Editorial: Security of Embedded Systems and Cyber Irons—Embedded Systems for Security

Security of embedded systems has been an active area of research for a long time. Concerns about Trojans, malware that affects BIOS and firmware components, vulnerabilities in software, operating systems, network stack or applications etc., have engaged many security researchers. In the past year, we have run one special issue on device forensics and security for embedded systems. Another special issue on secure and fault-tolerant embedded computing will appear soon. In May 2015, we presented a special issue on embedded platforms for cryptography in the coming decades, which was guest edited by Patrick Schaumont, Maire O'Neill, and Tim Guneyasu. However, this is the story of Cyber Irons, which many security companies have recently been bringing to the market. Instead of securing embedded systems with cryptographic techniques or other security controls, the idea here is that security controls, monitoring, and policy enforcements are designed into specific embedded systems—so-called Cyber Irons. Whereas the special issue by Schaumont et al. focused on designing cryptographic algorithms, digital signature schemes, and hashing techniques into hardware, Cyber Irons are more than just about cryptography. A few examples from current commercial product offerings will be illustrative: IBM recently brought the z13s mainframe into the market, which has hardware-accelerated encryption, as it is designed to encrypt all customer transactions for e-commerce, including orders placed over the phone. Beyond cryptography acceleration, it has hardware for cyber analytics that learns from behaviors of users to detect any malicious activities in the system. Cisco marketed its Firepower next-generation firewall product, which has hardware for stateful firewall technology as well as intrusion detection/prevention, advanced malware protection, and reputation-based URL filtering. We have seen email spam filters in hardware for some time now. Dell's SonicWall is more than just spam filtering in hardware; it provides deeper network security. Spikes security has a hardware-based browser malware isolation appliance that isolates and eliminates browser-borne malware. AirMagnet provides a wireless network intrusion detection device and wireless network monitoring. AvaLan's AW-HSNetAppliance provides hardware encryption at the end points of VPN tunneling appliances. Darktrace provides an appliance that uses machine learning hardware for detecting anomalous activities in an enterprise-wide network. These are only a few examples of hardware appliances designed for cybersecurity enforcement. Most of them actually can be categorized as embedded systems, as they typically have general-purpose processors; software stacks; software applications including dashboards for configuration, monitoring, and changing security policies; and hardware accelerators for cryptography, packet inspection, and even machine learning.

This is surely a burgeoning area of cybersecurity research, a growing market segment, and surely an active product space for companies. What is driving the growth is not only increasing awareness of cyber risks but also the imposition of various requirements by regulatory bodies on different sectors for cybersecurity control and policy implementations. In the past 6 months in India, the banking sector was given a mandate to implement a number of cybersecurity controls by the end of September 2016. The securities and exchange board also mandated similar requirements on financial market players. The power utilities will probably have a similar mandate in the near future. The appliances designed to be configured to enforce security policies specific

to a company or mandated by regulation will be very attractive for the cybersecurity teams.

The design of these appliances, verification that they are compliant to Federal Information Processing standards (e.g., FIPS 140-2) using common criteria evaluation, the power/dimensions/latency issues, issues of maintaining line speed for packet inspection, or stateful packet processing are certainly of interest to this journal. It is my hope that we will have some special issue proposals on Cyber Irons design, implementation, trade-offs, applications, algorithms, among others.

Coming to the current issue of ACM TECS, this is the last issue of Volume 15. I must thank ACM journal manager Ms. Laura Lander, our production editor Ms. Kelly Crooks, and our journal assistant Ms. Jeyel Tecson for their strong support and efficient handling of all editorial matters to bring ACM TECS publications on schedule. I must also thank the associate editors, and all guest editors of special issues for their timely handling of manuscripts and for proposing exciting special issue topics.

Here, we have a special issue based on the best papers of Embedded Systems Week (ESWEEK'15). This special issue is an invite-only issue, and extended versions of the best papers from all of the different conferences held as part of ESWEEK were invited by the guest editors; several rounds of reviews were carried out, and improved versions were selected. In addition to this special issue, we have eight regular issue papers that cover a wide range of topics in embedded systems.

Sandeep K. Shukla
Indian Institute of Technology Kanpur

July 23, 2016

Editor-in-Chief