Deepak Puthal

Bio

Deepak Puthal is an Assistant Professor (Senior Grade) in the School of Computing at Newcastle University, Newcastle upon Tyne, United Kingdom, and an Honorary Fellow in the Faculty of Engineering and Information Technology at University of Technology Sydney, Australia. Before this position, he worked as an Assistant Professor at the University of Technology Sydney and as a graduate research fellow at Data 61, Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia. He has received his Ph.D. in Engineering and IT from the University of Technology Sydney, Australia. His research spans several cybersecurity areas, focusing on user-centric security, blockchain, the scalable security solution for resource constraint consumer devices, and the Internet of Things. He has delivered several keynotes, invited talks, and industrial talks globally in the field of his domain of expertise.
He is on the editorial boards of 5 international journals, such as IEEE Transactions on Big Data, IEEE Consumer Electronics Magazine, Computers & Electrical Engineering, (Elsevier), International Journal of Communication Systems (John Wiley & Sons), and Internet Technology Letters. He served as a Co-Guest Editor of several reputed journals, including IEEE Consumer Electronics Magazine, Future Generation Computer Systems, Concurrency and Computation: Practice and Experience, Wireless Communications and Mobile Computing, and Information Systems Frontier. He was the Program Chair of IEEE CCCI 2020 (International Conference on Communications, Computing, Cybersecurity, and Informatics), CloudComp 2019 (9th EAI International Conference on Cloud Computing), AusPDC 2018-2019 (17th Australasian Symposium on Parallel and Distributed Computing), ICIT 2018 (17th International Conference on Information Technology), SPTIoT 2017-2018 (IEEE International Symposium on Security, Privacy and Trust in Internet of Things), and

PriSec 2014 (The 3rd International Symposium on Privacy and Security in Cloud and Big Data). He has been on over 50 TPCs of international conferences, symposiums and workshops.
He is the recipient of the three best paper awards from the IEEE Consumer Technology Society, 2019 Best IEEE ComSoc Young Researcher Award (For Europe, Middle East, and Africa Region), 2018 IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher), and 2017 IEEE Distinguished Doctoral Dissertation Award (IEEE STC on Smart Computing). He is a senior member of the IEEE and a member of the IEEE Consumer Technology Society.

Topics

Title: 360-degree view of Blockchain and its deployment in energy constraint consumer devices

Abstract: In today's connected world, resource-constrained devices are deployed for sensing and decision-making applications, ranging from smart cities to environmental monitoring. Those recourse constrained devices are interconnected to create real-time distributed networks popularly known as the Internet of Things (IoT). Current security solutions are problematic when there is a centralized controlling entity. The Blockchain is gaining a lot of interest in these domains to secure the system by ignoring centralized dependencies. A consensus mechanism in Blockchain plays a vital role in making the whole security solution decentralized. Due to the resource limitations of the IoT devices, traditional Blockchain consensus may not be the best solution to secure with desire system performances. Proof-of-Authentication (PoAh) is a consensus mechanism dedicatedly developed and designed for resource constraint consumer devices and further integrated with hardware security primitives called Physical Unclonable Functions (PUFs) to solve scalability, latency, and energy requirement challenges. This talk will answer the following questions to the audience: (1) What is Blockchain? (2) What is it’s advantages over traditional security solutions? (3) What are the drawbacks in integrating Blockchain in energy constraint consumer devices? (4) What is the PoAh and it's consequences in integrating PUF? (5) Does this secure both device and data?

Title: PUF-Based robust security solution designing for the Internet of Medical Things

Abstract: Various commercial off-the-shelf components are available for the development of communication-enabled consumer electronics devices. In the case of the Internet of Medical Things (IoMT) for smart healthcare, there are also many hardware and software vulnerabilities that the attackers can take advantage of to
gain access to the system. This opens new doors to attackers who can take advantage of various vulnerabilities to attack the entire network and compromise the system's integrity. The traditional cryptographic techniques may not be sufficient to provide the healthcare application's required level of security. The Physical Unclonable Functions (PUFs) are being developed as a security primitive that can generate random numbers on the fly and feed them to strengthen the overall security mechanism. PUF is hardware that uses the variability in the physical world, such as process verification during device fabrications. The talk will address many questions as follows: (1) what is the IoMT? (2) What are the security vulnerabilities of IoMT? (3) What are the drawbacks of current security solutions? (4) How is PUF going to strengthen the security solutions?

Title: Software-Defined Perimeter: The future of simultaneous device and data security

Abstract: The Internet of Things (IoT) is becoming a backbone of sensing infrastructure to several mission-critical applications such as smart health, disaster management, and smart cities. Due to the resource-constrained nature of sensing devices, IoT infrastructures use Edge datacenters (EDCs) for real-time data processing and decision-making. Generally, EDCs communicate with IoT devices in emergency scenarios to evaluate data in real-time. Protecting data communications from malicious activity becomes a key factor, as all the communication flows through insecure channels. The current communication security pattern of "communication before authentication" leaves a "black hole" for intruders to become part of communication processes without authentication. Software-Defined Perimeter (SDP) is a groundbreaking concept. It is developed to shifts the security models from a network-centric approach to a device-centric security approach by authenticating devices before communication is established. A trusted controller is initialized to authenticate and establishes the secure channel between the devices before they start communication between themselves. The centralized controller draws a perimeter for secure communications within the boundary to ensure both device and data security. The talk will elaborate on the concept, working model, use cases, pros and cons, and SDP's future research.