Study of Cost-effective Threat Analysis Methods for Embedded Devices in Various Domains

SERIKAWA Masataka, NIWA Toru, YOSHIOKA Sachie and HARADA Shintaro

By the arrival of the IoT era, embedded devices that connect to the Internet are being exposed to cyberattacks[1]. In order to provide products that users can use with assurance, it is necessary to analyze security threats and take countermeasures to avoid important cyberattacks. OMRON had a problem that there was no threat analysis method that focused on availability for embedded devices, and there was no efficient and effective threat analysis method.

To address these issues, we studied a method for effectively and efficiently analyzing security threats to embedded equipment products and found that it had the potential to significantly reduce the number of person-hours required for threat analysis while extracting all important threats and implementing countermeasures against those extracted threats.

1. Introduction

1.1 Growing cybersecurity risks

With the advent of the IoT era, all hardware has become connectable to the Internet, prompting the provision of new services or improved convenience in various fields. On the other hand, now with all devices internet-connectable, cyberattacks on embedded devices have become a reality, making cybersecurity incident prevention one of the challenges facing businesses. OMRON's products and services are similarly exposed to growing cybersecurity risks. OMRON provides public systems, health services, manufacturing systems, and other products and services used in a broad range of fields and handles large volumes of personal safety-related products and confidential information, including personal information. Hence, any cybersecurity incident involving OMRON would have a massive negative impact on society. With its products varied in characteristics to serve diverse business domains, OMRON now requires security measures tailored to individual business operations. So far, OMRON has not been armed with any systematic product security measures for diverse business domains and has managed to cope by relying on developers' skills. OMRON has already been required to analyze security threats with high efficiency during development processes and take appropriate countermeasures to prevent security incidents before they occur.

Contact : *SERIKAWA Masataka* masataka.serikawa@omron.com

1.2 Challenges to security measures at OMRON

Information systems use standard devices and operating systems. Besides, they often use common middleware and the like. With security know-how abundantly available, risks posing potential threats are systematically classified, and countermeasures are also systematically developed. When it comes to embedded devices, it's a whole different story. These devices differ in technology and risk from one domain to another. While searches are underway for a variety of countermeasures, publicly available know-how is scarce. Therefore, embedded devices require countermeasures based on the results of the analysis of security threats in products or their use environments. However, considering such factors as the increasing size of the software installed in recent embedded devices or the use of open-source software, it is unrealistic to perform an exhaustive threat analysis and take countermeasures for each product or use environment. Besides having a diverse product lineup, OMRON had to eliminate backtracking in new product developments or new business deployments by performing effective and efficient threat analysis upstream to product development and identifying high priority risks to be addressed.

To ensure the security of OMRON's flagship products, in other words, embedded devices, we specified the following requirements that threat analysis must meet:

- Applicability to diverse business domains
- Ability to detect critical risks in the planning stage

• Efficient implementation (at low cost in a short period)

We focused on developing a threat analysis method aiming to reduce security risks and maintain and enhance our market competitiveness.

2. Focus points for product security measures

"Product security measures" refer to efforts to protect the confidentiality, integrity, and availability of products from various security threats and recently mean security measures implemented with particular weight on cyberattack threats in an IoT world.

Security threats to products exist in each of the phases from product planning to disposal. Hence, implementation is necessary for security measures that will remain suitable for products throughout their entire lifecycles. We present below general security measures in the four phases of planning, development, operation, and disposal.

• Planning phase
Threat analysis is performed on the whole system to which a product belongs to grasp security threats surrounding the product and evaluate them for risk. The risk evaluation results are used to consider the development period and budget, with risk countermeasures factored in, to establish security requirements. In this way, the level of effort for security is determined to implement countermeasures against vulnerabilities attributable to the system requirements.

• Development phase
The security requirements established in the planning phase are used to design and implement security measures. Besides, vulnerabilities attributable to program coding and other implementation methods are prevented from making their way in. Moreover, in the development phase, security requirements-based verification is performed for vulnerabilities. Through the above, countermeasures are taken against vulnerabilities included during implementation.

• Operation phase
The operation phase refers to a state during which a product has market currency. During this phase, information is collected on vulnerabilities newly found in a product or its operating system or middleware to ensure prompt implementation of appropriate countermeasures, such as patch provision or mitigation measures, to prevent security incidents before they occur. If an incident should occur, similar countermeasures must be implemented to minimize the impact.

