



Global Business Dialogue on Electronic Commerce

GBDe 2007 Issue Group

Cyber Security

*Issue Group Leader: Mr. Buheita Fujiwara, Chairman,
Information-technology Promotion Agency*

*Issue Group Members: Mr. Junzo Nakajima, Vice President and Executive Officer,
Hitachi, Ltd.
Dr. Jyh-Sheng Ke, Senior Fellow and Board Member,
Institute for Information Industry
CyberSecurity Malaysia (IG Member Only)*

1. Overview - Almost Every Kind of Device Can Be Networked

The Internet, which has been sweeping the world since the late 1990s, has drastically changed our business models and lifestyles. Nowadays, many computers as well as software-embedded systems are networked. It is not a stretch to say that almost every kind of software-embedded system, including household electrical appliances, automobiles, and factory automation systems, can be connected in a network.

Diverse complex network environments bring new problems. In the computer world, attacks carried out through networks can cause computer damage such as service termination, file destruction, and information leaks. In the future, software-embedded systems (hereafter referred to as “embedded systems”) connected in a network may be targets of similar attacks. If that happens, both the developers of the software programs and the manufacturers of the embedded systems will have to deal with the ensuing problems. In addition, manufacturers must fully understand their responsibilities as suppliers, because they may have to pay for damages in accordance with Japan’s Product Liability Law.

In the near future, the increasingly serious security problems affecting the computer world may also affect embedded systems. Although there have not been many security incidents involving embedded systems yet, we cannot rule out the possibility of these incidents occurring more

frequently in the future. Knowing this, what should we do?

While security mechanisms are required to improve product quality, security measures are not adequately covered by the traditional quality improvement approach. Security measures need to be strengthened in the future.

In the past year, the GBDe Cyber Security Issue Group focused on this important issue. This current report aims to help embedded system manufacturers understand what they can do to ensure a secure networked society while also reducing business risks that might be associated with defects in their products.

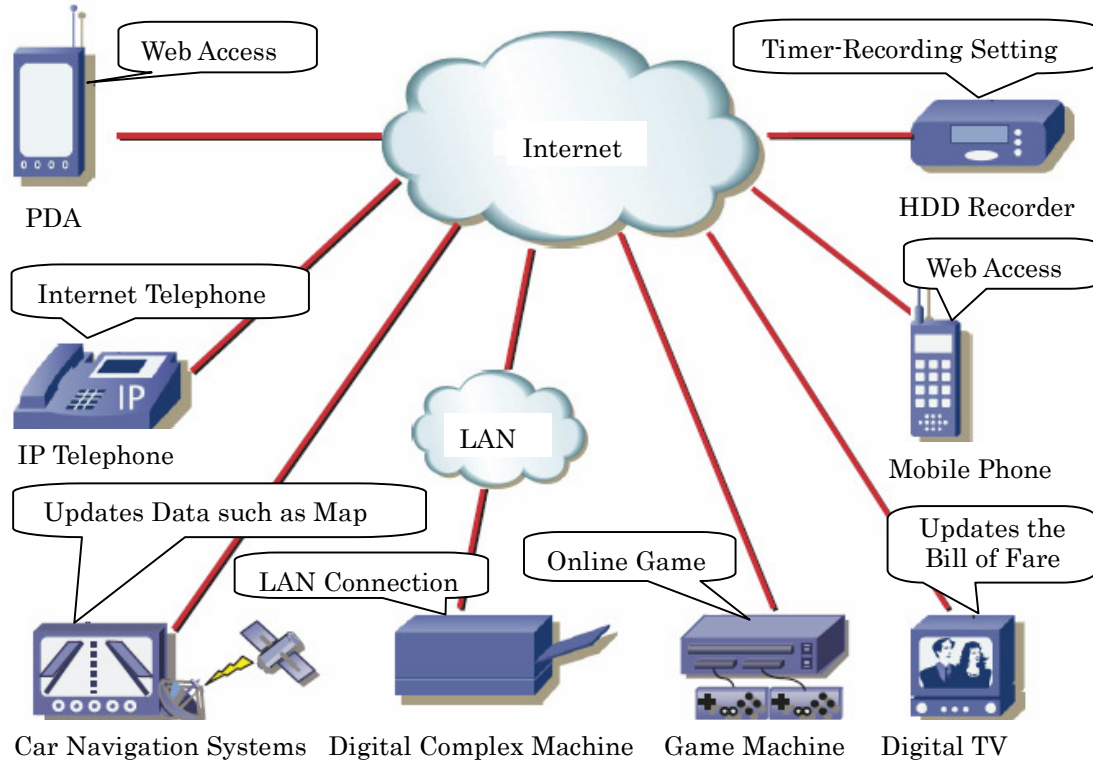


Figure 1 - Example of Embedded Systems Connected in a Network

Among the threats facing computer systems are hardware failure, software glitches, human errors such as wrong operations and settings, and computer attacks carried out by malicious users, including computer viruses¹, spyware², unauthorized access to the system, and Denial of Service

¹ A computer virus is a computer program written to infect other programs and databases. There are self-propagating viruses, latent viruses, and pathogenic viruses. ("Computer Virus Countermeasures Standards," announced by The Ministry of International Trade and Industry. The latest revision was made on December 28, 2000.)

² Spyware is a computer program to illicitly collect users' important information and access records. The program is automatically installed (or embedded) on computers without their owners' consent.

