ISSN 2277-3061

Study of Vulnerability Diagnosis and Sustaining Integrity of the Embedded Devices

Masaki Fujikawa
Security Science Institute, Edogawa-Ku, Tokyo, JAPAN

ABSTRACT

Security vulnerability of the embedded devices with Internet connectivity is frequently reported these days. In this paper, a diagnosis was made for a security vulnerability in the controller that is an element of the security system installed in homes and offices and connected to the Internet. The results showed a part of the functions of the controller may be suspended and the integrity of the security system may be lost due to an attack of known malware. In the latter part of this paper, the possible impacts on the controller and the security system were predicted based on the attack scenario on the security system initiated by the attack on the controller. It was also discussed what requirements must be fulfilled by the controller and the security system and about the need for a diagnosis for an unknown vulnerability.

Indexing terms/Keywords

Embedded devices, Security systems for homes and offices, Vulnerability, System requirements.

Academic Discipline And Sub-Disciplines

Information system

SUBJECT CLASSIFICATION

Embedded system security

TYPE (METHOD/APPROACH)

Diagnosis of a known (widely known) vulnerability

ISSN 2277-3061

1 INTRODUCTION

Today the Internet becomes a common and handy communication tool in daily life, and many embedded devices, as well as communication devices like PCs, tablets, and smartphones, can be connected via the Internet. Some appliance manufacturers develop and sell appliances that can be connected via wireless LAN installed in the home, and a resident can control such appliances using a smartphone in which a special application is installed at home or away from home [1].

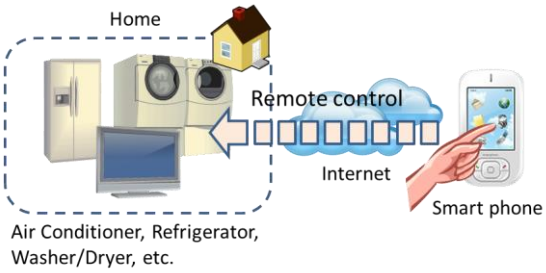

Fig 1: Control of appliances by the smartphone.

Additionally, owing to the expanded use of a network camera with Internet connectivity, numbers of homes and offices are increasing that install a simple security system. In such a system, when an abnormal event (intrusion, fire, etc.) is detected, the network camera is automatically activated and movies or pictures are taken, and such movies or images are transmitted to the smartphone of the resident or the office administrator [2].

While the increase in embedded devices with Internet connectivity will improve the convenience of life, horrifying events are reported frequently these days. Table 1 summarizes such reports made from July 26 to August 8, 2013, which all suggest that life and properties are jeopardized due to security vulnerabilities (security hole) in the embedded devices. Generally speaking, because security measures in the embedded devices fall far behind compared with measures of PC's OS, and communication equipment (router etc.) and research and development are still in the primitive stage, the problem of security holes (vulnerability) is frequently reported.

Table 1. Reports on vulnerability of the embedded devices.

Date	Summary
July 26	Possibility of steering and braking system of Toyota Prius being incapacitated while driving was due to hacking [3]
July 29	Possibility of car theft through invasion into the key ID authorization system of a luxury car was due to hacking [4]
July 30	Possibility of unauthorized access to the illumination and air conditioning control system by an outsider was due to hacking of the "Smart Home" [5]
July 30	Possibility of the vehicle controlled by an outsider (sudden acceleration, quick braking, false indication of the fuel gage, etc.) was due to hacking of the Ford Escape [6].
August 8	Possibility of the Smart Lavatory controlled by an outsider, such as to increase water volume intentionally, was due to a vulnerability in the Android application to control Smart Lavatory [7]

Telephone lines or private lines were used in the security system of homes and offices provided by security service companies to transmit information on an abnormal event like intrusion or fire, but recently services that use the Internet as an information line are increasing [8]. While the Internet provides the saving of communication costs borne by homes and offices, the possibility of a security hole (vulnerability) of the controller as the embedded device of the system that provides the connection to the Internet becomes a concern. Accordingly, in this report, the vulnerability diagnosis of the controller against a programmed attack is conducted, and the requirements on security to be incorporated in the security system including the controller are discussed.

