THE COMPUTER SCIENCE DISTINGUISHED COLLOQUIUM

Vasilios Siris

Vasilios Siris is Full Professor at the Department of Informatics, Athens University of Economics and Business, where he is since 2009. Previously he was an Assistant Professor at the University of Crete (2002-2008) and Research Associate at the Institute of Computer Science of FORTH (Foundation for Research and Technology - Hellas (1992-2011). He has held visiting positions at the Statistical Laboratory of the University of Cambridge, British Telecommunications (BT), UK, and the University of Bern, Switzerland. His current research interests include the application of Self-Sovereign Identity (SSI) technologies, Decentralized Identifiers, and Verifiable Credentials to the IoT, resource control in wireless and mobile networks, and the architecture of future networks. He has one International and two national patents related to wireless/mobile network management. He has served as the general chair or program chair for many international conferences and workshops, and has represented Greece in numerous EU research and coordination actions. He has recently co-founded the AUEB spinoff ExcID, which focuses on identity, security, and privacy solutions based on SSI.

Date: Tue, Aug 23
Time: 10:00 AM
Location: UC 363

New results on Decentralized Identifiers and their application to the Internet of Things and Content Delivery

Self-Sovereign Identity (SSI) technologies such as Decentralized Identifiers (DIDs) and Verifiable Credentials enable users to take full control of their identities and information, avoiding reliance on centralized identity providers, hence can fundamentally support user privacy. User control and privacy are significant requirements of EU's eIDAS (electronic IDentification, Authentic and trust Services) 2.0 framework revision, among other initiatives around the world. In this talk, after reviewing the key properties of DIDs and Verifiable Credentials, I will present a new DID method that is compatible with W3C's DID specifications, but does not require a blockchain/DLT, a 3rd party registry or any other trusted entity. This is achieved by treating the DID's original key pair as the root of trust, thus providing self-verifying properties. Benefits of the proposed scheme include key rotation without having to change the public key/DID, controlled delegation, and document sharing between untrusted entities. We present applications to the Internet of Things, including device-to-device communications between constrained devices with limited resources and limited/no Internet connectivity, and content delivery. Results of this work are applied and further extended in the NGIatlantic.eu project SECOND "Securing Content Delivery and Provenance", which is a collaboration between the Athens University of Economics and Business and the University of Memphis.

THE UNIVERSITY OF MEMPHIS

Department of Computer Science
The University of Memphis
Memphis, TN 38152