FINAL – SUBJECT TO BSC APPROVAL – November 8, 2007

(DoS) attacks³.

Over the past few years, there have been a number of computer attacks targeting vulnerabilities already existing in products. Vulnerabilities are security holes in programs and settings. If they are exploited, a chunk of unintended data can be set to the memory or an impermissible command can be accepted by the system, allowing attackers to illicitly obtain data or access privileges or halt services.

Even if devices connected to the Internet have never before experienced security problems, they may still be exposed to dangers if an attacker obtains information about vulnerabilities. This is because the attacker who acquired the information can create programs and tools to exploit the vulnerabilities and post them on the Internet, leading to the spread of computer viruses by other malicious users.

It is not easy to completely eliminate vulnerabilities; however, if we want to minimize computer attacks and provide a higher level of security, we must do our best to reduce them.

2. Risks Involved in Embedded Systems

The GBDe Cyber Security Issue Group conducted a study called, “Research Reports on the Embedded Software Industry for 2005.” According to the results, software-related problems accounted for 34% of the defects in embedded systems that were detected after shipment. It has become apparent that the quality of software programs embedded in such devices can greatly affect manufacturers’ business.

Product quality is also, ultimately, a responsibility of management. As this report concludes, “To improve product quality, people in the field must make more effort, but in many cases, management can also play a role by establishing appropriate policies and rules, enriching the software development environment, and securing qualified full-time workers.”

What happens when vulnerabilities are detected in embedded systems already on the market? Generally software developers and vendors make available programs, or “patches”, that users can obtain online and use to fix any vulnerabilities. The same approach, however, might not be effective for embedded systems, because embedded systems are not necessarily connected to the Internet. With embedded systems, developers or vendors will likely have to recall the products, replace the software/hardware (such as memory unit or boards), and deal with other potentially costly issues. For example, when cell phone users reported some failures⁴ on their cell phone application in May 2001, it cost the cell phone carrier about 12 billion yen (USD\$102 million) for product recalls and replacements.

³ A denial of service (DoS) attack is an attack which causes degradation in the functions of servers connected to the Internet by issuing a large number of commands to the servers.

⁴ Vulnerability was detected in an upgraded version of i-Appli, which allowed attackers to read or overwrite its data.

The possibility of hardware failures caused by computer attacks exploiting vulnerabilities in the software installed on the hardware can also not be ruled out. If such failures occur, manufacturers of the products will inevitably be asked to compensate for any losses. Thus, not only for security, but also for the business bottom line, measures to mitigate vulnerabilities must be established.

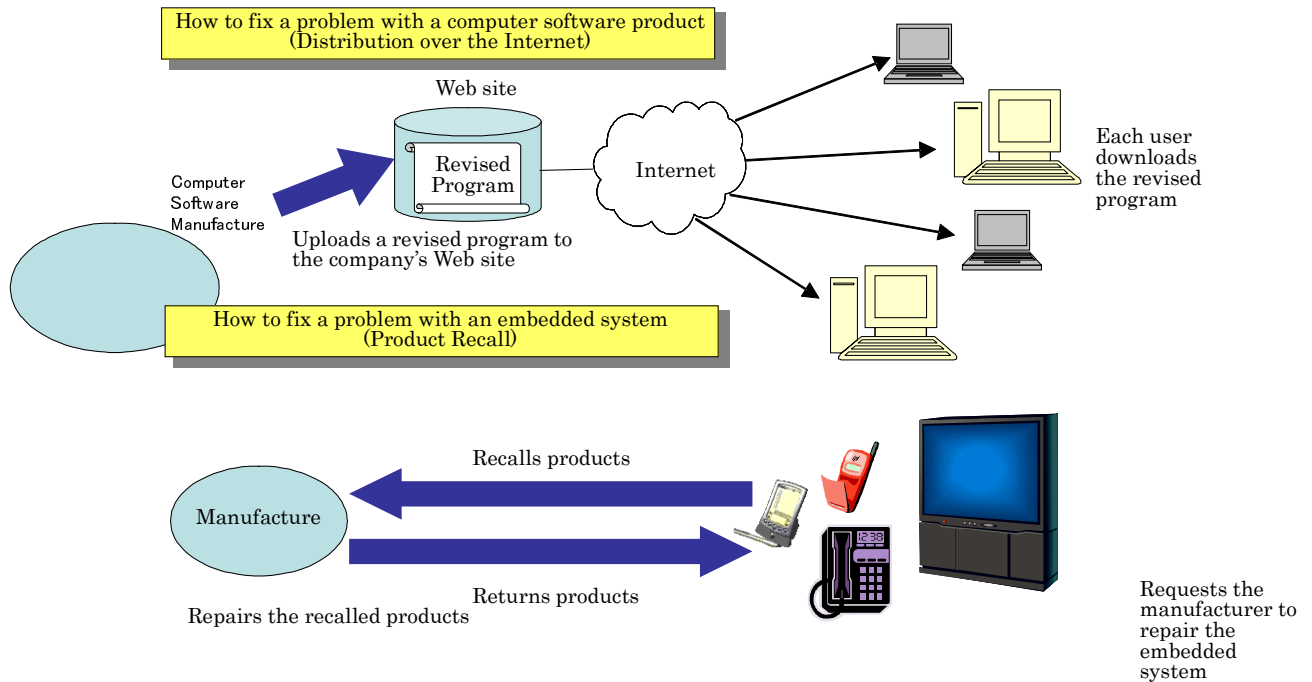


Figure 2 - How to Fix Problems of Computer Software Products and Embedded Systems

3. Examples of Incidents Involving Embedded Systems

There are some instances already where embedded systems have experienced computer attacks exploiting their vulnerabilities.