Discussions are made in the following order in this report. In Section 2, an outline of the security system serviced by the security company is explained. Section 3 provides an explanation of the functions of the controller, a component of the security system. Section 4 provides a description of the attack scenario on the controller assumed by the author and a discussion about the appropriateness of the scenario. In Section 5, the environment according to the assumed scenario was constructed and a vulnerability diagnosis of the controller was conducted. Section 6 provides a prediction of the possible attack and the associated problems based on the scenario and the results of the diagnostic. In Section 7, a discussion is given about the security requirements with which the controller and the security system must be equipped. Section 8 provides a discussion about the requirement of the diagnosis of the unknown vulnerability.

ISSN 2277-3061

2 OUTLINE OF THE SECURITY SYSTEM

Fig. 2 shows a schematic of the common security system (details are different between security companies but Fig. 2 applies generally). Sensors, network cameras, and a controller are installed in the house or office. These devices are centrally controlled by the monitoring center of the security company, which responds to an abnormal event detected in the house or office by sending security guards or informing the police or fire department.

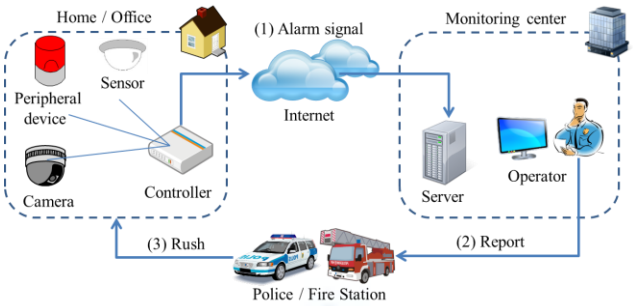

Fig 2: Common security system.

The sensors detect an abnormal event in the house or office and transmit the corresponding signal to the controller. The sensors and controller are interconnected via a communication cable or wireless circuit network peculiar to the respective security company, but recently connections may be made via cables or Wi-Fi to a LAN installed in the house or office.

Network cameras observe the circumstances in the house or office and send movies and images to the controller. While network cameras can send movies and images whether or not an abnormal event occurs, they are sent only when an abnormal event occurs via linkage to the sensors. Network cameras and the controller are usually connected through cables or Wi-Fi using a LAN installed in the house or office.

The controller transmits the information from the sensors in the event of an abnormal event and movies and images captured by the network cameras to the monitoring center. Until today, a telephone line or private line was used as the connection between the controller and the monitoring center, but the Internet is now used.

A security company usually employs a unique cryptographic protocol or HTTPS (hypertext transfer protocol secure) or VPN (virtual private network) when using a LAN and the Internet as a communication line to ensure confidentiality and the security of the information communicated.

3 FUNCTION OF THE CONTROLLER

In this section, the functions of the common controller are explained. (The details are different between security companies but the following descriptions apply generally.)

3.1 Function 1 (Switching ON and OFF of the system and personal authentication)

The controller has a function to switch on and off the security system and has a function to authenticate a person who switches on and off the system. Personal authentication is usually made by input of a PIN, a smart card, or by biometrics for a person who tried to switch on/off the system by pressing a button. When it is verified that such person is a real resident or an authorized employee, the system can be switched on/off.

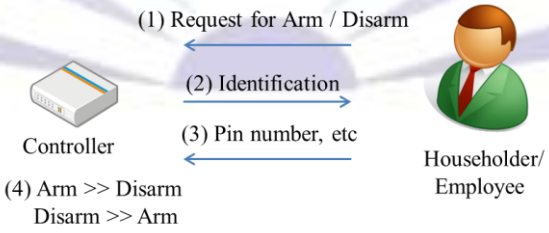

Fig 3: ON/OFF of the security system and personal authentication.

3.2 Function 2 (Control of Peripheral Devices of the Security System)

The controller has a function to control the peripheral devices of the security system (beacon light, alarm horn, electric lock, etc.). For example, the controller operates the beacon light to report an abnormal event or intimidates an intruder by sounding an alarm horn according to the preprogrammed control parameters when a sensor detects an abnormal event. It also releases an electric lock installed on the door linked to the function of personal authentication explained in Function 1.

