Security Orchestration with a Global Threat Intelligence Platform

Takaaki Koyama, Bo Hu, Yukio Nagafuchi, Eitaro Shioji, and Kenji Takahashi

Abstract

The NTT Innovation Institute, Inc. has developed a system for collecting and distributing information on the threats posed by cyber-attacks: the Global Threat Intelligence Platform (GTIP). By connecting with NTT Secure Platform Laboratories' security orchestration technologies, GTIP makes it possible to run advanced cyber defenses based on threat data. In this article, we demonstrate how we jointly built and connected these technologies and discuss their future global deployment.

Keywords: GTIP, security orchestration, network security

1. Introduction

Cyber-attacks against companies and public organizations have continued to evolve in recent years. Security appliances have been used to detect, filter, and otherwise protect against these attacks—primarily with the help of virus definition files and signature updates. However, attackers have been able to employ new techniques to hack into networks while avoiding detection. As a result, data leaks, tampering, and other damage incurred via the Internet continue to be a problem. To deal with this, we may need security operations that take a more unconventional approach. In this article, we introduce these new types of cyber-attacks and the initiatives to deal with them at NTT's laboratories and NTT Innovation Institute, Inc. (NTT I^3); we also present our jointly developed cooperative system along with plans for its global deployment.

2. New types of cyber-attacks and countermeasures

Attackers use spear phishing emails, watering hole attacks, and other strategies to get their targets to download malicious programs on the Internet. Once installed on a victim's computer, these programs accept remote commands to leak data, upgrade themselves, set up command-and-control (C&C) servers, and cause other damage. Because this series of operations is conducted over the Internet and even newer malicious programs continue to be created, we believe that the following three-step process is an effective way to respond to these threats.

(1) Actively collect external threat intelligence to prevent damage

Threat intelligence includes blacklists of Internet protocol (IP) addresses and Uniform Resource Locators (URLs) as well as the behavior of the latest malicious programs discovered on the Internet; this information is helpful in preventing both infiltration and subsequent actions by attackers.

(2) Automatically configure security operations to respond quickly

By promptly configuring the appropriate countermeasures as new malicious programs emerge, we can mitigate their effects.

(3) Choose appropriate appliances and countermeasures using diverse threat intelligence

There are a variety of security appliances installed within private companies' intranets as well as at the connection points between these intranets and the Internet. By configuring the appropriate appliances and countermeasures, we can stop attackers' Internet-based actions.

