Information Security in Korea IT839 Strategy

Ho-Ick Suk

Ministry of Information and Communication, Korea
hisuk@mic.go.kr

Korea now has world-class IT infrastructure such as broadband Internet and mobile communications, and produces high-quality products based on broadband networks and IT technologies including semiconductors, mobile handsets, digital TV, etc. The achievement was made possible thanks to new services that create demand, establishment of infrastructure that enables the provision of new services, and enhanced manufacturing capability. To formulate a new virtuous cycle, the Ministry of Information and Communication (MIC) developed the IT839 Strategy

The IT839 strategy is composed of 8 services, 3 infrastructures and 9 new growth engines. 8 services are WiBro (Wireless Broadband) Service, DMB (Digital Multimedia Broadcasting) Service, Home Network Service, Telematics Service, RFID-based Service, W-CDMA Service, Terrestrial Digital TV, and Internet Telephony (VoIP). 3 infrastructures are Broadband Convergence Network (BcN), Ubiquitous Sensor Network (USN), and Next-Generation Internet Protocol (IPv6). And 9 new growth engines are Next-Generation Mobile Communications, Digital TV, Home Network, IT System on Chip (SoC), Next-Generation PC, Embedded SW, Digital Contents, Telematics, and Intelligent Service Robot. The success of the Strategy will enhance the quality of our lives and bring us into ubiquitous society.

But, with the advance of new services, intelligent devices such as telematics, home networking, and digital TV, the adverse effect of information society would become one of the major concerns in forthcoming information society. Users living in ubiquitous society propelled by IT839 Strategy will be very sensitive to security and privacy issues. We anticipate possible new information security threats. These are the diffusion of threats caused by network convergence, a sheer of collection and disclosure of personal information through pervasive devices, unestablished authentication framework for emerging transaction devices, and transition from the threats of the cyberspace into ones of the real world.

If we fail to prepare for adequate and timely policies and related technical solutions to cope with such security and privacy challenges, IT839 Strategy would not be successfully implemented in our society. For IT839 Strategy to be successful, we need the proper security policies to overcome the anticipated threats of the future. First, to develop trustworthy convergent network, we will develop cryptography and authentication technologies for secure network connection, agent technology for rapid hand-off, and will standardize interface technologies for secure interoperability among different networks. Secondly, to ensure ubiquitous service's safety, we will establish safety criteria for new intelligent devices, develop lightweight cryptography technologies for privacy protection, and develop DRM (Digital Right Management) technologies for protection of illegal digital contents distribution. Lastly, we will improve legal system in preparation for the future IT environments, and will try to formulate security culture.

It is obvious that a higher level of information security will be required to effectively sustain the ubiquitous society. For information security to be more effective, we should take not only technological countermeasures but also social and legal ones. MIC will try to build secure Korea by means of considering information security from the initial stage of IT839 Strategy implementation.