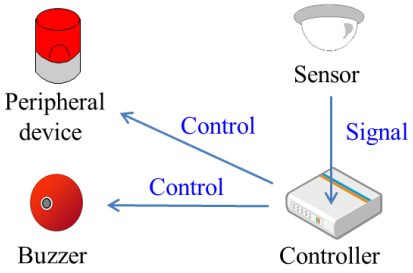

Fig 4: Control of peripheral equipment.

3.3 Function 3 (Control of Network Cameras)

The controller also has a function to control network cameras. For example, the timing of taking movies or images and the recipient of such movies and images are controlled according to preprogrammed control parameters. Linked to the function of personal authentication in Function 1, the authentication of a person trying to view movies or images from the camera via a smartphone is also made.

3.4 Function 4 (Alive Monitoring)

The controller has a live monitoring function of the sensors, network cameras, and peripheral devices connected to the controller. For example, the controller periodically sends a packet for diagnosis to the devices and verifies their responses (alive or not). When no response is received, the controller notifies the monitoring center to request maintenance of the device.

3.5 Function 5 (Cryptographic Communication Function)

The controller has an encryption function for transmission and a decryption function for received information. There are a number of cryptographic communication methods available and a method used is determined by respective security company.

3.6 Function 6 (Transmission/Receiving, Recording and Storage of Information)

The controller transmits and receives information via LAN and/or Internet, and it records and stores information internally. Table 2 shows example of the information recorded and stored by common controllers. Confidentiality, integrity, and availability of the recorded and stored information, which are basic components of information security, must be established similarly to the information transmitted and received.

Table 2. Information recorded and stored in the controller

	Description
Information on the controller	Firmware, control parameters, etc.
Information on communication	Cryptographic key, electronic certification, etc.
Information on personal authentication	PIN, information on the smart card, biometric information, etc.
Information on security	On/off record of the security system, record of the signals received from sensors, movies and images of the cameras, etc.

4 Creation of the Scenario

In this section, an explanation of the scenario (attack and its effect on to the controller) assumed by the author is given and the appropriateness of the scenario is discussed.

4.1 Senario

As explained in Section 3, the controller is located in the home or office and connected to the monitoring center via the Internet. To enable this, the controller is connected to the LAN installed in the home or office as shown in Fig. 5.

ISSN 2277-3061

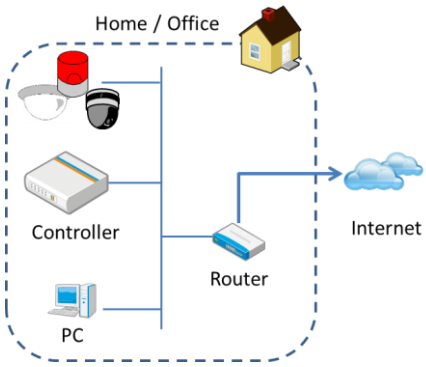

Fig 5: Controller is connected to the LAN.

The scenario (attack and its effect on to the controller) assumed by the author is as follows.

(1) The PC connected to the LAN to which the controller is connected is infected by malware (see Fig. 6)

(2) The malware infected PC attacks the embedded devices connected to the LAN through the known vulnerability of the embedded devices.

(3) A part of or entire functions of the controller stop functioning due to the attack from the PC.

(4) If, for example, information transmission/receiving function of the controller stops due to the attack in (3), the consequences to the security company and household or office are as follows.

Household and office: Psychological and economic damage due to expanded losses and damage because the security company cannot recognize the intrusion or fire.

Security company: Liability for claimed compensation against losses and damage caused by a defect in the security system and loss of credibility as a security service provider.

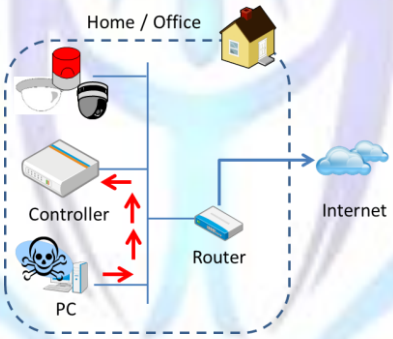

Fig 6: Malware infected PC transmits attack packets to the controller (red arrows).

