"Protecting Information Systems from Insider Threats - Concepts and Issues"

Elisa Bertino

Keynote abstract

Past research on information security has focused on protecting valuable resources from attacks by outsiders. However, statistics show that a large amount of security and privacy breaches are due to insider attacks. Protection from insider threats is challenging because insiders may have access to many sensitive resources and high-privileged system accounts. Suitable approaches need to combine several security techniques, like fine-grained access control, stronger authentication protocols, integrated digital identity management, intrusion detection, with techniques from areas like information integration, machine learning, and risk assessment. In this talk, after an introduction to the problem of insider threats, we will present recent work addressing the problem of anomaly detection and response policies for database management systems and then discuss open research issues, by emphasizing the role of techniques from the area of information integration.