Cybersecurity

Cybersecurity Research Institute

Director General Tetsuya Miyazaki

In the Internet of Things (IoT) era, many sensors and other devices will be deployed in our surroundings and connected to networks. They will allow us to lead more convenient and 'smart' lives. However, security measures for guaranteeing the safety of such devices are becoming a pressing issue behind the scenes. The scope that cybersecurity should cover is expanding daily; in particular, it must be able to protect people from information leaks and privacy violations when big data collected from such IoT devices is utilized. The Cybersecurity Research Institute conducts research and development (R&D) on how to deal with the latest pressing concerns and emergent issues in our information society.

The Cybersecurity Research Institute consists of the Cybersecurity Laboratory and Security Fundamentals Laboratory. The Cybersecurity Laboratory conducts R&D on advanced cybersecurity technologies and security testbed development and operations technology, while the Security Fundamentals Laboratory conducts R&D on cryptographic technologies.

Advanced cybersecurity technologies

We conduct R&D on monitoring cyberattacks and analyzing the increasingly sophisticated and evolved cyberattacks against government and other important infrastructure. We also engage in research that involves collecting and analyzing huge amounts of data from these diverse attacks in order to develop automatic countermeasures. We strive for the quick deployment of our R&D outcomes by verifying them on NICT's own cyber incident response system. In order to reinforce the capability of responding to cyberattacks against governments or critical infrastructure, we carry out R&D on visualization-driven security operation techniques and machine-learning-based analysis. NIRVANA-KAI (NICTER Real-network Visual Analyzer KAI) is a security platform against advanced persistent threats (APTs). It collects and analyzes security alerts provided by various security appliances and end hosts, and it automatically deploys new controls to the appliances to prevent APTs (Fig.1). This security platform, in combination with other security appliances, visualizes security-related events (e.g., cyberattacks) in real time and thus facilitates the implementation of prompt and adequate measures. We have been successfully transferring the technology of NIRVANA-KAI to Japanese industry since 2015.

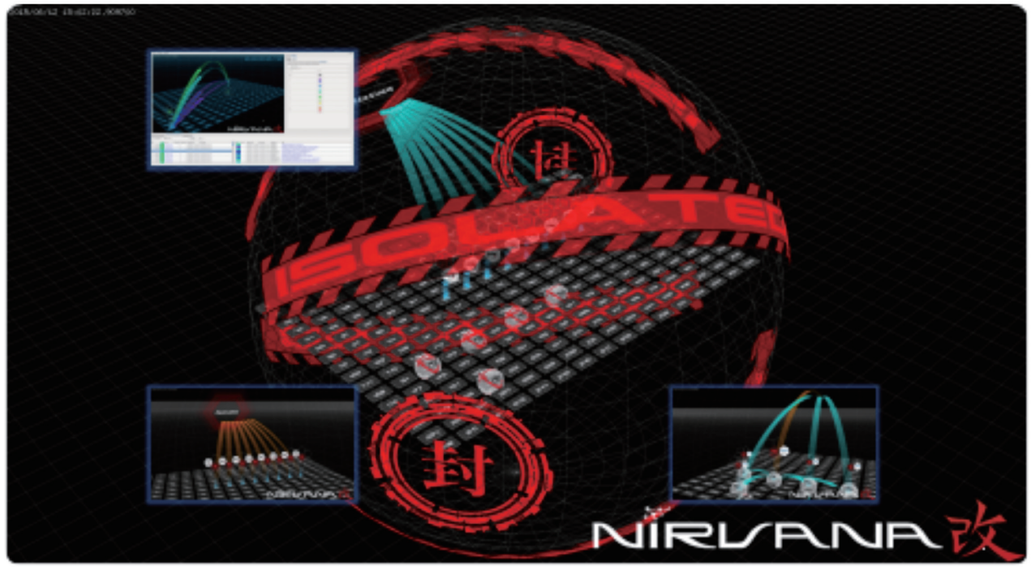

Fig.1 : NIRVANA-KAI
Visualization of defensive actuation in NIRVANA-KAI to isolate an infected class C address.