4.2 Suitability of the Senario

There is a good chance that the PC located in the home or office is infected by malware. Recently, the presence of malware that attacks an unknown vulnerability inherent in the software installed on the PC is reported [9], and even if antivirus software is installed, such malware may not be able to be detected. (The PC is infected by such malware.)

It is also possible that the infected PC attacks the embedded devices connected to the same LAN. It was reported, for example, malware called Stuxnet intruded into the PC located in the nuclear facility in Iran and attacked the SCADA (Supervisory Control And Data Acquisition) via LAN [10].

5 Vulnerability Diagnostics

5.1 Diagnositic Method

In this report, diagnosis of a known (widely known) vulnerability in the controller was conducted based on the attack scenario explained in Section 4 by constructing the network shown in Figure 7. Three types of diagnostic tools shown in Table 3 are installed on the PC. Each diagnostic tool provides a diagnosis looking at the response of the controller to four types of packets (ARP, ICMP, TCP, and IP).

Two types of controllers (Controller 1 and Controller 2) that are used by security companies operating worldwide were used for the diagnosis. Disclosure of the specific name of the security company and the details of the controller are withheld in this report for security reasons.

ISSN 2277-3061

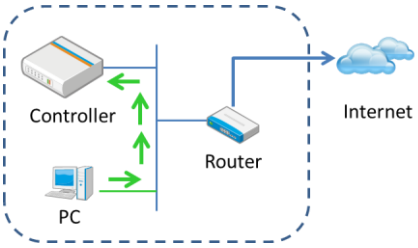

Fig 7: PC for diagnosis transmits diagnostic signal to the controller (green arrows).

Table 3. Diagnostic tools used.

Tool No.	Tool Name (Organization Name)
1	Retina Network Security Scanner (eEye Digital Security)
2	Nexpose (Rapid7)
3	Known Vulnerability Verification Tool (IPA:Information-technology Promotion Agency, Japan)

5.2 Results of Diagnosis

Table 4 shows the results of the diagnosis. The results using three tools were almost the same.

Table 4. Results of diagnosis using 3 tools.

Type	Results of Diagnosis
Controller 1	No known vulnerability was detected.
Controller 2	The known vulnerability was detected. Functions of the controller partly stopped due to an attack through the vulnerability.

The author made an attack on Controller 2 through the vulnerability identified. The following items were identified as a result. (The vulnerability identified here was already reported to the manufacturer of the controller and measures were taken.)

(1) Transmission/receiving function of information with the monitoring center partly stopped.

(2) The above phenomenon is reproducible (the same attack always stops the function).

(3) In order to restore the function stopped, restarting of the controller (i.e. turn off the power switch manually and turn it on again) is required.

6 Discussion 1 (Assumed Attack and Prediction of Problems Occurred)

Generally, a phenomenon that takes place when the embedded device is attacked (suspension of the function, restarting, etc.) is the same as the phenomenon that occurs when the device physically fails. This fact can be easily understood when the results of the attack explained earlier are considered. Accordingly, it is frequently interpreted that the problem of the embedded device caused by the attack of malware is caused by the failure of the embedded device. If an attack by malware cannot be identified quickly, it may lead to expanded damage to the entire system from local damage (in a part of the system).

In this section, the types of problems that are anticipated in the controller (a part of the system) and the security system (entire system) due to the attack of the malware (including infection by the malware) are explained. Examples of specific problems are shown as follows according to the magnitude of the problem.

6.1 Occurrence of Small Scale Ploblems

The assumed attack and the expected problems are as follows. The reason why it is defined as a small-scale problem is because the anticipated problem is small and primitive compared with the problems explained later.

Assumed attack:

As shown in Fig. 8, one of the controllers is subject to an attack or intrusion by malware.