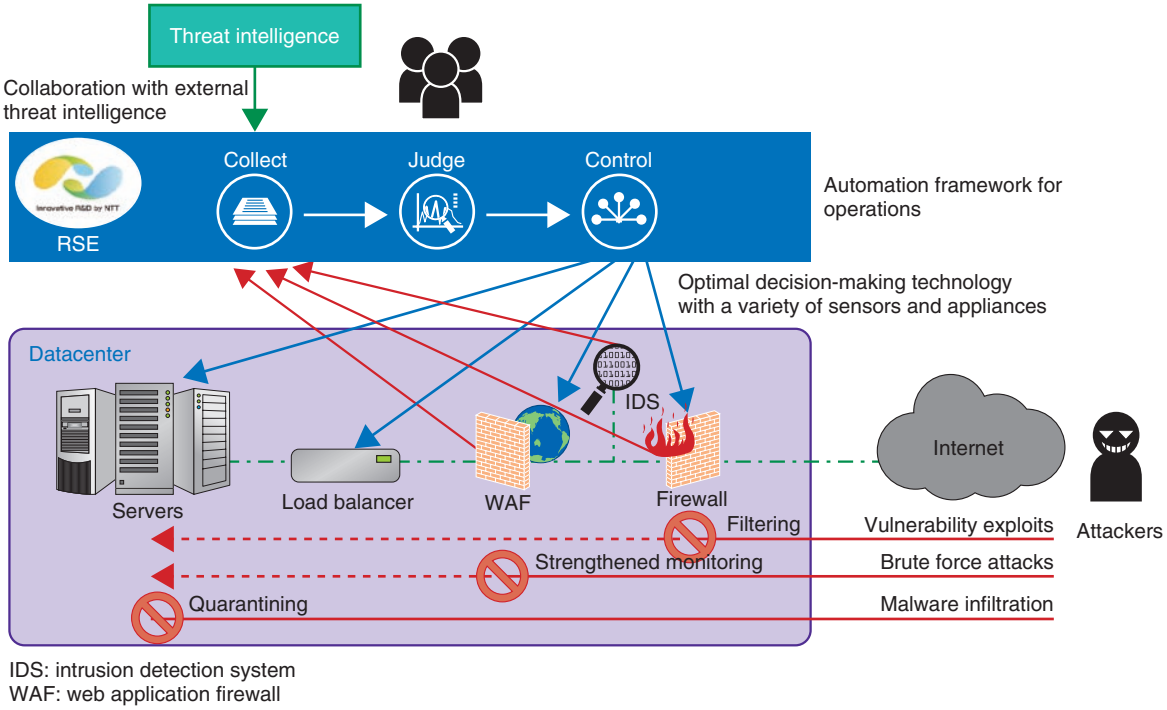

Fig. 1. Resilient Security Engine (RSE).

3. Initiatives at NTT Secure Platform Laboratories

At NTT Secure Platform Laboratories, we have researched and developed security orchestration technologies to automatically respond to cyber-attacks [1]. In the interest of establishing methods of coping with new and even more sophisticated cyber-attacks in the future, we are also currently carrying out research and development (R&D) efforts focused on a Resilient Security Engine (RSE), which implements three technical components (**Fig. 1**).

3.1 Proactive defense technologies incorporating threat intelligence

We actively collect external threat intelligence to protect users from Internet-based cyber-attacks. We specifically collaborate with a threat intelligence platform that collects cyber-attack data from around the world, blacklisting IP addresses and URLs associated with attackers to prevent attacks and their subsequent damage before they can occur. For example, when suspicious behavior is detected, we receive information about the source of the attack from the threat intelligence platform; this allows us to make more accurate decisions.

NTT Secure Platform Laboratories is moving forward by connecting the RSE system and the threat intelligence platform developed by NTT I^3. By using an automation framework for operations (as explained in the next section) along with a variety of sensors and appliances, our technology is able to choose optimal countermeasures; we can thus expect attacks and threats to be handled promptly and appropriately.

3.2 Automation framework for security operations

When an incident occurs, the datacenter's security operators determine what course of action to take after they confirm the type of attack from logs that are used to detect attacks and threats. The security operators must then find and send commands to the appropriate hardware or software solution (e.g., the firewall) dictated by the network structure. The aforementioned process of collecting data on attacks and threats is currently consolidated under a Security Information and Event Management (SIEM)*1 system;

*1 SIEM: A system that collects log data from servers, network devices, and other security-related equipment. When a malfunction, attack, or other unusual event is detected, the system notifies its administrators with information on and steps to resolve the situation based on the collected log data.

dedicated tools provide a simplified interface to the firewall's controls. However, operators must manually respond to incidents using multiple administrative systems and control tools with an understanding of security policies and network structures. As a result, these operations are problematic both in terms of the time and effort they require.

For these reasons, we are proposing an automation framework that will promptly carry out security operations—from data collection to decision making to response. Our proposed framework does not simply define a single program to link multiple administrative systems and control tools with one another; it is also intended to allow users to choose from different methods of responding to the same types of attacks (e.g., malware infections) for a desired level of security. Responses can include strengthened monitoring, filtering, and quarantining; for example, users should be able to filter network traffic or completely isolate a device from the network. Furthermore, our proposal is intended to implement general-purpose operations that can make use of different types of equipment (e.g., physical switches or virtual switches in a hypervisor) according to the user's information and communications technology (ICT) environment for the same attack response (e.g., network filtering).