• Disposal phase
Products may be disposed of on account of replacement purchases, termination of use, breakdowns, or some other reasons. Therefore, reliable data erasure or product recovery mechanisms must be established in advance as security measures to prevent disclosure of confidential information in products.

Security measures are thus varied depending on the phase. In any case, threat analysis must be performed to grasp security threats throughout the entire product lifecycle for exhaustive identification of critical risks. Accordingly, we turned our attention to a threat analysis method implementable from the planning stage and suitable for our products.

2.1 Common security threat analysis methods

The most commonly used threat analysis methods include the following (Table 1):

Table 1 Comparison of threat analysis methods[3)]

Analysis method		Number of person-hours	Risk identification accuracy	
Baseline Approach		Small	Medium	Low in suitability on account of being countermeasure-based risk identification
Informal Approach		Small	Unknown	Dependent on specific personnel and experience
Detailed Risk Analysis	Asset-based	Medium	Medium	Exhaustive identification of threats to components
	Attack tree analysis (ATA)	Large	Medium	Exhaustive risk identification based on attack entry points
	Fault tree analysis (FTA)	Large	Medium	Exhaustive risk identification based on expected final damage
Combination Approach		Medium	Medium to high	Accuracy variable depending on the combination

• Baseline Approach
In this approach, existing standards and criteria provide the basis for specifying certain security levels to be secured in advance for a typical assumed system. Security requirements for achieving these security levels are then established to check, among other things, the compatibility between the analysis target system and countermeasures.

• Informal Approach
In this approach, organizational or personnel's experience and judgments are relied on to perform risk analysis.

- Detailed Risk Analysis
  A method, such as attack tree analysis (ATA)[2], is used to perform risk analysis on the analysis target system per se or a business undertaking implemented based on it in terms of the evaluation indicators of criticality (or the level of damage that may occur), threat, and vulnerability.

- Combination Approach
  This approach aims at improving drawbacks through advantages taken from multiple methods to enhance work efficiency and exploit different evaluation viewpoints to improve analysis accuracy and prevent increases in person-hours worked. However, it should be noted that no guidelines have been presented for how to make combinations of methods or how to handle inherent differences among individual systems or business undertakings.

These general threat analysis methods differ in analysis approach from one another. The analyst must choose an appropriate one to suit the analysis target. While exhaustive analysis is possible depending on the method, many analysis person-hours will be required depending on the analysis target's scale.

2.2 Challenges in the application of threat analysis to OMRON's products

The Detailed Risk Analysis method presented above relies on such a method as attack tree analysis (ATA) to analyze security threats to various information assets and functional assets. The number of threats thus identified reaches somewhere between several hundred and several thousand, depending on the number of all assets multiplied with that of various attack patterns. If such an exhaustive method had been adopted for OMRON's products, security measures might have required more person-hours than required to design and develop the products' main requirements. Meanwhile, the adoption of the Combination Approach would have resulted in coping guidelines insufficiently tailored to the characteristics of OMRON's business domains. The reason is that OMRON deploys products and services in business domains centered around factory automation (hereafter FA), healthcare, mobility, and energy management, handles a diverse range of information and functions, and is faced with risks of varied types and severity levels.

There are countermeasures established in the information system domain based on the outcomes of past efforts in the real world. In the embedded device domain, however, devices to be covered and information to be handled are so diverse that no common threat analysis method so far has been established. Thus, we expected that we would have to rely on different threat analysis methods for each business domain or product to take security measures and hence that each business domain would require enormous workloads for know-how accumulation, human resources development, mechanism/regime construction, and other tasks. These considerations led us to turn our attention to a threat analysis method applicable to diverse business domains and efficient implementation (at low cost in a short period) and decide to develop a threat analysis method suitable for OMRON's flagship products of embedded devices.

3. Our proposed threat analysis method

Some authors[4] have proposed creating a list of threat-prone points in a system with specific architecture features as a low-cost threat analysis method in the planning phase to reduce the cost of threat analysis for systems with similar architecture. However, such a method requires creating a list of threat-prone points for each type of architecture and hence will not easily produce expected effects for companies with a broad product lineup, such as OMRON.