Problems that may occur (those occurring on the controller, in no particular order):

- Suspension of the functions in part or entirely: A part of or entire functions of the controller (see Section 3) stop functioning.
- Abnormal functioning: Examples include on/off of the security system becomes impossible, failure in personal authentication of the resident or authorized employee (or authentication of a person not authorized), control of the network cameras different from the control parameters, alive monitoring becomes impossible, cryptographic communication becomes impossible, transmission/receiving, recording, and storage of the information become impossible, etc.
- Unintended functioning: Examples include on/off of the security system switches or the system is reset and restarted irrelevant to operation of the resident or employee, etc.
- Leakage of information: Information stored in the controller (see Table 2) leaks out due to malware.

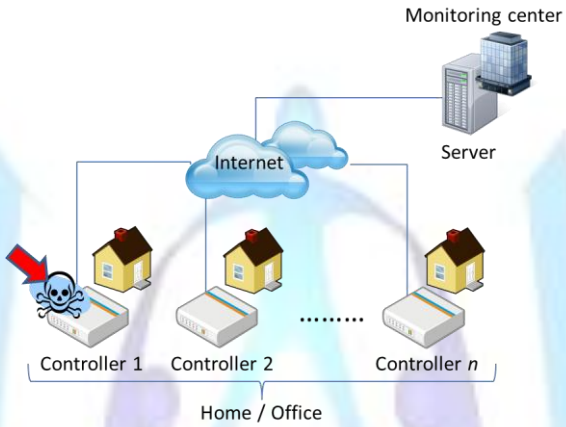

Fig 8: One of the controller is subject to attack of intrusion by the malware.

6.2 Occurrence of Medium Scale Problems

The assumed attack and the expected problems are as follows. The reason why it is defined as a medium scale problem is because the scale of the anticipated problem is larger than that of the problem in 6.1 but smaller than 6.3.

Assumed attack:As shown in Fig. 9, malware intruded into Controller 1 attacks or intrudes into the server in the monitoring center. Problems that may occur (those occurring on the server located in the monitoring center, in no particular order):

- Suspension of the functions in part or entirely: Suspension of the functions of the server in part or entirely.
- Abnormal functioning: Examples include that log-in to the server becomes impossible, control of the controllers from the center becomes impossible, etc.
- Unintended functioning: Examples include reset and restart of the server irrelevant to the intention of the operator/administrator of the monitoring center.
- Leakage of information: Information stored in the server leaks out due to malware.

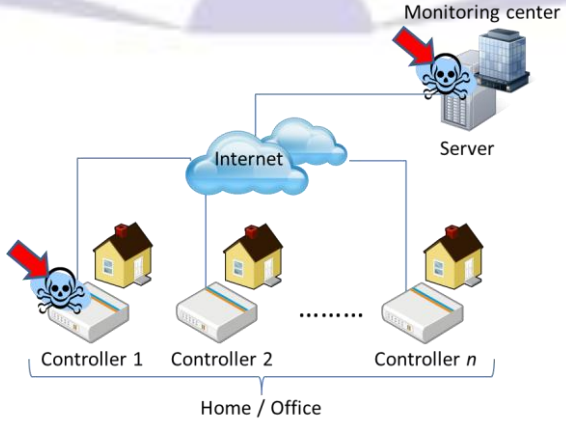

Fig 9: Server located in the monitoring center is subject to an attack or intrusion by the malware.

6.3 Occurrence of Large Scale Problems

The assumed attack and the expected problems are as follows. The reason why it is defined as a large-scale problem is because scale of the anticipated problem is larger than those defined earlier and the entire security system is affected by problems.

Assumed attack:

As shown in Fig. 10, all the controllers and the server located in the monitoring center are subject to an attack or intrusion by the malware.

Problems that may occur (those occurring on the controllers and the server in the monitoring center, in no particular order. Multiple problems may occur at the same time.)

- Suspension of the functions in part or entirely: A part of or entire functions of the controllers (see Section 3) and the server stop functioning due to the attack.
- Abnormal functioning:

  [Controller] On/off switching of the security system becomes impossible, failure in personal authentication of the resident or employee (or authentication of an unauthorized person), control of the network cameras different from the control parameters, alive monitoring becomes impossible, cryptographic communication becomes impossible, transmission/receiving, recording, and storage of the information become impossible, etc.