Security testbed development and operations technology

We oversee R&D on technologies for emulating cyberattacks in a safe environment. In particular, we are developing a security verification platform for verifying new protection technologies and countermeasures in an emulation environment. In this security testbed development, we are investigating a large-scale deception framework called STARDUST for luring human adversaries with the aim of attributing sophisticated cyberattacks such as APTs (Fig.2). STARDUST can quickly and flexibly build mimetic enterprise networks called 'parallel networks.' In a parallel network, APT malware can be executed and observed in a highly stealthy manner. A wormhole connects parallel and real networks so that the parallel-world network can pretend to have the same IP addresses as the real-world network. STARDUST enables us to stealthily observe adversaries' activities on parallel networks and to feed-forward the findings of the observation to APT countermeasures such as NIRVANA-KAI to promote their evolution.

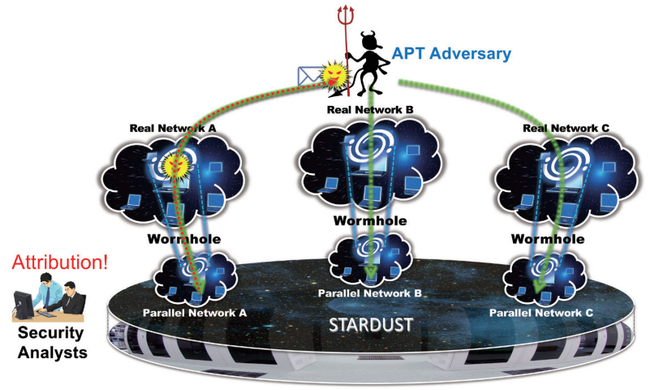

Fig.2 : STARDUST
A 'parallel network' imitating an organization network can be built on the STARDUST platform to attract attackers. It can observe the behavior of an attack on the network.

Cryptographic technologies

Our R&D on functional cryptographic technologies provides new functionalities to meet the evolving social needs accompanying the growth of IoT and to evaluate cryptographic technologies. We are contributing to the standardization of new cryptographic technologies and to the construction of safe and secure ICT systems. We also engage in R&D on privacy-enhancing technologies aimed at the safe utilization of personal data and technical support for appropriate privacy measures. Recently, deep learning has gained considerable attention in both industry and academia. Although the collection of massive amounts of data is vital for deep learning, it raises the issue of privacy. To resolve this issue, we are building a privacy-preserving deep learning system, where many learning participants perform neural-network-based deep learning over a combined dataset of all participants without revealing the participants' local data (Fig.3). This privacy-preserving deep learning system allows us to integrate isolated and hidden small data as big data. One of our promising technologies for realizing the system is 'homomorphic encryption,' which allows computations to be carried out on encrypted data without decryption. We are investigating the application of this system to a broad range of fields, such as medical genetics and illegal remittance detection, in a privacy-preserving manner.

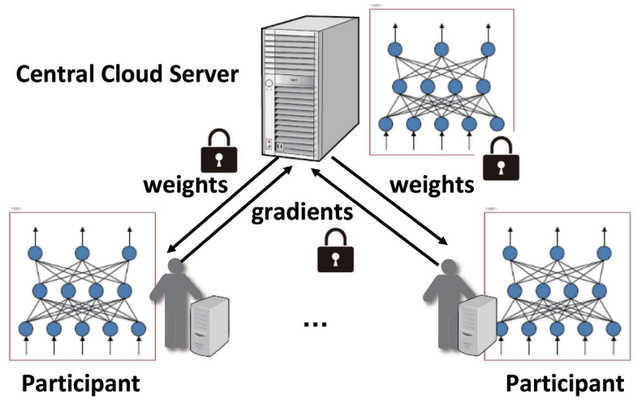

Fig.3 : Privacy-preserving deep learning
Many learning participants perform neural-network-based deep learning on a combined dataset of all participants without revealing the local data of individual participants.