Our proposed threat analysis method has as its characteristics the following two capabilities:

(1) Focusing on protection target assets and access routes thereto to filter threats and use threat classification names as guide words to control the divergence of analysis
(2) Setting appropriate evaluation criteria for business domains and system characteristics to perform analysis based on criteria tailored to individual products

Our proposed method aims at efficiently performing risk analysis by identifying and prioritizing risks using these capabilities to deal with identified risks in the order of their priority without leaving critical risks unaddressed. Besides, this method uses the assets to be protected as the starting point of analysis and hence allows analysis from the product planning and conceptual stages, whereby analysis results can be reflected in development plans.

3.1 Settings reflecting the business domain

For a business domain and system characteristics to be reflected in a development plan, it is necessary to set the filtering conditions for efficiently narrowing down the list of security threat candidates and the risk evaluation criteria for threats identified.

3.1.1 Setting the threat filtering conditions

For security threats to the analysis target product, identification must be performed of protection target assets, access routes, and threat types for each business domain. Where cyberattacks actually pose potential threats, there are always attack-target protection target assets and access routes thereto. Hence, attack-target protection target assets and access routes must be put into combinations for analysis. The threat filtering conditions set here as prerequisites for threat analysis are Protection Target Asset Levels (Table 2) and Access Route Levels (Table 3). The Protection Target Asset Levels must be set, taking into account the characteristics of the business domain to reflect the viewpoints of safety (deaths and serious and minor injuries), affected ranges (society, enterprises, and individuals), and operating losses (monetary amount of damage). As for the Access Route Levels, the presence or absence of physical barriers (e.g., room entry and exit control) or the height of the barriers (e.g., firewall protection level) must be determined to suit the system characteristics. Facilities, such as public systems or factory manufacturing lines, usually require stable system operation. Hence, for OMRON's products, importance is attached to their availability. For general information systems, risk considerations priority goes first to confidentiality, followed by integrity and then availability. For OMRON's products, it is critical to set the Protection Target Asset Levels, keeping in mind the priority order of availability, integrity, and then confidentiality. For example, a threat analysis of an FA controller covers assets at Protection Target Asset Level "Medium" or higher and access routes at Access Route Level "Medium" or higher.

Besides, potential threats must be classified ahead of threat identification as guide words (Table 4) to analyze the threat classification's applicability to combinations of protection target assets and access routes.

Table 2 Typical Protection Target Asset Level settings (FA controller)

Level	Protection target asset (information)	Protection target asset (functional)
High	Program or recipe data for operating the control system	Device operation control function; and program-and-parameter-changing function
Medium	Quality control data	Access control function (authentication)
Low	Critical monitoring information for the device	Ladder program debugging function

Protection target assets are divided into information assets and functional assets.

Table 3 Typical Access Route Level settings (FA controller)

Level	Access route
Remote (High)	Equipped with (a) communication means directly accessible via the Internet or equipped with (a) wireless communication means.
Adjacent (Medium)	Connected to an intranet isolated by a firewall or VPN.
Local (Low)	Internet connection route unavailable and direct device manipulation required.

Table 4 Typical guide words (STRIDE)[5)]

Threat type	Remarks
Spoofing	Assumption of a false identity
Tampering	Falsification of information
Repudiation	Denial of the fact of committing an attack
Information Disclosure	Disclosure of personal information or confidential information to external parties
Denial of Service	Forced stoppage of service
Elevation of Privileges	Theft and abuse of administrator or equivalent privileges

3.1.2 Setting the risk evaluation criteria

Appropriate evaluation criteria must be set for the business domain in advance based on the risk occurrence probability and severity (Table 5) to perform risk evaluation of threats identified. Mission-critical products or services require risk countermeasures, even though their risk occurrence probability is low. The risk evaluation criteria must be set to suit the circumstances surrounding the product. Table 6 specifies occurrence probability levels based on combinations of access route, need of expertise, and attacker's effort conditions. By "attacker's effort," we mean that it takes physical time and equipment or multiple procedures before a successful attack is achieved.

Table 7 specifies severity levels from the viewpoints of the risk evaluation criteria of safety, reputation, and operating loss. Appropriate levels for these parameters must be selected with the product's characteristics taken into account for adaptation to various business domains.

