

The 2015 IEEE International Conference on Software Quality, Reliability and Security

QRS 2015

Vancouver, Canada, August 3-August 5, 2015

<http://paris.utdallas.edu/qrs15>

Keynote Speech

Data Protection from Insider Threats — Concepts and Research Issues

Elisa Bertino

Department of Computer Science

Purdue University

<https://www.cs.purdue.edu/people/faculty/bertino/>

Abstract

Attempts by insiders to exfiltrate data have become a severe threat to the enterprise. Conventional data security techniques, such as access control and encryption, must be augmented with techniques to detect anomalies in data access that may indicate exfiltration attempts. In this talk, we first present DBSAFE, a system to detect, alert on, and respond to anomalies in database access designed specifically for relational database management systems. The system automatically builds and maintains profiles of normal user and application behavior, based on their interaction with the monitored database during a training phase. Application profiling uses a novel technique based on concolic testing by which DBSAFE is able to track and record the queries executed by an application depending on the application input parameters. The system then uses these profiles to detect anomalous behavior that deviates from normality. Once an anomaly is detected, the system uses predetermined policies guiding automated and/or human response to the anomaly. We then discuss future work and open research directions.

About the speaker

Elisa Bertino is professor of computer science at Purdue University, and Director of the Purdue Cyber Center (Discovery Park). She also serves as Research Director of the Center for Information and Research in Information Assurance and Security (CERIAS). Prior to joining Purdue, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory (now Almaden) in San Jose, at the Microelectronics and Computer Technology Corporation, at Rutgers University, at Telcordia Technologies. Her recent research focuses on database security, digital identity management, policy systems, and security for web services. She is a Fellow of ACM and of IEEE. She received the IEEE Computer Society 2002 Technical Achievement Award, the IEEE Computer Society 2005 Kanai Award, and the 2014 ACM SIGSAC Outstanding Contributions Award. She is editor in chief of IEEE Transactions on Dependable and Secure Computing and has served as chair of the ACM Special Interest Group on Security, Audit and Control (ACM SIGSAC).