3.3 Optimal decision-making technology with a variety of security sensors and appliances

One effective strategy for dealing with multi-vector attacks is a layered area defense using several varieties of security sensors and appliances distributed across a user's ICT environment. However, intrusion detection systems (IDSs)[*2] and web application firewalls (WAFs)[*3]—as well as other similar sensors and appliances—have been designed to run independently; they do not give sufficient consideration to sharing data and working together with other devices. Although some vendors offer value-added solutions to connect their own products, attempts to create synergy by improving detection and control capabilities with products from multiple vendors have not taken off; this has led us to believe that the effectiveness of linking products together is limited.

For these reasons, we have been researching and developing technology that collects information on threats from a wide variety of sensors, determines what types of attacks or threats it encounters as well as the best way to deal with them, and finally, makes use of the most suitable network devices to respond to them. This technology can combine data from multiple sensors to determine when attacks or threats are present and how to deal with them appropriately; it can also manage an attack or threat situation by defining relationships between the sensors' data. Using configuration data for the appliances distributed across a network, the technology can even select a location close to the root cause of an attack from several candidates and direct its response there.

4. Initiatives at NTT I^3

This section introduces the Global Threat Intelligence Platform (GTIP) being developed by NTT I^3. GTIP is a comprehensive platform for collecting, analyzing, and distributing actionable intelligence (data) on cyber-threats from around the world. We intend to use this platform within the NTT Group to contribute to improving the quality of the entire group's security services.

GTIP has three major features: data collection, which involves gathering diverse threat data from both inside and outside the NTT Group; data analysis, which involves employing advanced analytics based on proprietary technology; and data sharing, which provides flexible input and output interfaces. By combining these features, we can counteract the complex and wide-ranging threats that in recent years have become difficult to defend against through conventional methods (**Fig. 2**).

4.1 Data collection

GTIP collects data provided by proprietary commercial web crawlers, large numbers of community vendors, the NTT Group's security professionals (e.g., managed security services providers), and threat sensors (e.g., honeypots) installed around the world. We plan to continue adding more data sources, such as those obtained from network traffic.

4.2 Data analysis

Using the advanced program analysis technology (also known as taint analysis[*4] technology) developed by NTT I^3 in collaboration with NTT Secure

*2 IDS: A system that monitors the packets sent over a network and notifies its administrators when any indication of unauthorized access occurs.

*3 WAF: A firewall that can detect and protect against unauthorized breaches from external networks (e.g., the Internet) using data exchanged with web applications.

*4 Taint analysis: An analysis technique that tags important data at runtime and then closely follows data flows so it can detect when data have been exfiltrated.