Table 5 Typical risk evaluation criteria settings

Risk	Low severity	Medium severity	High severity
Occurrence probability (High)	B	A	A
Occurrence probability (Medium)	C	B	A
Occurrence probability (Low)	C	C	B
Occurrence probability (Zero)	C	C	C

A = high risk score; B = medium risk score; and C = low risk score

Table 6 Typical occurrence probability settings

Occurrence probability	Access route	Need of expertise	Attacker's effort
High	Remote (High)	No	Small
Medium	Remote (High)	No	Large
Medium	Remote (High)	Yes	Small
Medium	Adjacent (Medium)	No	Small
Low	Remote (High)	Yes	Large
Low	Adjacent (Medium)	No	Large
Low	Adjacent (Medium)	Yes	Small
Zero	Adjacent (Medium)	Yes	Large
Zero	Local (Low)	Not considered	Not considered

For cases in which the access route is Local (Low), the occurrence probability is specified as "Zero" without considering the need of expertise and the attacker's effort.

Table 7 Typical severity settings

Severity	Safety	Reputation	Operating loss
High	Death, serious injury, and fire	Reputational damage to corporate brand	One or more days of manufacturing line stoppage
Medium	Hospital visits for treatment; and ignition of the product	Reputational damage to the product	Less than one day of manufacturing line stoppage
Low	Minor injury and smokes	-	-

3.2 Threat analysis procedure

Our proposed threat analysis procedure works in principles broadly similar to those of the Asset-Based Detailed Risk Analysis method. More specifically, a threat analysis proceeds according to the flow shown below (Fig. 1). The following subsections will explain in detail the mechanism for adaptation to the product's business domain as the procedure for performing detailed tasks in each process.

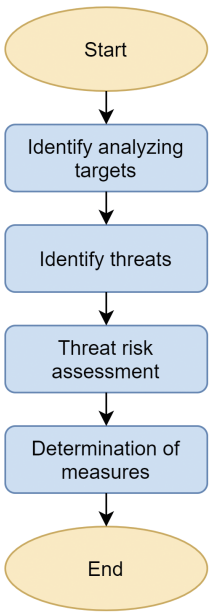

Fig. 1 Threat analysis flow

3.2.1 Identifying the analysis targets

An attempt at exhaustively identifying assets from system requirements and other input documents would end up with an excessively broad scope of analysis, which would result in a huge number of required person-hours. Hence, the aim here is to clarify the analysis target product and the use environment to identify the assets to be protected and the access routes thereto. For this purpose, an overall system configuration diagram must be prepared based on the assumed use environment. For the analysis target product, the assets to be protected and the access routes thereto must also be indicated so that low-criticality information, functions, and access routes can be filtered out using the Protection Target Asset Level and Access Route Level tables that determine which one of the criticality levels predefined based on the product's business domain should apply. In the example in Fig. 2, the scope of analysis excludes the ladder program debugging function, which is a functional asset found at the Low level in Table 2, and the risk of cyberattacks via access routes, such as contact inputs and outputs, which is found at the Local (Low) level in Table 3. In this way, identification must be performed of protection target assets and access routes to be analyzed.

In this case, the functions and information other than the debugging function are the protection target assets to be analyzed. Besides, LAN1, LAN2, and an SD memory card are the access routes to be analyzed.

3.2.2 Identifying the threats

The system configuration diagram (Fig. 2) with the analysis targets specifically defined serves as the basis for identifying potential threats to each protection target asset based on the guide words in Table 4 by paying attention to the connecting access routes. As a result, it is possible to identify threats using a minimum required number of combinations and hence to perform an exhaustive identification of threats while keeping the analysis person-hours down.

