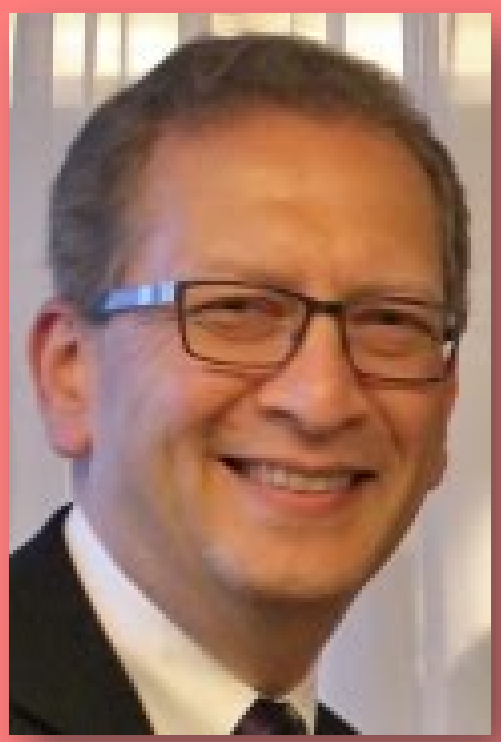
SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING

INFORMATICS COLLOQUIUM SERIES



Azer Bestavros

Boston University

Friday, November 16, 2018

3:00 PM

Luddy Hall, Rm. 1106

Sharing Knowledge without Sharing Data:

On the false choice between the privacy and utility of information

Abstract: Boston's high-profile initiative to study the gender pay gap in the city was stalled by concerns about the confidentiality of payroll information of over 120,000 employees from more than 170 employer organizations. At its essence, the issue was the mistaken belief by city officials and corporate executives that data sharing is a prerequisite to knowledge sharing. This false choice between data utility and data privacy is the result of an over-emphasis in the research community on the development of infrastructures and platforms for “data sharing” with an expectation of altruism from data owners. In this talk, I will argue for an alternative tack that allowed this first-of-its-kind initiative to be carried out, namely the development of infrastructures and platforms that allow knowledge extraction from multiple data sets that remain otherwise private, using a cryptographic technique called secure multi-party computation (MPC).

MPC techniques enable society to benefit from collective data analysis in contexts where the raw data are encumbered by legal and corporate policy restrictions on data sharing. However, MPC's substantial social benefits cannot be realized unless principals of participating organizations have a clear, confident understanding of how MPC protects their sensitive data and mathematically guarantees compliance with data sharing restrictions. With that goal in mind, In the first part of this talk, I will provide details of the architectural design and implementation of our MPC platform which was informed by nearly two years' worth of discussions with personnel from key participating organizations (including CIOs, CTOs, HR executives, and lawyers), social scientists, and members of the city council that commissioned the study.

Real-world applications that could benefit significantly from MPC are developed by data analysts who lack MPC knowledge. Moreover, these applications require the use of very large data sets managed by organizations that employ different computational stacks internally, and which are subject to different compliance constraints. To address these challenges, we have extended our platform by integrating it with existing big-data workflow management in a cloud setting, and by incorporating optimized MPC implementations of common algorithms into software libraries. In the second part of my talk, I will summarize these extensions and will show performance results from a number of at-scale deployments, including the computation of the Herfindahl-Hirschman Index (HHI) of market concentration used in antitrust regulation on an aggregate 156 GB of data from five mutually distrusting companies, and the analysis of cybersecurity risks associated with threat propagation through the interconnection of multiple ISP networks. Time permitting, I will discuss a number of secure MPC platforms that we developed in support of other applications, including private network security analytics and privacy-preserving ride sharing services.

Biography: Azer Bestavros is Warren Distinguished Professor of Computer Science and Founding Director of the Hariri Institute for Computing at Boston University, which was set up in 2011 as an incubator for high-risk, high-reward cross-disciplinary collaborations. Notable incubated efforts that he launched at the Institute, which matured into multi-million-dollar projects, include the $25M+ Mass Open Cloud Exchange, $10M NSF Cloud Security Frontier project, $5M Red Hat open-source innovation collaboratory, and the $1M+ SCOPE cloud platform for enabling smart-city applications. In addition to research, the Institute has served as the anchor of number of university initiatives, including the Data Science Initiative, the Digital Health Initiative, the Digital Learning Initiative, and the BU Spark! program for student-driven innovation.

Professor Bestavros pursues research in networking, distributed computing, cybersecurity, and high-assurance systems. His seminal contributions include pioneering studies of web push caching through content distribution networks, self-similar Internet traffic characterization, game-theoretic cloud resource management, and safety certification of networked systems and software. His current research projects include the development of toolkits for secure multi-party computation, the design and implementation of scalable software platforms for privacy-preserving big-data analytics, and the use of edge clouds for control of cyber-physical systems. As of 2018, funded by over $30M from government and industry sponsors, his research has yielded 18 PhD theses, 8 issued patents, 2 startups, and hundreds of refereed papers with over 18,500 citations according to Google Scholar.

Professor Bestavros received a number of awards for distinguished teaching, research, and service, including the ACM Sigmetrics Inaugural Test of Time Award for 1996 research work “whose impact is still felt 15 years after its initial publication” and the 2010 United Methodist Scholar Teacher Award in recognition of “outstanding dedication and contributions to the learning arts and to the institution.” In 2017, he was named a William Fairfield Warren Distinguished Professor, the highest distinction bestowed upon senior faculty members at Boston University for “representing our community with distinction, enriching the academic experience for our students, and raising our stature as a major research university.”

Prior to his inaugural role at the Hariri Institute for Computing, Professor Bestavros chaired the Computer Science Department at Boston University from 2000 to 2007, having joined it in 1991 after completing his PhD in Computer Science at Harvard University.

More information is available from http://azer.bestavros.net

INDIANA UNIVERSITY

SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING