Nippon Telegraph and Telephone Corporation
Mitsubishi Electric Corporation

New Authenticated Encryption Algorithm Features Robust Resistance to Multiple Misuse

TOKYO, March 17, 2014 – Nippon Telegraph and Telephone Corporation (TOKYO: 9432) and Mitsubishi Electric Corporation (TOKYO: 6503) announced today that in collaboration with the University of Fukui they have jointly developed an authenticated encryption algorithm offering robust resistance to multiple misuse. The algorithm has been entered in the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) project, based on which the algorithm is expected to be deployed for increasingly secure and reliable information technology.

The new algorithm's major advantage is its resistance to multiple misuse in authenticated encryption operations that provide simultaneous confidentiality and integrity.

One problem of misuse is an attacker making a fake message if plaintexts are released before their integrity is verified. Once a conventional system outputs decrypted plaintext from tampered data without authentication, the attacker can show tampered data as being non-tampered. Whereas this occurs with many conventional systems, the new algorithm fixes the problem, thereby enabling relatively low-memory devices to handle large-volume data.

Another typical problem is the reuse of nonce. In the case of a common authentication algorithm called Advanced Encryption Standard with Galois Counter Mode (AES-GCM), a non-repeatable special parameter, or nonce, is required to achieve security. However, the algorithm is largely bleached if the nonce is reused, so the new algorithm fixes this problem to maintain security even after multiple reuse.

The new algorithm accepts messages longer than the 64-gigabyte limit of AES-GCM, and it works faster than AES-GCM on many platforms.

CAESAR Competition

CAESAR is a competition organized to thoroughly evaluate authenticated encryption algorithms by testing their resistance to multiple third-party cryptanalyzing attacks to prove their security, applicability and robustness. Algorithms that receive third-party cryptanalysis through CAESAR are expected to gain wide acceptance, which is why this new algorithm has been submitted to the competition. Candidate algorithms will be screened annually and the first results will be announced on January 15, 2015, with the final results to be announced on December 15, 2017.

Based on the results of the CAESAR competition, NTT and Mitsubishi Electric intend to research and develop services and products for machine-to-machine (M2M) applications incorporating their new algorithm, thereby contributing to increased security and reliability in information technology.

Background

Cryptography is widely used to establish secure and reliable information technology by encrypting data with symmetric-key cryptography. However, symmetric-key cryptography does not necessarily prove data integrity. To prove data integrity, an authentication algorithm Message Authentication Code is required to detect forgery. Conventional algorithms can achieve either confidentiality or integrity. Combining the two is possible, but presents many problems. For example, recent threats to SSL/TLS involving attacks with BEAST (2011), BREACH (2013) and Lucky Thirteen (2013) have highlighted misuse problems. Authenticated encryption offers concrete instantiations, but the method is not used widely because its benefits are not fully recognized. In addition, conventional algorithms have demonstrated certain problems with weak keys.

PRESS CONTACT

Nippon Telegraph and Telephone Corporation
Service Innovation Laboratory Group
Public Relations, Planning Division
E-mail: randd@lab.ntt.co.jp

Mitsubishi Electric Corporation
Public Relations Division
TEL: +81-3-3218-2346
E-mail: prd.gnews@nk.MitsubishiElectric.co.jp

About Nippon Telegraph and Telephone Corporation

NTT (Nippon Telegraph and Telephone Corporation) is the world's largest global IT and telecommunications services company and is ranked 32nd on Fortune's Global 500 list. The company's roots go back over 100 years to the introduction of the telegraph in Japan and focuses today on innovation in the cloud, mobility, network and communications. The company had operating revenues of over US$130 billion for the fiscal year ended March 31, 2013 and employs 227,150 people worldwide. The company's subsidiaries include Regional Communications Businesses: NTT EAST, NTT WEST; Mobile Communications Businesses: NTT DOCOMO; Long-Distance and International Communication Businesses: NTT Communications and Dimension Data; and Data Communication Businesses: NTT DATA. For more information, visit http://www.ntt.co.jp/index_e.html

About Mitsubishi Electric Corporation

With over 90 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 3,567.1 billion yen (US$ 37.9 billion*) in the fiscal year ended March 31, 2013. For more information visit http://www.MitsubishiElectric.com

*At an exchange rate of 94 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2013