  [Server] Log-in to the server becomes impossible, control of the controllers from the center becomes impossible, etc.
- Unintended functioning:

  [Controller] The security system switches on/off or is reset and restarts etc. independently from the intention of the resident or employee.

  [Server] The server is reset and restarts independent from the intention of the operator/administrator of the monitoring center etc.
- Leakage of information:

  [Controller] Information stored in the controller (see Table 2) leaks out due to malware.

  [Server] Information stored in the server leaks out due to malware.

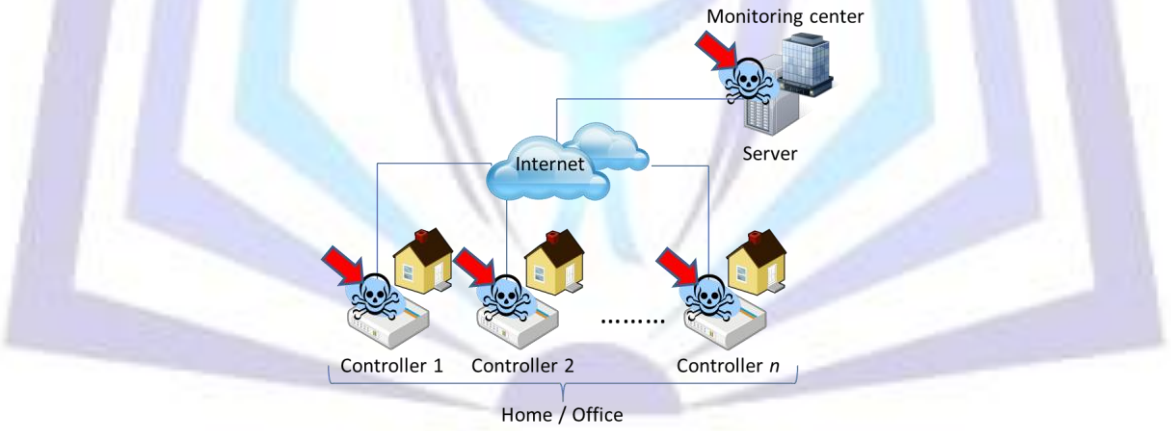

Fig 10: Entire security system is subject to attack or intrusion by malware.

7 Discussion 2 (Security of the Controller and the Security System)

In this section, discussion is given to the security requirements that the controller and the security system must be equipped with.

7.1 Security of the Controller

In conducting the vulnerability diagnosis, it was found that certain controllers have known vulnerabilities and problems of the controller caused by vulnerability may affect the security system.

The author considers that two approaches should be made so that the controller is free from the known vulnerability. The first approach is to conduct a vulnerability diagnosis in the design and manufacture of the controller to confirm that the controller is free of such vulnerability. Recently tools for vulnerability diagnosis are available both paid and free, and vulnerability can be identified efficiently and effectively with the combined use of these tools. When the security company

asks the design and manufacture of its controller to the device manufacturer, the specification or purchase order must clearly require a vulnerability diagnosis and the submission of a report on the results.

The second approach should be to construct a system environment where a patch can be easily applied if a vulnerability is detected after the controller is released. In the case of the OS and software installed on the PC, software manufacturers provide an environment where updates to patches or firmware are distributed to individual PCs via the Internet. Such environment should be also constructed by the security company.

7.1 Security of the Security System

As explained in Section 6, problems may spread over an entire security system when the controller has a vulnerability. (In case of such an event, it may become a social issue because homes and offices suffer from psychological impact and economic damage, and the security company may become liable for such damage.)

The author considers that two approaches should be made so that the security system is protected from the spread of problems. The first approach is to maintain the integrity of the controller (maintain the controller free of vulnerability). This is as explained in Subsection 7.1.

The second approach is to concentrate efforts in sustaining the integrity of the security system. Some approaches are specifically considered for this approach. They are, for example, application of the ISMS (Information Security Management System) in the organization of the monitoring center and construction of an environment where the presence and attack of the malware can be detected quickly (honey pot etc.) in the LAN installed in homes and offices.