Example 1: Mobile devices infected with computer viruses did not boot up.

Outside Japan, a number of viruses affecting Symbian OS-based mobile phones have been detected. According to an April 2005 report, most of the viruses detected up to then were designed to cause system failure, exploiting vulnerability in Bluetooth⁵. In September 2005, a

⁵ Bluetooth is a standard for short-range wireless communications between mobile devices such as mobile phones. Using this protocol, a variety of devices can be networked in an easy-and- autonomous manner. As long as the distance between devices is less than 10m, the devices can communicate with each other, even if there is an obstacle between them. Unfortunately, it can also serve as a propagation path for computer viruses, since no authentication is performed when a device initially connects.

report on a mobile phone virus that prevailed in northern Europe was also aired. Further, in October 2005, the existence of viruses targeting handheld gaming devices was disclosed. These viruses deleted system files on the devices, causing them to boot abnormally.

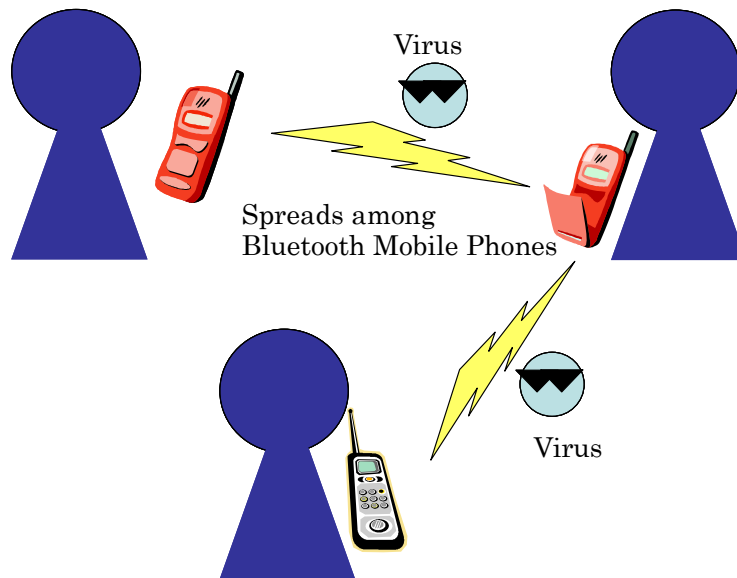


Figure 3 - Characteristics of Computer Virus Affecting Symbian OS-based Mobile Phones

Example 2: Dedicated systems infected with computer viruses did not function properly.

In August 2003, the computer virus “MS Blaster” struck all over the world. The virus targeted PCs having vulnerability and autonomously spread its infection, rapidly increasing damages.

In northern Europe, the “MS Blaster” affected not only PCs but also dedicated systems, including Automated Teller Machines (ATMs), Point of Sale (POS) terminals, and airline check-in systems, and many of them had system failures. Most of the systems affected were Windows-based systems. It is believed that vulnerability in the dedicated systems, which had not been fixed because of difficulty in applying patches, was exploited. Japanese manufacturers also indicated that printer servers in Japan might have been infected by the virus.

