SECURITY AND PRIVACY FOR HUMAN SOCIETY

DR KAZUE SAKO

C&C INNOVATION INITIATIVE, CENTRAL RESEARCH LABORATORIES, NEC CORPORATION

Information Technologies, known as IT, have changed behavior of human being and thus human society. Yet, as there are many differences between IT world and real world, humans need to cope with technically driven restrictions in IT world. One big issue is the identification of a user. We need to authenticate users in order for them to enjoy IT services they have contract with. On the other hand, knowing the identifier or usernames of the user allows the server to learn how the user behaved, and possibly link several transactions in IT world which results in the invasion of user's privacy. A big advancement was made in the field of cryptography where the servers can authenticate an attribute of a user without knowing the identifier of the user. Based on the technologies called group signatures and/or blind signatures, the notion of anonymous authentication have been standardized in ISO/IEC SC27 projects. In this talk we will discuss what kind of privacy and security we can enjoy by employing anonymous authentication.

Kazue Sako is an Innovation Producer at NEC. She received B.S. degree in Science (Mathematics) and Ph. D degree in Technology from Kyoto University. Her research interest lies in how to benefit from cryptographic protocols in real life. She is currently a Director of The Institute of Electronics, Information and Communications.