Recently, numbers of cyber-attacks on power plants or manufacturing plants are increasing where closed systems without Internet connection are also increasing. Although attacks on the security system serviced by the security company may be less significant when compared with the impact on the power plants and manufacturing plants, it must become a social issue. As explained so far, the security system makes use of the Internet, construction of the system environment to cope with cyber-attacks by malware etc. is necessary.

8 Discussion 3 (Necessity to Detect Unknown Vulnerability)

In this section, a discussion about the requirement for the diagnosis of an unknown (i.e., not commonly known) vulnerability is given. The vulnerability of the OS, software, or communication equipment (such as a router) is generally found before the product is released and after it is released, the manufacturers continue publishing patches for the vulnerability identified [11], [12]. This is made by continuing the investigation of any unknown vulnerability after the release of the product to sustain the reliability of the product.

In this report, the results are reported investigating whether the controller has a known (i.e., commonly known) vulnerability, but it will not be sufficient to sustain the reliability of the controller. So, the security company (or the manufacturer of the controller) should establish an organization to continuously investigate an unknown vulnerability and to issue security patches quickly the same as the manufacturers of the OS, software, and communication devices do.

9 Conclusion

In this paper, the controller, which is a component of the security system among embedded devices connected to the Internet, was considered. An attack and the impact on the controller (scenario) were assumed, and a diagnosis for the presence of the known vulnerability was conducted. The result revealed that one of the controllers tested had a vulnerability and a part of the controller's functions stopped by the attack on such vulnerability. Additionally, it was found that damage due to an attack by the malware could be classified in three magnitude scales.

A security system is a system to prepare for an abnormal event in homes and offices (intrusion, fire, etc.) and to reduce expansion of damages due to such abnormal event, but so that the system can function correctly as intended, the integrity of the controller must be sustained. The author intends to continue diagnosis of the known and unknown vulnerabilities by increasing the numbers of controller types that are subjected to testing and to feed back the results for the purpose to sustain reliability of the controller.

REFERENCES

[1] Panasonic Corporation (August 2012), Panasonic to Expand Smart Home Appliance Lineup with Full-Scale Launch of Smart Cloud Services, Available: http://panasonic.co.jp/corp/news/official.data/data.dir/2012/08/en120821-9/en120821-9.html

[2] Absolute Computer Design (August 2013), Monitoring your home or business from your smart phone, Available: http://denvercamerasecurity.com/?q=Android-Smartphone-Webcam-Viewing

[3] Mike Szczys (July 26), Defcon presenters preview hack that takes Prius out of driver's control, Available: http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/

[4] BBC News Technology (July 29), Car key immobiliser hack revelations blocked by UK court, Available: http://www.bbc.co.uk/news/technology-23487928

[5] John-Paul Power (July 30), Hacking Smart Homes, Available: http://www.symantec.com/connect/blogs/hacking-smart-homes

[6] Steve Henn (July 30), With Smarter Cars, The Doors Are Open To Hacking Dangers, Available: http://www.npr.org/blogs/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves

[7] Vignesh Ramachandran, Smart Toilets Vulnerable to Hackers, Available: http://mashable.com/2013/08/03/smart-toilet-hack-threat/

[8] ADT, ADT Plus Solutions, Available: http://new.adt.com/pulse?ecid=bgtresi000102&mboxSession=1377397806481-905944

[9] SCIP AG, VulDB: Adobe Photoshop CS5 12.x unknown vulnerability, Available: http://www.scip.ch/en/?vuldb.4342

[10] IEEE spectrum, The Real Story of Stuxnet, Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[11] Microsoft Windows Update, Available: http://update.microsoft.com/

[12] CISCO, Available: http://tools.cisco.com/security/center/publicationListing.x

Author' biography with Photo

Masaki Fujikawa, Ph.D., is a senior researcher of the Security Science Institute. He received his Master degree in information engineering in 1998 from Tokushima University. In 2004 he received his Ph.D. in information engineering from Chuo University. Now, He is researching and developing a variety of security and safety systems in order to build a safer society.