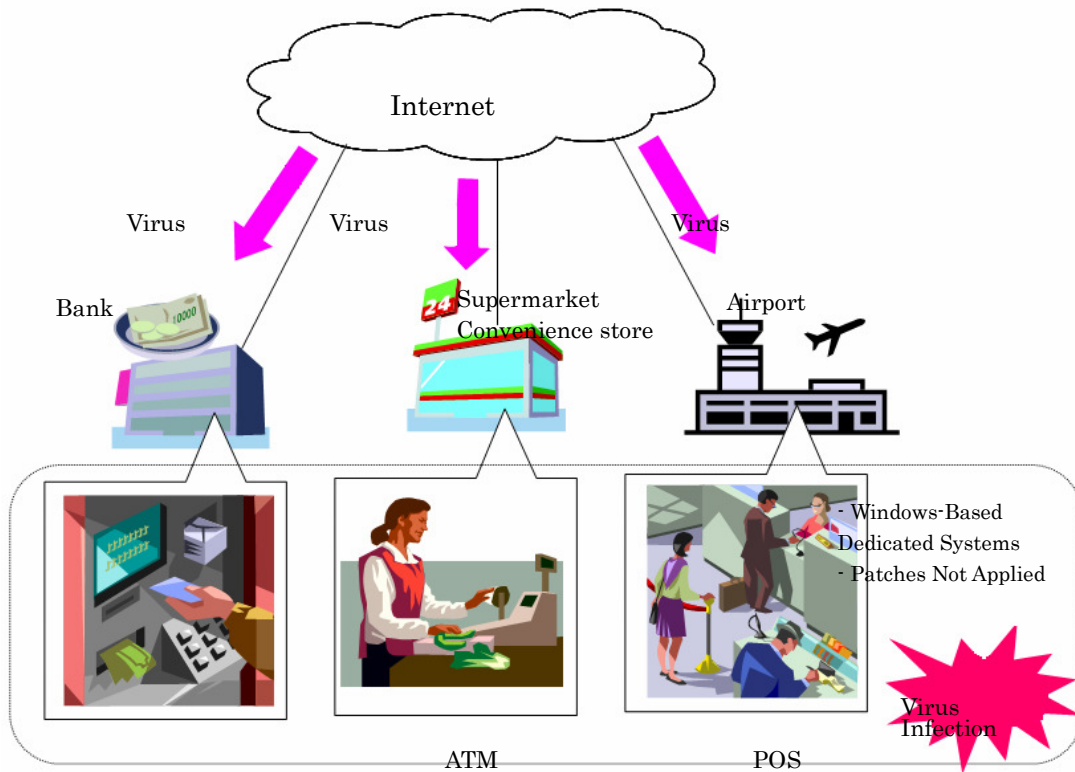


Figure 4 - Image of Dedicated Systems Infected with the “MS Blaster”

Example 3: Vulnerability in a router⁶ was exploited and router control was lost.

There have also been a few reports of vulnerabilities in operating systems installed on routers. During an IT security exposition held in July 2005, U.S. security researchers demonstrated how to take control of a router by exploiting its vulnerability. The manufacturer of the router filed a lawsuit against the group of researchers, saying that the researchers had illicitly obtained information regarding the vulnerability (later, they reached an out-of-court settlement). In the demonstration, the researchers did not give details of how to carry out an attack, but the Information and Communication industry was shocked to learn that routers, which are key Internet infrastructure components, are also vulnerable to computer attacks.

If information detailing such attack methods is posted on the Internet, malicious users may create and spread computer viruses, wrecking serious havoc unless necessary steps, such as applying patches, are taken for all routers in the world.

⁶ A router is a device that forwards packets from one network to another. The router looks at Network Layer information (such as IP addresses in packets), then determines where the packets should go.

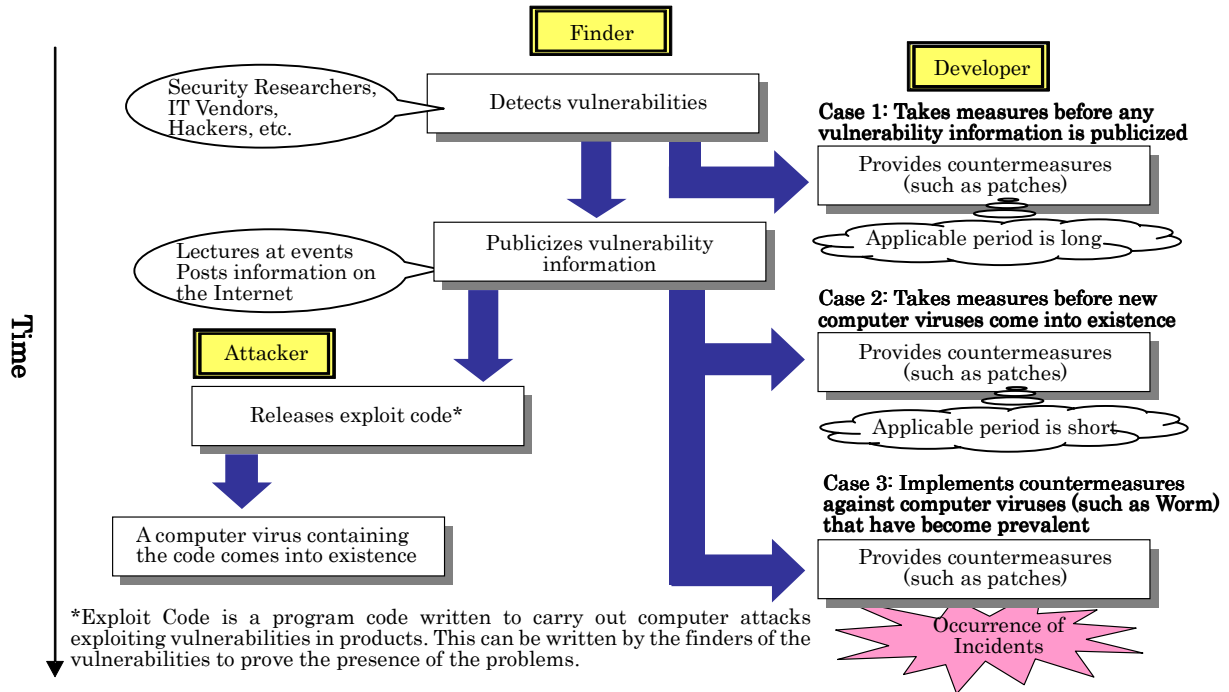


Figure 5 - Vulnerability Detection, Computer Attack, and Countermeasures

If a computer virus is created and distributed before the relevant vulnerability is dealt with (see “Case 3” in Figure 5), the situation could be devastating.

4. IT Security for Embedded Systems

4.1. Establishment of Security Measures

Unless necessary steps (such as enforcing security measures or applying patches) have been taken, personal computers connected to the Internet can be infected with a computer virus in just a few seconds. It is time to establish proper security measures for embedded systems, since networked systems are becoming more prevalent and the risk of operating without security measures is high.

For embedded systems, it is important to consider potential vulnerability problems from the planning phase and take protective measures early on; if not, such problems could cause extensive damage. Consideration of potential vulnerability problems should be considered part of an overall effort to improve quality and services, but it requires different expertise than that

required for quality improvement.

