[13] C. Helfmeier *et al.*, "Cloning physically unclonable functions," in *HOST*. IEEE, 2013, pp. 1–6.

[14] X. Wang *et al.*, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *HOST*. IEEE, 2008, pp. 15–19.

[15] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *HOST*. IEEE, 2008, pp. 51–57.

[16] J. Li and J. Lach, "At-speed delay characterization for ic authentication and trojan horse detection," in *HOST*. IEEE, 2008, pp. 8–14.

[17] P. Subramanyan *et al.*, "Evaluating the security of logic encryption algorithms," in *HOST*. IEEE, 2015, pp. 137–143.

[18] K. Shamsi *et al.*, "Appsat: Approximately deobfuscating integrated circuits," in *HOST*. IEEE, 2017, pp. 95–100.

[19] "English - Google Scholar Metrics," https://scholar.google.com/citations?view_op=top_venues.

[20] "Trusted and Assured MicroElectronics Forum," https://www.tameforum.org.

[21] "IEEE Conference on Physical Assurance and Inspection of Electronics," http://paine-conference.org/.

[22] "Women in Hardware and Systems Security," http://www.hostsymposium.org/host2018/wise-workshop.php.

[23] "Attacks and Solutions in Hardware Security," http://ashesworkshop.org.

[24] "Top Picks in Hardware and Embedded Security," http://toppicksinhardwaresecurity.alari.ch.