MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FOR IMMEDIATE RELEASE **No. 3649**

Customer Inquiries

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

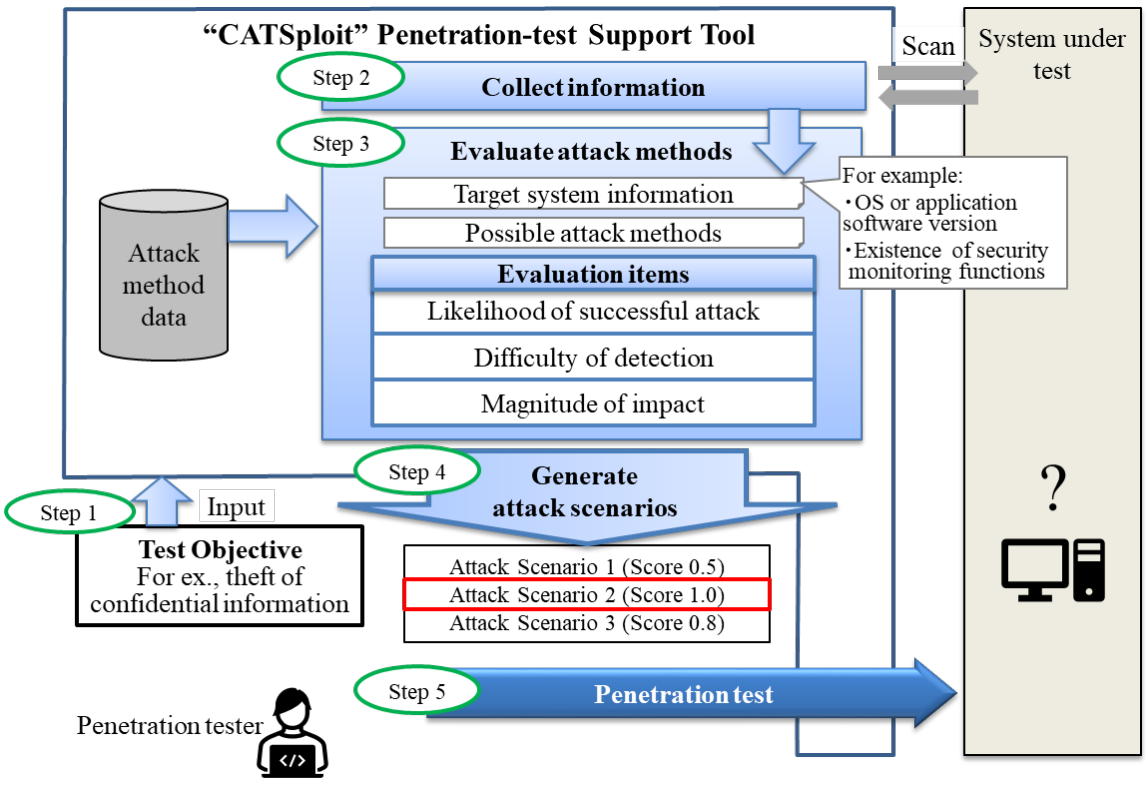
Media Inquiries

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric Develops World's First Penetration-test Support Tool that Generates Attack Scenarios from Hacker Perspectives

Expected to improve cyberattack resistance of all products connected to networks



Usage example of the support tool during penetration testing

TOKYO, December 5, 2023 – Mitsubishi Electric Corporation (TOKYO: 6503) announced today that it has developed the world's first[1] penetration-test[2] support tool, CATSploit, which automatically generates attack scenarios based on the test objectives of a penetration tester, such as the theft of confidential information, to evaluate the effectiveness of test attacks. Using the attack scenarios and resulting test results (scores), even inexperienced security engineers can easily perform penetration tests.

In recent years, control systems including infrastructure, factory equipment, etc., have become increasingly

[1] According to Mitsubishi Electric's research as of December 5, 2023
[2] Test to confirm that if a system or equipment can be compromised by an actual attack

connected to networks, raising the risk of disruptions, such as power outages or public transportation shutdowns, due to cyberattacks. The need to implement security measures in such systems has become urgent. In addition, ISA/IEC 62443[3] standards require that fuzzing[4] and penetration security tests be performed on systems and equipment to evaluate their resistance to cyberattacks, including vulnerabilities due to implementation or configuration errors. Penetration testing is highly sophisticated and requires the involvement of white-hat hackers[5] to actually attack the system or product being tested, but such individuals, who must possess very high levels of expertise, are scarce and difficult to find.

Mitsubishi Electric, by focusing on the factors that white-hat hackers consider when selecting their attack vectors, has now developed a penetration-test support tool that generates lists of possible attack scenarios and their effectiveness (expressed as numerical scores).

Details of the tool will be presented on December 6 (11 am local time) during the Black Hat Europe 2023 Arsenal in London, which will take place on December 6 and 7.