Implementing proper security measures during the development stage may be difficult because it often requires additional resources, such as manpower, time or hardware. Further, even if manufacturers put time and money into implementing security measures during the development stage, they are not likely to see such changes reflected in their products' value and price. Nevertheless, it is still manufacturers' responsibility to take steps and use whatever resources are necessary to ensure system security.

If vulnerability is detected in an embedded system already on the market, the manufacturer of the product must do its best to protect its clients and other users from damages. Should a security incident (including hardware failure) occur, they will have to take appropriate measures to avoid a crisis situation.

4.2. Implementing Security Measures for Embedded Systems

4.2.1. Organizing a Team to Ensure IT Security

There are several options for organizing a team within the company that manufactures embedded systems to ensure IT security. For example, the company could set up a special team to oversee and promote its product's IT security (including measures to mitigate vulnerabilities), establish a committee with personnel from multiple divisions to share information and understanding about IT security, or put an existing section (such as the quality control department) in charge of security-related issues. In any case, common recognition and cooperation among the sections within the company, including the security control department and the quality control department, are essential. Above all it's important to apply knowledge of relatively-new quality assurance systems and security-specific technical issues.

In one case study involving Manufacturer A, the president set up a committee to oversee company-wide IT security. Its main roles were to "promote IT security within each office," "protect personal information and trade secrets," and "provide IT security for products." Since the company considered vulnerability issues as security issues that must be addressed at all its company offices (including its subsidiaries), the committee members were selected from multiple sections to form a company-wide IT security team. The technical division handled vulnerability-related information and other associated information, while the R&D department established technical guidelines and security measures, conducted pre-shipment tests, among other tasks.

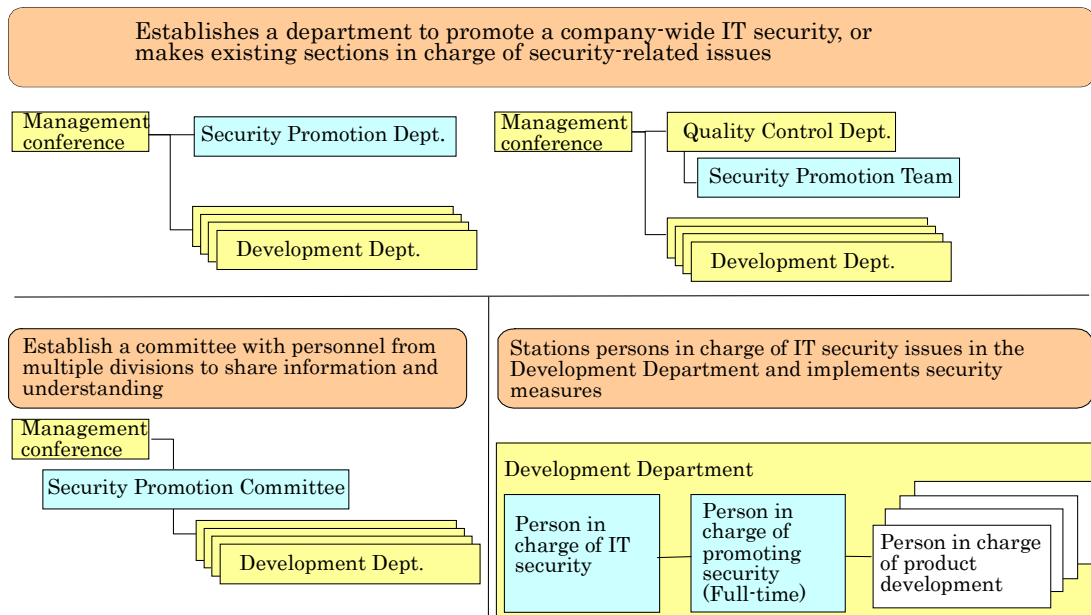


Figure 6 - Example of Organization for Ensuring IT Security

4.2.2. Education and Rules on IT Security

Since people working in product development are responsible for removing vulnerabilities detected in their products, it is vital that they understand the importance of establishing security measures. For this, they must provide checklists to ensure IT security, establish security policy and guidelines appropriate for their development process (such as a list of “Do's and Don'ts”), and educate their employees in IT security.

Generally, the development of embedded systems is carried out on a project-to-project basis; upon completion of a project, the development team is disbanded, leaving disintegrated information. If any vulnerability is detected, records and information related to each stage of work become keys to tackling the problem. In order to make use of such information when vulnerabilities are detected, it is necessary to establish a framework for collecting and managing such data and to specify rules on how to share the information.

In another case involving Company B, embedded software development guidelines were developed by the researchers within the R&D department who specialize in IT security. Company B requires its development staff to satisfy the international standard “ISO/IEC15408”⁷

⁷ ISO/IEC15408 is the International IT security standard for IT products and computer systems. The “IT Security Evaluation and Certification” systems, in which security level and functions of products and systems evaluated by a third-party organization based on this standard are being used.

(Common Criteria) by planning, designing, developing, and testing products in such a way that all vulnerabilities are overcome. The “ISO/IEC15408” is a government-backed standard, which may become one of the “Security Musts” for manufactures in the near future. The use of this standard is an effective approach. It is a common standard used in 25 countries joining the Common Criteria Recognition Arrangement.

