TRACK D: CYBER-SECURITY ECOSYSTEM

Track co-Chairs

- **Haidong Xia,** *Intel Corp., USA*
- **Vidyasagar Potdar,** *Curtin University, Australia*
- **Hongxia Jin,** *Samsung R&D, USA*

Cyber-Security Ecosystems are a synergetic composition of technologies addressing both proactive and reactive strategies to create countermeasures for security. Their objective is to prevent attacks to our various connected systems and devices. Enablement requires much industry, political and ecosystem cooperation that is often lacking.

Cyber-Security Ecosystems utilize a collection of countermeasure technologies from simple heuristic and patter matching methodologies, such as anti-virus techniques, to preventive, even hardware based schemes to isolate computation from attack strategies. These systems are typically challenging to use, only partially effective, and most significantly lack adoption for many systems within our connected network of devices. Devices from all markets are of interest including consumer, business and industry, since they all interact through network connectivity and can be used for security attacks directly or as an agent. Research on the methodologies and effectiveness of these strategies would be welcome along with studies where elements of the computational infrastructure are weak in countermeasure adoption would be welcome. Also of particular interest to the ecosystem is an understanding how to measure effectiveness of any solution strategy. The domain focus of this track will be accordingly on security technologies, their effectiveness and usage across the ecosystem but it is open to adjacent domains as well.

978-1-4799-0786-1/13/$31.00 ©2013 IEEE