Features

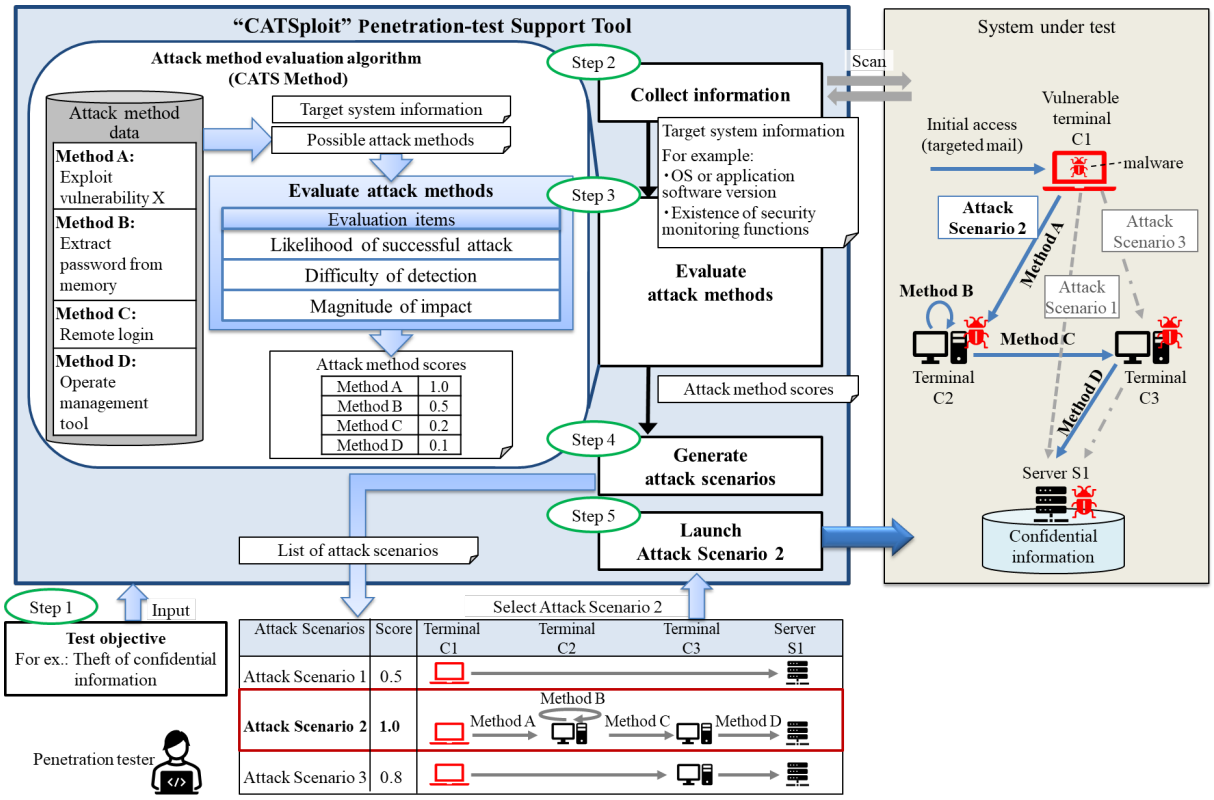
1) Automatically generates attack scenarios from white-hat hacker's perspective

- Mitsubishi Electric focused on factors that white-hat hackers consider when choosing their attack methods, such as the likelihood of successful attack, the difficulty of detection, and the magnitude of impact. By adjusting for the objectives for specific tests, the system is able to automatically generate scenarios that show the steps necessary to implement an attack to achieve those objectives.

2) Optimal tests evaluate the effectiveness of attack scenarios from a white-hat hacker's perspective

- Mitsubishi Electric's proprietary CATS[6] method calculates the effectiveness of each attack method (expressed as a numerical score) from the perspective of a white-hat hacker, based on which a list of attack scenarios is proposed so that the most effective scenario (highest score) can be selected.
- The CATS evaluation takes into account not only known system information, such as the operating system, application version and security monitoring devices, but also missing system information, which helps to realize attack scenarios that closely replicate an actual attacker's point of view.
- The automated evaluation of attack scenarios likely to be used by white-hat hackers enables less-experienced security engineers to perform penetration tests with ease.

[3] Security Standards for Industrial Control Systems
[4] A test method for detecting software defects or vulnerabilities by entering invalid or incorrect data
[5] Ethical hackers who use advanced knowledge and computer technology to identify security issues, etc.
[6] Cyber Attack Techniques Scoring: Proprietary method of Mitsubishi Electric for evaluating the effectiveness of attack vectors



CATSploit penetration-test support tool

Future Development

To further improve the cyberattack resistance of systems and devices developed by Mitsubishi Electric, the company will continue to research and develop this new tool with the goal of using it for actual security testing of the company's products by 2026.

###

About Mitsubishi Electric Corporation

With more than 100 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. Mitsubishi Electric enriches society with technology in the spirit of its "Changes for the Better." The company recorded a revenue of 5,003.6 billion yen (U.S.$ 37.3 billion*) in the fiscal year ended March 31, 2023. For more information, please visit www.MitsubishiElectric.com

*U.S. dollar amounts are translated from yen at the rate of ¥134=U.S.$1, the approximate rate on the Tokyo Foreign Exchange Market on March 31, 2023