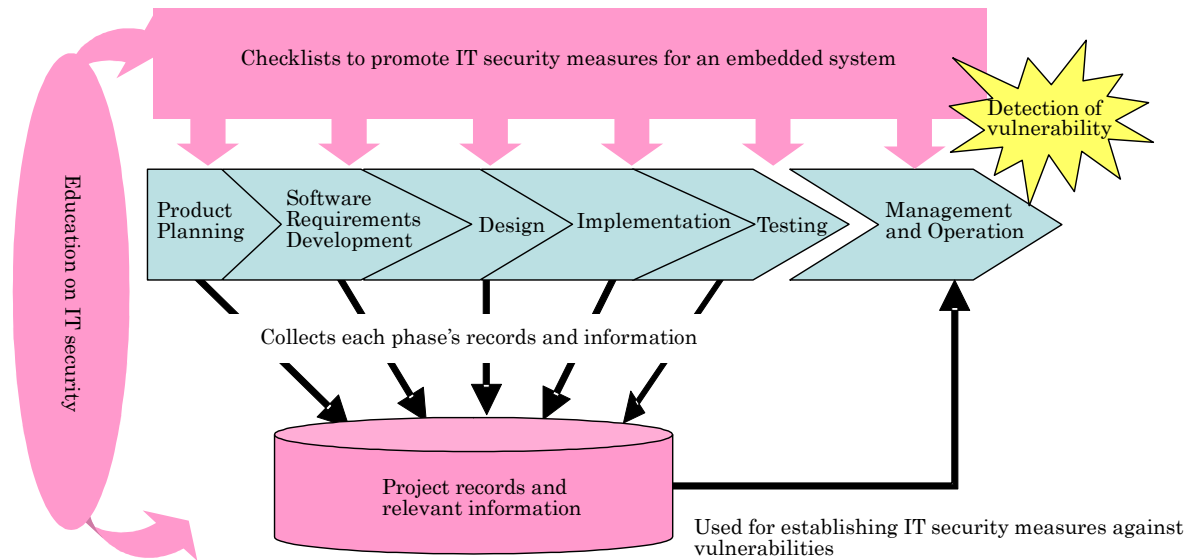


Figure 7 - Education and Rules on IT Security

4.2.3. Evaluation and Inspection of IT Security

Conducting appropriate reviews at each stage of development can eliminate the need to go back to any previous stage. The scope and frequency of reviews should be determined by the budget and development period, as in the case of debugging programs to fix problems. In order to ensure that the appropriate IT security has been put in place, it is important to conduct IT project audits by those in charge of IT security issues as well as those who are not members of the development team.

For example, in a case involving Company D, the company asked an IT security provider to inspect its products prior to shipment. During the tests, it was found that an attacker could potentially carry out an attack via a network to degrade the functions of the devices. The cause of the vulnerability was an inaccurate input-check routine in a program developed by the Company. The problem was fixed for 20,000 units that were due to be delivered, and the company was successfully able to ship them.

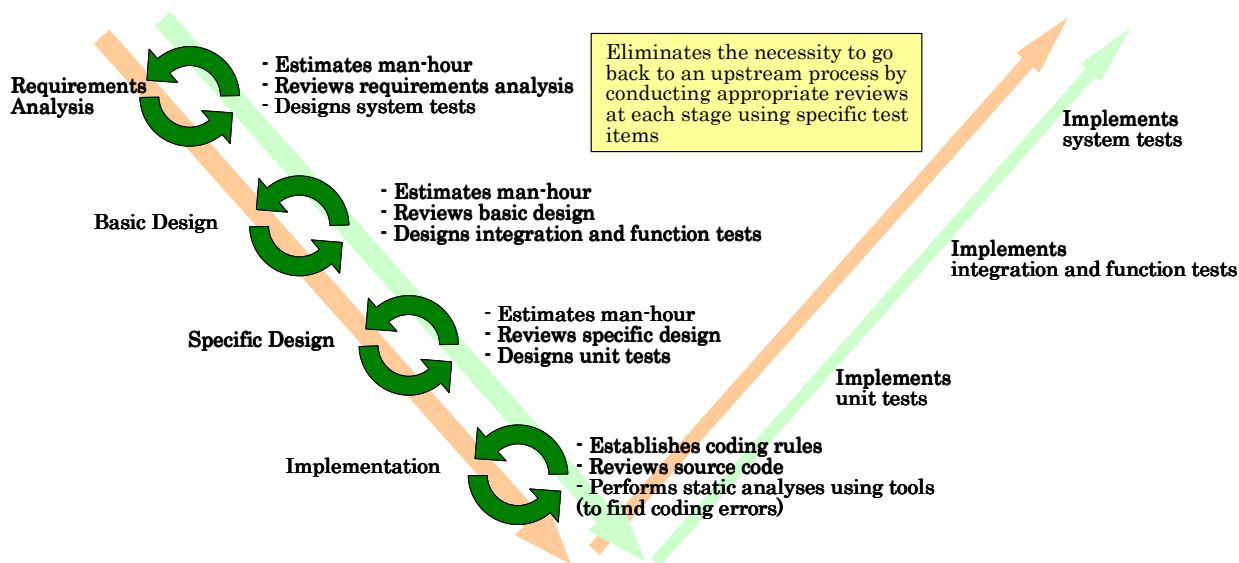


Figure 8 – Reviews Conducted at Each Stage of Development

4.2.4. Incident Response

For responding to security incidents, refer to the following examples.

