Fall 2017 Seminar Series

Leveraging Blockchain-based protocols in IoT systems
October 11th 2017

Time 9:15am-10:15am – HEC 113

The Internet of Things (IoT) encompasses a wide range of processes: sensing, computation, communication, time, context, and data, to name only a few. How does all of these function as a system when using commercially available components that can be purchased from anywhere and at a low cost, and with little or no component pedigree available? To provide some practical answers to the these questions, we purchased components and created a set of small use cases to see how it all interoperated.

In this talk, we will focus on use cases where the application of cryptography is not done properly or the cryptographic libraries employed exhibit security flaws. To that end, we demonstrate the need for mechanisms that will allow low-resource sensors to authenticate and exchange data in a way that does not rely on heavy cryptographic operations. We believe the need for group authentication and message integrity can be adequately satisfied using modified blockchain protocols that rely on proof-of-storage for some of the sensor operations creating groups of networked sensors that prove their membership not only using key material but also historical transactional data. Our work shows how blockchain protocols can be applied in IoT systems in a meaningful manner solving an actual need without the burden of complex operations that usually accompany the blockchain concept.

Furthermore, I will be presenting my research over the past few years on Cyber Security defenses spanning from Cloud-enabled Moving Target defenses to host-based intrusion detection and security for IoT devices. I will also emphasize why Cyber Security is going to play a central role in our future research and education partly owed to the ever increasing adoption of technology in our everyday life and exposure of critical infrastructure to Internet connectivity. I will also discuss the role of research in education and the challenges of building a comprehensive security program that is appealing not only to computer scientists but other disciplines as well including electrical engineering, business, and policy.

Dr. Angelos Stavrou

George Mason University and the Director of the Center for Assurance Research and Engineering at GMU

Dr. Angelos Stavrou is a Professor at George Mason University and the Director of the Center for Assurance Research and Engineering (CARE) at GMU. Stavrou has served as principal investigator on research awards from NSF, DARPA, IARPA, DHS, AFOSR, ARO, ONR, he is an active member of NIST's Mobile Security team and has written more than 90 peer-reviewed conference and journal articles. Stavrou received his M.Sc. in Electrical Engineering, M.Phil. and Ph.D. (with distinction) in Computer Science all from Columbia University. He also holds an M.Sc. in theoretical Computer Science from University of Athens, and a B.Sc. in Physics with distinction from University of Patras, Greece. Stavrou is an Associate Editor of IEEE Transactions on Reliability and IET Journal on Information Security. His current research interests include security and reliability for distributed systems, security principles for virtualization, and anonymity with a focus on building and deploying large-scale systems. Stavrou received the GMU Department of Computer Science Outstanding Research Award in 2010 and 2016 and was awarded with the 2012 George Mason Emerging Researcher, Scholar, Creator Award, a university-wide award. In 2013, he received the IEEE Reliability Society Engineer of the Year award. He is a NIST guest researcher, a member of the ACM and USENIX, and a senior IEEE member. Under DHS funding, he designed next generation analysis and defenses for mobile devices for both Android and iOS systems and was awarded the DHS Cyber Security Division's "Significant Government Impact Award" in 2017.

*Hosted by: **Dr. Gary Leavens***