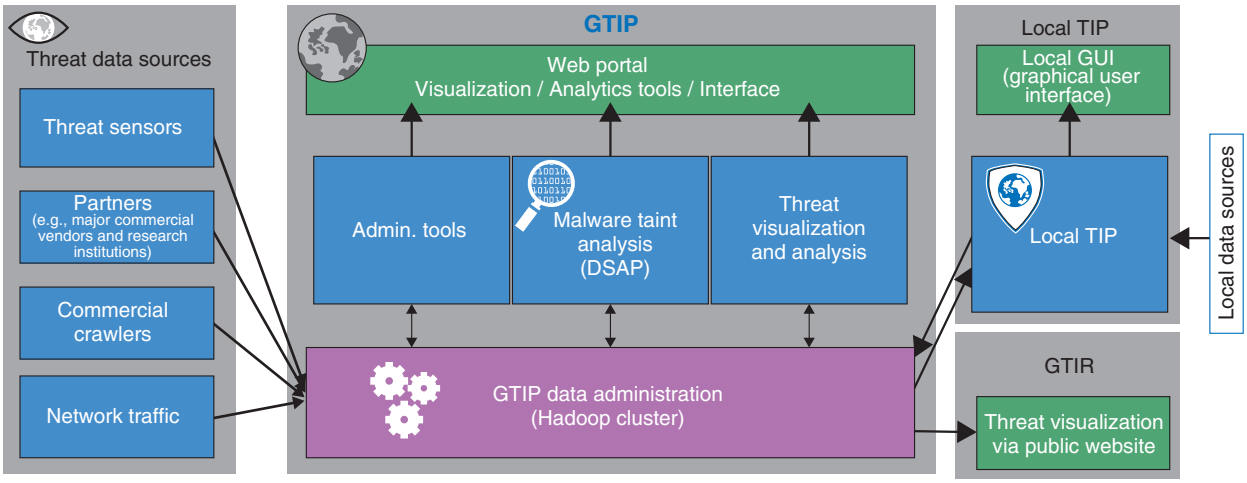

Fig. 2. GTIP.

Platform Laboratories, we can create a list of malicious servers with which malware communicates. By also calculating reputations and analyzing correlations in the data, we can produce easily actionable intelligence supported by detailed evidence and maliciousness ratings.

4.3 Data sharing

GTIP stores the enormous amount of data it collects and analyzes in a Hadoop cluster that restricts access according to permissions configured for individual types of data. GTIP provides a web portal, an Apache Thrift application programming interface, and other user-facing interfaces to support many different service patterns and requirements. GTIP also provides a client-side local TIP that synchronizes GTIP data with users' local environments, and we have taken it upon ourselves to supply information through a public website: the Global Threat Intelligence Report (GTIR) [2].

One of GTIP's use cases is increasing our ability to detect and defend against attacks by supplying shared intelligence as input to firewalls, IDSs, and other network security devices. However, it is not easy to integrate these disparate components because different user environments have different security policies for making decisions and different interfaces for controlling devices. We expect RSE connections to serve as an intermediate layer for alleviating these obstacles.

5. System for connecting GTIP with RSE and future global deployment

NTT Secure Platform Laboratories and NTT I^3 currently conduct periodic information exchanges. At the beginning of 2015, we found that the collaboration between RSE and GTIP had allowed us to strengthen our cyber defenses even further; RSE was reinforced with threat intelligence for defending against more advanced cyber-attacks, and GTIP benefited from simpler integrations with user environments. As a result, during the first quarter of 2015 we jointly developed a proof of concept for connecting RSE and GTIP.

Although we can think of many different configurations for connecting the systems together, we implemented automatic defenses in our demonstration based on GTIP data (**Fig. 3**).

As can be seen in the figure, GTIP first detects an attack (1) and then notifies RSE with data relevant to the attack (2). Finally, RSE determines a response based on the attack data and configures the appropriate network devices to block the attack (3). Automating this series of actions allows us to proactively defend ourselves. Through this experiment, we proved that we could successfully connect RSE and GTIP together and could thus expect to make further progress on implementing and enhancing the combined system. Our next step will be to demonstrate that this solution works in actual user environments during our GTIP beta trial in the second half of 2015. We expect to continue discovering issues (some related to operational logistics) and considering ways

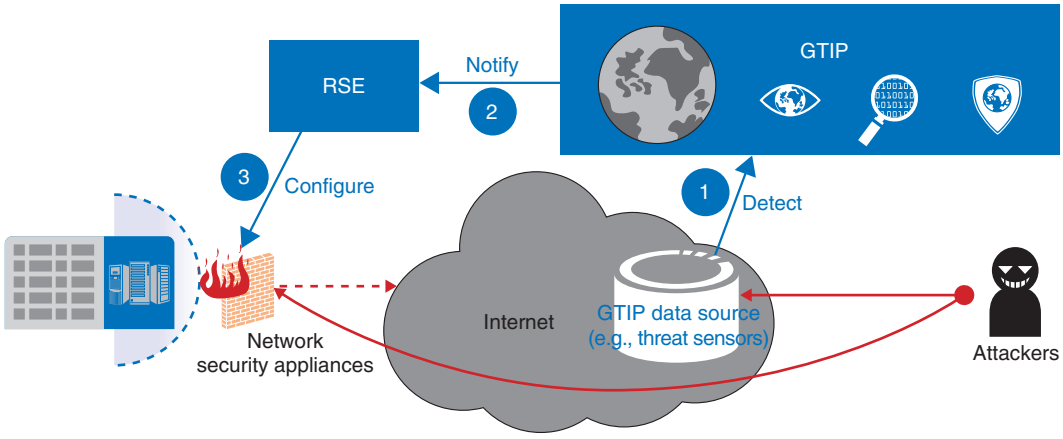

Fig. 3. System for connecting GTIP and RSE.

to resolve these issues in the future.

