Journal of Information Processing Vol.20 No.4 823 (Oct. 2012)

[DOI: 10.2197/ipsjjip.20.823]

Editor's Message to Special Issue on Computer Security Technology Achieving Smart Society

Satoru Torii[1,a)]

Sensors now capture a wide variety of information unimaginable before. Data storage holds immense information coming from distributed sources. Analytic software discovers meaningful correlation patterns from a vast amount of data. Devices and computer systems have become ever smarter. Latest user interface allows users easier and more intuitive operations. Our everyday life is greatly affected by these recent technological advances. All these changes lead to a smart society, which should enable us to make much more appropriate and better decisions according to up-to-the-minute circumstances.

For example with the spread of smartphones and SNSs (Social Networking Services), we are now able to access a variety of information almost at any time anywhere. Furthermore, situation-aware terminals give their users timely advices. Information collected through smartphones and SNSs is expected to help provide solutions for complicated social problems, such as traffic congestion, aging society, food safety, and environmental pollution. Such a society is at the heart of achieving it.

Then computer security technologies play an important role in making the smart society a safe and secure place. In order to minimize risks and threats to the smart society, computer security technologies should be employed to reduce various threats, such as exploitation of vulnerability of embedded devices, denial of service attacks, illegal changes and leakage of stored information, and so on.

From the point of view realizing a safe and secure smart society, this special issue focuses on papers that describe such computer security technologies in terms of basic theories and techniques, protocols, architectures, software systems, applications and implementations, operation and management, and social-scientific analyses. Forty eight manuscripts were submitted to the RFP of this special issue. With two manuscripts withdrawn, twenty two manuscripts have made into this issue out of forty six manuscripts.

Along with those high quality papers, I am pleased to announce that there is also an invited paper. The paper describes achievements of the DETER Project that aims to provide experimental infrastructure to support cybersecurity technology development. The initial focus of DETER Project was to develop a testbed framework for evaluating security mechanisms. SIG-CSEC (Special Interest Group on Computer Security), the proposer of this special issue, has been hosting Anti-Malware Engineering WorkShop (MWS). MWS's focus has been on malware research development and evaluation using datasets captured in testbeds of some of its member organizations. With this invited paper, I wish this activity of MWS would expand beyond Japan into all over the world.

Finally, I would like to thanks those involved in this special issue: the editorial team members, the reviewers, the secretariat, and of course, to the authors. This special issue would not have been possible without their contributions. In particular, I would like to acknowledge valuable hard work by the Editorial Board members, Koji Chida (NTT Corporation) and Katsunari Yoshioka (Yokohama National University).

[1] Fujitsu Laboratories Ltd., Kawasaki, Kanagawa 211–8588, Japan
[a)] pro104@labs.fujitsu.com