December 19, 2013

Establishment of Cryptographic Protocol Evaluation Toward Long-Lived Outstanding Security (CELLOS) Consortium

The National Institute of Information and Communications Technology (President: Dr. Masao Sakauchi), Hitachi, Ltd. (President: Hiroaki Nakanishi), KDDI R&D Laboratories, Inc. (President & CEO: Yasuyuki Nakajima) and Nippon Telegraph and Telephone Corporation (President & CEO: Hiroo Unoura), together with experienced experts, companies and organizations both from Japan and overseas, established the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) Consortium (led by Tokyo University of Technology: Professor Satoru Tezuka). CELLOS strives to improve the security of cryptographic protocols that achieve functions such as authentication and privacy protection with the aim of promoting secure network utilization.

The consortium will consolidate security evaluation information including new attacks against cryptographic protocols and countermeasures against them, and promptly publish the results of examinations conducted by consortium experts. This will help system vendors and network users easily access the cryptographic protocol usage information examined by the experts, which has been difficult for individuals and stand-alone organizations to monitor. Furthermore, since the information can be utilized in determining the feasibility of future cryptographic protocols, it will lead to the promotion and the usage of secure cryptographic protocols and prospects for new ICT systems.

1. Founding Statement of the Consortium

In addition to promoting communication, advances in network technologies in recent years are opening up new possibilities in terms of information and communications, as technologies such as mobile networks and cloud computing continue to enrich our lives. At the same time, a higher level of security in privacy protection is required and it is no longer sufficient merely to encrypt and authenticate communications.

With that in mind, research and development is active in the field of cryptographic protocols, combining a whole host of cryptographic technologies. Currently, more than 400 cryptographic protocols have been internationally standardized. However, the security of these protocols has not been analyzed to a sufficient extent in actual ICT systems. In particular, little effort has been made to organize the latest security information on a global scale, engage in expert discussion, and make detailed technical security information widely available to the public.

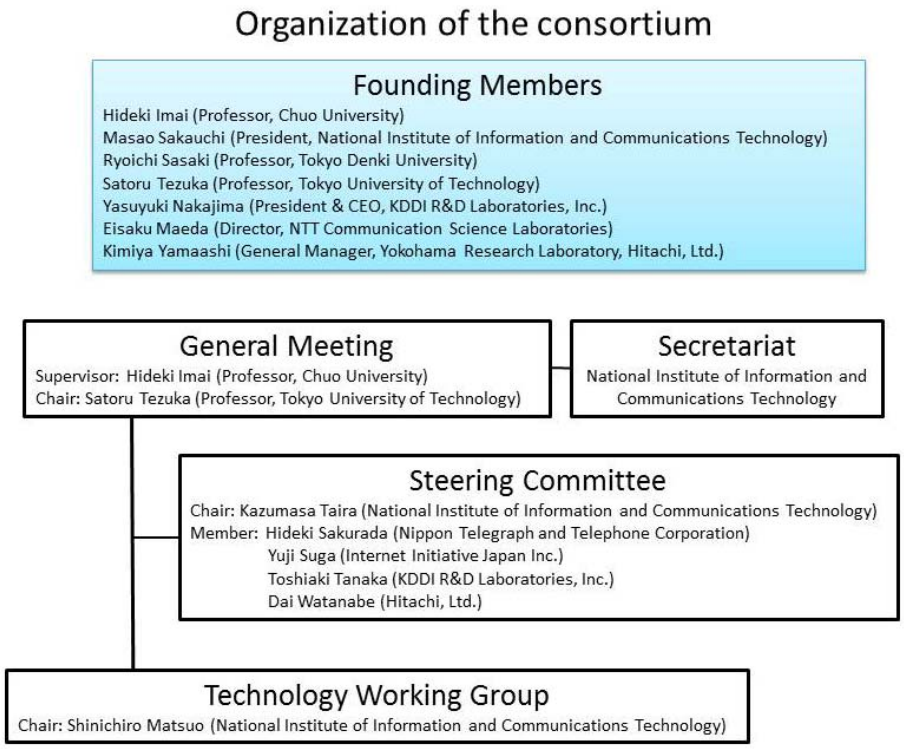
We therefore decided to establish the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) Consortium with the aim of promoting the widespread adoption of secure cryptographic protocols by organizing and sharing technical information relating to cryptographic protocols, discussing technical issues for actual ICT systems, and publishing the resulting security information.