The following (Fig. 3) shows a typical analysis focusing on firmware as an example of protection target assets:

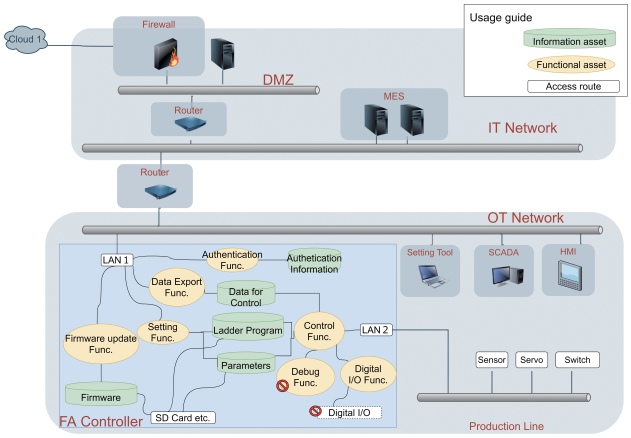

Fig. 2 Typical system configuration diagram (of an FA controller)

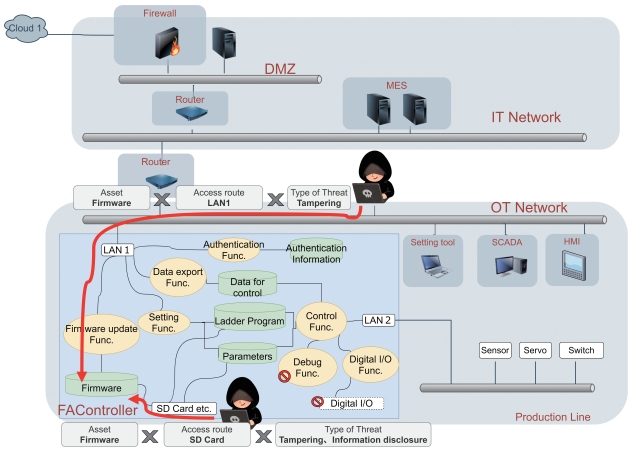

Fig. 3 Firmware-focused threat identification

This example includes LAN1 and an SD memory card as routes accessible to the firmware. For each access route, potential threats must be recorded as identified based on the guide words. In this way, threats to all analysis target assets must be identified and included in a threats list (Table 8).

A use case scenario consisting of the four phases found in Chapter 2 “Focus points for product security measures” must be created to verify the threats identified. Threat verification based on such a scenario allows identification of, if any, overlooked threats.

Table 8 Typical threats list

No.	Target asset	Access route	Threat type	Threat
1	Firmware	LAN1	Tampering	The firmware may be overwritten by a malicious third party using the setting tool.
2	Firmware	SD memory card	Information disclosure	The firmware may be identified by a malicious third party through the SD memory card.
3	Firmware	SD memory card	Tampering	The firmware may be overwritten by a malicious third party through the SD memory card.
4	Ladder program	LAN1	Tampering	The ladder program may be overwritten by a malicious third party using the setting tool.
5	Ladder program	LAN1	Information disclosure	The ladder program may be exploited by a malicious third party using the setting tool.
6	Ladder program	LAN1	Information disclosure	The ladder program may be exploited by a malicious third party using packet capture.

3.2.3 Evaluating the threat risks

For each threat identified, problem events attributable to them must be enumerated. The problem events must then undergo risk evaluation (Table 9) for severity and occurrence probability in light of the settings in Tables 5 to 7.

3.2.4 Determining the countermeasures

The obtained risk scores serve as the basis for determining the need of countermeasures. The need of countermeasures must be determined based on their cost-effectiveness and the post-countermeasure residual risks. For this purpose, assumed countermeasures must be outlined, starting from the one for the most critical high-level risk. During the consideration of countermeasures for individual risks, it may turn out that

Table 9 Typical risk evaluation

No.	Target asset	Threat-induced problem events	Severity	Occurrence probability factors			Occurrence probability	Risk score
				Access-route viewpoint	Attacker's-expertise viewpoint	Attacker's-effort viewpoint		
1	Firmware	Prolonged stoppage of manufacturing line; and reduced manufacturing quality	High: operating loss	High	Medium	High	High	A
2	Firmware	Disclosure of PLC design secrets	Medium: operating loss	Low	Medium	Medium	Medium	B
3	Firmware	Prolonged stoppage of manufacturing line; and reduced manufacturing quality	High: operating loss	Low	Medium	Medium	Medium	A
4	Ladder program	Prolonged stoppage of manufacturing line; and reduced manufacturing quality	High: operating loss	High	Medium	High	High	A
5	Ladder program	Customer's manufacturing data leakage	Medium: reputational damage	High	Medium	High	High	A
6	Ladder program	Customer's manufacturing data leakage	Medium: reputational damage	Medium	Low	High	Medium	B