References

[1] T. Koyama, K. Hato, H. Kitazume, and M. Nagafuchi, "Resilient Security Technology for Rapid Recovery from Cyber Attacks," NTT Technical Review, Vol. 12, No. 7, 2014. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa3.html

[2] Website of NTT I^3 GTIR, http://www.nttgroupsecurity.com

Takaaki Koyama
Senior Research Engineer, Network Security Project, NTT Secure Platform Laboratories.
He received a B.A. and M.M.G. in media and governance from Keio University, Kanagawa, in 1994 and 1996. He joined NTT Software Laboratories in 1996 and began studying software CALS (client access license). Since 1999, he has been developing network equipment and studying GMN-CL, a kind of IP-virtual private network technology. His research interests also extend to enterprise cloud network systems and security orchestration systems. He is a member of the Information Processing Society of Japan (IPSJ).

Bo Hu
Researcher, NTT Secure Platform Laboratories.
He received an M.S. in wireless network engineering from Osaka University in 2010 and joined NTT the same year. He has mainly been engaged in researching network security technology and inter-cloud technology and has developed security orchestration architecture and inter-cloud protocols. He has also worked on cloud computing standardization activities in the Telecommunication Standardization Sector of International Telecommunication Union, and other standardization organizations. He received the Telecommunication Technology Committee standardization performance award and has contributed to Institute of Electrical and Electronics Engineers (IEEE)/Institute of Electrical, Information and Communication Engineers (IEICE) international academic conferences as a member of the Technical Program Committee or Organizing Committee.

Yukio Nagafuchi
Senior Research Engineer, Network Security Project, NTT Secure Platform Laboratories.
He received his B.S. and M.S. in science and engineering from Saga University in 1996 and 1998. He joined NTT in 1998 and has been engaged in the design and development of network systems, VoIP (voice over IP) network systems, and virtual network systems. His current interests include traffic and security issues in computer networks. He is a member of IEICE and IPSJ.

Eitaro Shioji
Software Engineer, Security, NTT Innovation Institute, Inc.
He received a B.E. in computer science and an M.E. in communications and integrated systems from Tokyo Institute of Technology in 2008 and 2010. He joined NTT in 2010 and has been conducting research on network security. Since joining NTT I^3 in 2013, he has been developing a threat intelligence platform. His current and past research interests include vulnerability exploitation and mitigation, mobile security, malware analysis, and secure network coding. He is a member of IEICE and received the Information and Communication System Security Research Award from IEICE in 2013.

Kenji Takahashi
VP, Product Management, Security, NTT Innovation Institute, Inc.
He received his B.S., M.S., and Ph.D. in computer science from Tokyo Institute of Technology. He has over 28 years of international experience in the information and communication industry. He has led many projects at NTT R&D in Japan, including those related to cloud computing, software engineering, digital identity management, collaboration environments, and ubiquitous computing. He was previously President and CEO of NTT Multimedia Communication Laboratories, Inc. (NTT MCL) in Silicon Valley, where he successfully launched and led open source, open standard based cloud, and software-defined networking projects. He was a visiting scientist at the College of Computing at Georgia Institute of Technology and a member of the Discovery Park Advisory Council at Purdue University. He received the Kiyasu Special Industrial Achievement Award from IPSJ for his pioneering work on federated identity management. He is a member of IEICE, IPSJ, IEEE Computer Society, and Association for Computing Machinery.