Example 1: A problem with hard disk recorders used as a stepping-stone⁸ to attack other systems was fixed.

It has become clear that an Internet-capable hard drive Digital Versatile Disk (DVD) recorder can become an anonymous proxy⁹ when connected to the Internet. Manufacturer A discovered this vulnerability when it traced an attacker who posted a large amount of comments on a particular electronic bulletin board by using Internet connected DVD recorders as proxy servers. It is very difficult to trace back to the original attacker if the attacker is using multiple proxy servers to hide his identity. After this incident, manufacturer A asked users to update (or upgrade) their programs or to modify their security-settings. Later, the company announced that it would alter its basic planning policies so that products coming out in the future would not contain vulnerability allowing wrong security-settings.

This is a typical example of an attack in which a device was used as a stepping-stone to attack other devices. It was also the first such incident in the information appliance sector. Apparently

⁸ Stepping-stone means to take control of another user's computer to carry out attacks, such as unauthorized access to other systems.

⁹ Anonymous proxy is a relay server that anybody can use. A malicious user can abuse this server as a stepping-stone to attack other servers or systems, with his identity concealed.

the development staff had to cope with this problem by using trial-and-error methods.

Software programs for digital TV and similar devices are updated and distributed using airwaves. The same method can be used for hard drive DVD recorders, as illustrated in Figure 9 below.

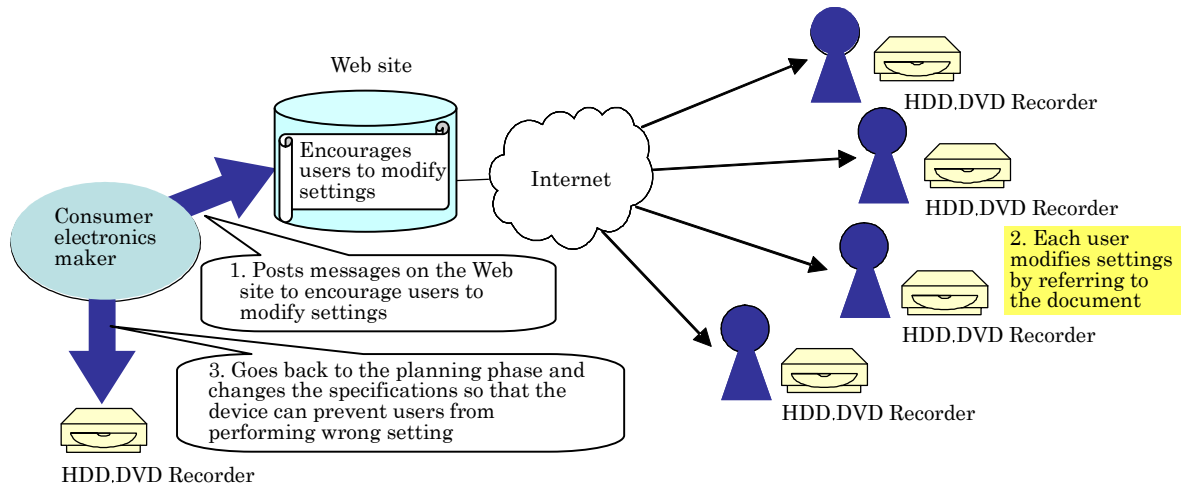


Figure 9 - How to Fix a Problem with Hard Drive DVD Recorders

Example 2: A problem with routers used as a stepping-stone to attack other devices was fixed.

A manufacturer discovered that its routers had been used as a stepping-stone to carry out a denial-of-service (DoS) attack. Vulnerability in TCP/IP¹⁰ was believed to have been exploited. Organizations that experienced the attack suffered damages, such as service stoppage. Tens of thousands of units had already been shipped. To deal with the problem, the manufacturer of the routers uploaded a revised program to its Web site, and its service staff made phone calls to users asking them to patch the routers program application.

The management of the company considered this a quality-related problem and alerted all its employees. They set up a special team to cope with similar problems in the future and added several items to their checklists to prevent similar incidents.

Because routers are internet infrastructure components, any problem related to the devices can affect business continuity. It was the right decision for the manufacture to treat the problem not just as a router-related problem but also as a quality-related problem.

¹⁰ TCP/IP is a standard protocol used on the Internet. TCP/IP stands for Transmission Control Protocol/Internet Protocol.

