KEYNOTE TITLE: Big Data Security and Privacy

Dr. Elisa Bertino,
Purdue University,
bertino@cs.purdue.edu

ABSTRACT: Technological advances and novel applications, such as sensors, cyber-physical systems, smart mobile devices, cloud systems, data analytics, and social networks, are making possible to capture, and to quickly process and analyze huge amounts of data from which to extract information critical for security-related tasks. In the area of cyber security, such tasks include user authentication, access control, anomaly detection, user monitoring, and protection from insider threat. By analyzing and integrating data collected on the Internet and Web one can identify connections and relationships among individuals that may in turn help with homeland protection. By collecting and mining data concerning user travels and disease outbreaks one can predict disease spreading across geographical areas. And those are just a few examples; there are certainly many other domains where data technologies can play a major role in enhancing security. The use of data for security tasks is however raising major privacy concerns. Collected data, even if anonymized by removing identifiers such as names or social security numbers, when linked with other data may lead to re-identify the individuals to which specific data items are related to. Also, as organizations, such as governmental agencies, often need to collaborate on security tasks, data sets are exchanged across different organizations, resulting in these data sets being available to many different parties. Apart from the use of data for analytics, security tasks such as authentication and access control may require detailed information about users. An example is multi-factor authentication that may require, in addition to a password or a certificate, user biometrics. Recently proposed continuous authentication techniques extend access control system. This information if misused or stolen can lead to privacy breaches. It would then seem that in order to achieve security we must give up privacy. However this may not be necessarily the case. Recent advances in cryptography are making possible to work on encrypted data – for example for performing analytics on encrypted data. However much more needs to be done as the specific data privacy techniques to use heavily depend on the specific use of data and the security tasks at hand. Also current techniques are not still able to meet the efficiency requirement for use with big data sets. In this talk we will discuss methods and techniques to make this reconciliation possible and identify research directions.

SHORT BIO: Elisa Bertino is professor of computer science at Purdue University, and serves as Director of Purdue Cyber Center and Research Director of the Center for Information and Research in Information Assurance and Security (CERIAS). She is also an adjunct professor of Computer Science & Info tech at RMIT. Prior to joining Purdue in 2004, 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 data security and privacy, digital identity management, policy systems, and security for the Internet-of-Things. 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 ACM SIGSAC 2014 Outstanding Contributions Award. She is currently serving as EiC of IEEE Transactions on Dependable and Secure Computing.

KEYNOTE TITLE: Adversarial Signal Processing And The Hypothesis Testing Game

Dr. Mauro Barni
University of Siena, Italy
barni@dii.unisi.it

ABSTRACT. Security-oriented applications of signal processing have received increasing attention in the last years. Digital watermarking, steganography and steganalysis, multimedia forensics, biometric security, are just a few examples of such an interest. In many cases, though, researchers have failed to recognize the single most unique feature behind any security-oriented application, i.e. the presence of one or more adversaries aiming at making the system fail. One of the most evident consequences is that security requirements are misunderstood, e.g. quite often security is exchanged for robustness. Even when the need to cope with the actions of a malevolent adversary is taken into account, the proposed solutions are often ad-hoc, failing to provide a unifying view of the challenges that such scenarios pose from a signal processing perspective. Times are ripe to go beyond this limited view and lay the basis for a general theory that takes into account the impact that the presence of an adversary has on the design of effective signal processing tools, i.e. a theory of adversarial signal processing.

Short Bio. Mauro Barni graduated in electronic engineering at the University of Florence in 1991. He received the PhD in informatics and telecommunications in October 1995. He has carried out his research activity for over 20 years first at the Department of Electronics and Telecommunication of the University of Florence, then at the Department of Information Engineering of the University of Siena. During the last decade he has been studying the application of image processing techniques to copyright protection and authentication of multimedia, and the possibility of processing signals that has been previously encrypted without decrypting them. Lately he has been working on theoretical and practical aspects of adversarial signal processing. He is author/co-author of almost 300 papers published in international journals and conference proceedings, and holds four patents in the field of digital watermarking and image authentication. He is co-author of the book "Watermarking Systems Engineering: Enabling Digital Assets Security and other Applications", published by Dekker Inc. in February 2004. He participated to several National and European research projects on diverse topics, including computer vision, multimedia signal processing, remote sensing, digital watermarking, IPR protection. He was the funding editor of the EURASIP Journal on Information Security. He is the Editor in Chief of the IEEE Transactions on Information Forensics and Security for the years 2015-2017. He has been serving as associate editor of many journals including several IEEE Transactions. Prof. Barni has been the chairman of the IEEE Information Forensic and Security Technical Committee (IFS-TC) from 2010 to 2011. He is a fellow member of the IEEE and a member of EURASIP. He was appointed DL of the IEEE SPS for the years 2013-2014. He was the technical program chair of ICASSP 2014.