Table 10 Typical risk countermeasures and residual risks

No.	Target asset	Occurrence probability factors			Occurrence probability	Risk score	Need of countermeasures	Countermeasures	Residual risk
		Access-route viewpoint	Need-of-expertise viewpoint	Attacker's-effort viewpoint					
1	Firmware	High	Medium	High	High	A	Yes	• Encrypted communication • User authentication function	None
2	Firmware	Low	Medium	Medium	Medium	B	Yes	• Encrypted firmware	None
3	Firmware	Low	Medium	Medium	Medium	A	Yes	Addressed with countermeasure taken for No. 2	None
4	Ladder program	High	Medium	High	High	A	Yes	Addressed with countermeasure taken for No. 1	None
5	Ladder program	High	Medium	High	High	A	Yes	Addressed with countermeasure taken for No. 1	None
6	Ladder program	Medium	Low	High	Medium	B	Yes	Addressed with countermeasure taken for No. 1	None

countermeasures to be implemented for higher-level risks will eliminate the need to implement individual countermeasures for some other risks. Threats for which common countermeasures are effective should be omitted from the consideration of countermeasures (Table 10). As a result, the time required to consider and implement countermeasures will be reduced, thereby contributing to efficiency enhancement. Regarding assets with lower protection priority, not all potential vulnerabilities and risks of attacks through them can be identified and addressed. These assets must be deemed and accepted as low in business risk on the basis of the probability of occurrence and severity levels and must be provided with countermeasures in the event of an incident. Finally, the feasibilities of the countermeasures to be implemented and the post-countermeasure residual risks must be evaluated to develop and adopt risk countermeasures as security requirements.

4. Outcome-and-effect verification

Using the products in Table 11, we compared our proposed method and a brute-force method of threat analysis, such as the asset-based Detailed Risk Analysis, in terms of the number of patterns of threats to be analyzed (Fig. 4). As shown by the figure, our proposed method first assigned priorities to the protection target assets and then analyzed them to keep the divergence of analysis patterns under control. As a result, the numbers of threat patterns necessary for analysis were reduced to approximately one-tenth or less.

Table 12 shows the detailed results for the case of Product D. The specifics of the procedure taken are as follows, except that some details are omitted for the protection of the product's secrets:

Table 11 Numbers of protection target assets and routes for the products under verification

Product	Number of information assets	Number of functional assets	Numbers of routes
Product A	17	18	2
Product B	5	1	4
Product C	14	1	7
Product D	7	7	5
Product E	8	11	8
Product F	27	1	7
Product G	20	16	7

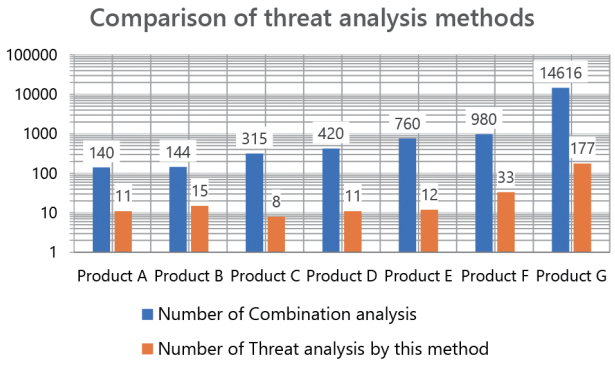

Fig. 4 Comparison of the numbers of analysis target threats' patterns

Table 12 Comparison of threat analysis results for Product D

Threat level	Number of threats per brute force attack	Number of threats excluded because of the asset-route combination	Number of threats excluded because of duplication or the proposed method	Number of threats identified
High	60	0	58	2
Medium	240	0	143	7
Low	120	120	-	2

Two Asset Level "Low" threats were included in the post-process count, through verification, on account of their occurrence probability levels.

(1) Of Product D's 14 assets, four with an incident severity rating of acceptably "Low" were excluded from the

scope of analysis (Table 13).

(2) Of Product D's five access routes, the following three were excluded from the scope of analysis (Table 14): direct device manipulation, which is difficult because of the characteristics of the product's installation environment; and serial communication and USB communication, both exposed only to low-level attacks.