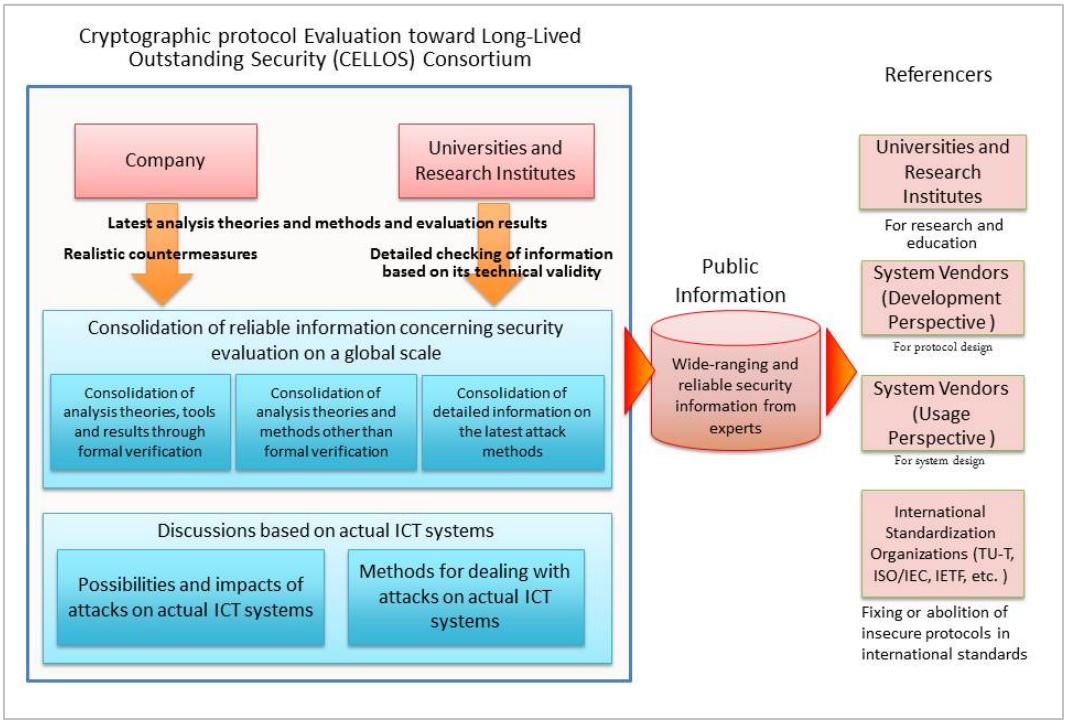
With involvement from universities, research institutions and companies conducting research into cryptographic protocols all over the world, the consortium will act as an international hub for organizing, sharing and disseminating information in an effort to ensure a high level of security for cryptographic protocols underpinned by an international cooperative framework.

Through activities such as these, we will continue to make significant contributions to improve network security and fulfill a pioneering and leading role in allowing people to use networks securely in the future.

2. Overview of the Consortium

The consortium consolidates theories and methods for conducting security evaluations, evaluates results of cryptographic protocols and information concerning new attack methods, confirms technical facts and discusses their impact on actual ICT systems as well as countermeasures. The consortium's activities will work in compliance with the cryptographic protocol evaluation system developed by the National Institute of Information and Communications Technology. Swiftly disseminating information gained from expert discussions regarding the security of cryptographic protocols enables judgments on the feasibility of cryptographic protocol usage and the design of secure cryptographic protocols, which promotes secure network usage.





3. Roles of Each Company

(1) National Institute of Information and Communications Technology (NICT)

NICT conducts research and development regarding cryptographic protocol evaluation technologies as a part of its research into network security. To date, NICT has promoted the standardization of ISO/IEC 29128 “Verification of Cryptographic Protocols,” an International Standard concerning the evaluation of cryptographic protocols, as a project editor, and launched a Cryptographic Protocol Analysis Portal Site to publish the results of cryptographic protocol evaluation conducted in accordance with ISO/IEC 29128. In the consortium, NICT will spread the results of research into cryptographic protocol evaluation, serve as the consortium’s secretariat and contribute to producing reliable results on a global scale.

(2) Hitachi, Ltd.

Hitachi, Ltd. has continued a range of research and development and standardization activities regarding security technologies including promoting the standardization of ISO/IEC 29128 “Verification of Cryptographic Protocols,” an International Standard concerning the evaluation of cryptographic protocols, as a project editor. In the consortium, Hitachi, Ltd. will utilize this knowledge to contribute to the realization of more secure network usage.

(3) KDDI R&D Laboratories, Inc.

KDDI R&D Laboratories, Inc. has engaged in research and development regarding security technologies to ensure that anyone can use network services with peace of mind. With respect to cryptographic protocols, which are essential for ensuring the security of services, KDDI R&D Laboratories, Inc. has conducted research into evaluation technologies based on computational complexity theory and developed its own security verification tool. In the consortium, KDDI R&D Laboratories, Inc. will use the theoretical evaluation technologies and the aforementioned unique tool to conduct cryptographic protocol evaluation.

(4) Nippon Telegraph and Telephone Corporation (NTT)

NTT has developed security technologies for realizing a safe and secure society. With respect to cryptographic protocol evaluation in particular, NTT has developed formal methods for cryptographic protocols, which enables rigorous evaluations by applying mathematical logic. In the consortium, NTT will focus on providing rigorous evaluation of cryptographic protocols based on technologies and expert knowledge it has acquired to date.

4. Direction of Future Progress

The consortium will swiftly publish information on the impact new attack methods have on actual systems and the countermeasures against such attacks through its website.
Detailed information on the consortium members and its activities is provided on the consortium’s webpage (https://www.cellos-consortium.org).

Technical Contact

Shin’ichiro Matsuo
Security Architecture Laboratory
Network Security Research Institute, NICT
Tel: +81-42-327-5782
E-mail: smatsuo@nict.go.jp

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