(3) For the 20 (10×2) combinations that remained after (1) and (2) above, six STRIDE guide words (Table 4) were used to exclude attack patterns same in methods from 120 (20×6) patterns and then access route combinations with assets unconnected, to narrow down the threat list to nine threats.

(4) The nine threats were analyzed for specific threats and potentially resulting risks. Based on the impact scenario for the identified threats in the product lifecycle, the narrowed-down list of assets and access routes was reexamined to add two new threats.

(5) The finally identified 11 threats were evaluated, prioritized, and addressed with countermeasures based on the risk evaluation criteria in Table 5.

Table 13 Product D-related assets

Severity	Number of assets	Definition of the level
High	2	Assets with risks that may lead to deaths, serious injuries, or personal information disclosure
Medium	8	Assets with risks that may lead to monetary damages to the user or the company
Low	4	Assets with risks that may cause minor information disclosure or malfunctioning

Table 14 Product D's access routes

Level	Number of access routes	Definition of the level
Remote (High)	2	LAN-compatible communication protocols
Adjacent (Medium)	1	Direct device manipulation
Local (Low)	2	Serial communication and USB communication

The above threat analysis procedure provides a method of identifying threats to important assets on a priority basis and reducing the person-hours required for analysis, thereby making efficient analysis possible. The graph data in Fig. 4 shows the analysis results for products in multiple domains, such as FA, healthcare, social solution, and device/module products. The results of applying our proposed method to these products revealed that it was effective for them all. Hence, we consider that the method can be applied to various domains.

5. Conclusions

For the challenge of the absence of efficient threat analysis methods suitable for embedded devices, our proposed method produced some positive results in terms of efficiency as a threat analysis method applicable to various domains and suitable for effective threat analysis embedded devices. However, it should be noted that the probability of incident occurrence in reality varies depending on the malicious attackers' intent. We conclude that the occurrence probability settings with attackers' motivations taken into account will provide an improvement measure that leads to threat identification with more concreteness.

On the other hand, we must incorporate the threat analysis procedure based on our proposed method into conventional development procedures and position the practice of threat analysis per se as part of each development process to strike the right balance between ensuring product quality and ensuring product security. We are currently performing threat analysis only for some products and hence will have to expand the range of analysis target departments and products. We will also deploy campaigns, including awareness-raising activities and education for developers, to promote its incorporation into development processes.

Because cyberattack technologies and cyberattack prevention technologies are evolving daily, we must remain well versed in new technologies and improve the way threat analysis methods are to continue performing effective and efficient threat analysis.

References

1) Information-Technology Promotion Agency, Japan (IPA), *Whitepaper on Information Security 2019* (in Japanese). Information-Technology Promotion Agency, Japan (IPA), 163 p.

2) V. Saini, Q. Duan, and V. Paruchuri, "Threat Modeling Using Attack Trees," 2008, https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees (accessed Mar. 1, 2020).

3) Information-Technology Promotion Agency, Japan (IPA)/Security Center, *Security Risk Analysis Guide for Control Systems, Second Edition* (in Japanese), 2017, https://www.ipa.go.jp/files/000069436.pdf. (accessed Mar. 1, 2020).

4) M. Nakano, Y. Horibe, T. Kobayashi, and T. Matsuki, "Threat Analysis Method: Reducing Costs and Variability in Results" (in Japanese), *SCIS*, no. 1C2-5, 8 p., 2018.

5) Microsoft Corporation, "The STRIDE Threat Model," https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) (accessed Feb. 27, 2020).

About the Authors

SERIKAWA Masataka
SPI & SPL Integrated Tasks Promotion Dept.
Design & Engineering Process Technology Center
Global Manufacturing Innovation H.Q.
Specialty: Software Engineering

NIWA Toru
Design & Engineering Process Technology Center
Global Manufacturing Innovation H.Q.
Specialty: Software Engineering
Affiliated Academic Society: IEICE

YOSHIOKA Sachie
SPI & SPL Integrated Tasks Promotion Dept.
Design & Engineering Process Technology Center
Global Manufacturing Innovation H.Q.
Specialty: Software Engineering

HARADA Shintaro
Process Engineering Dept.
Information and System Technology DIV.
OMRON Software Co., Ltd.
Specialty: Software Engineering