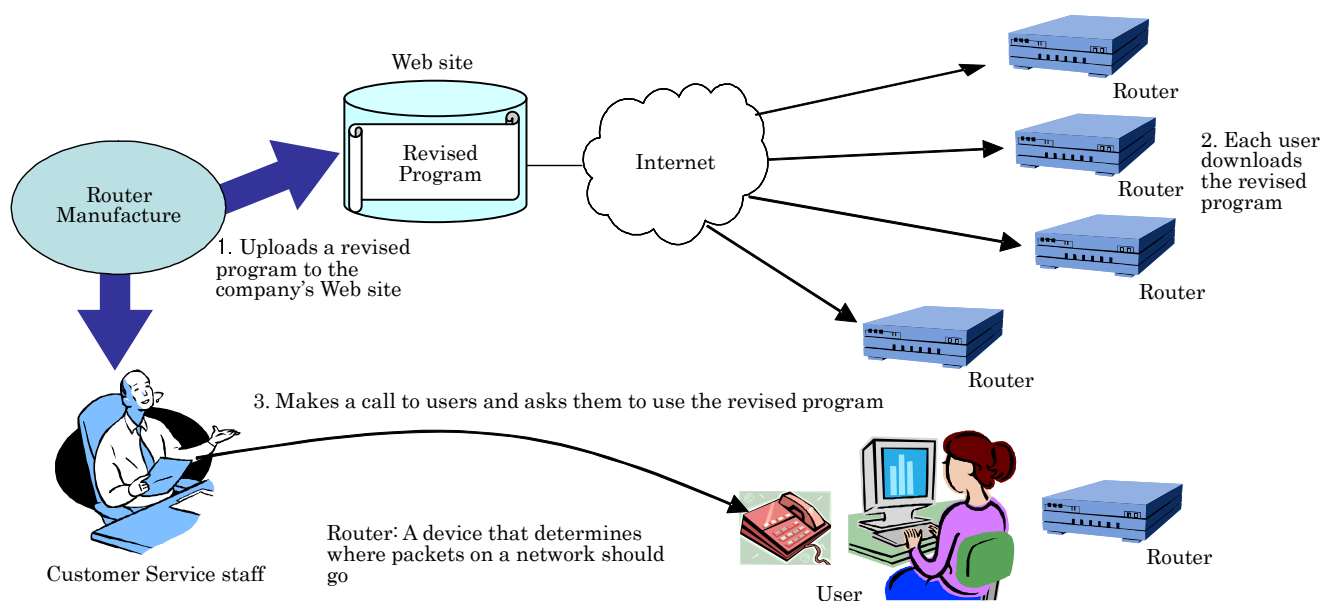


Figure 10 - How to Fix a Problem with Routers

Example 3: A problem with mobile phones in which URL of current page relayed to linked page was fixed.

Mobile phones manufactured by a company had a problem in which the URL¹¹ of the current page was automatically relayed to a linked page. Many browsers have a function that passes the URL information of a Web page to a linked page when its link is selected, but with the above-mentioned phones, when users performed certain operations, the URL was sent to a linked page, even though the users did not click any link. To resolve the problem, the manufacturer had users bring their phones to its outlets to update the program. On average, the service staff took thirty minutes to one hour to update the program for each unit.

For mobile phones that are widely used by many people, it is not easy to implement such recuperative measures because of the cost and time required. In the above case, it must have been a tough choice for the manufacturer to ask users to bring their phones to its outlets and have the sales staff fix the problem.

¹¹ Uniform Resource Locator (URL) is the address system used by the Internet to locate resources (such as web sites containing texts and images.) You can think of this as an address on the Internet.

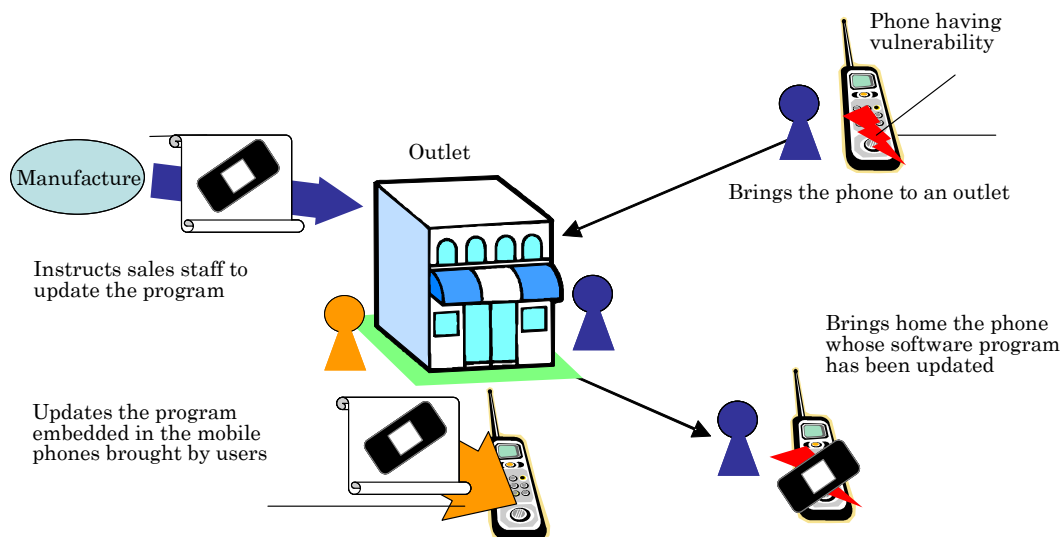


Figure 11 - How to Fix a Problem with Mobile Phone Browsers

Example 4: Measures were taken to reduce vulnerability in a protocol that could have significantly affected devices connected in a network.

The Centre for the Protection of National Infrastructure (CPNI)¹², a security agency in the U.K., released a report on vulnerability in the protocol “IPsec”¹³, which is widely used for a variety of network attached devices. It had become a topic of conversation as it could have caused system failures had it been exploited by an attacker. Ambiguities in its specifications and different interpretations of its users are believed to have caused the problem, creating security holes during the system-development stage.¹⁴

A wide variety of devices were targeted for an attack exploiting this vulnerability, and in fact, some manufactures had to take measures for almost all of their networking products. As a concrete measure, they posted a revised program on the Internet so that users could download it.

Vulnerability in a protocol can affect not only computers but embedded systems and, therefore, the computer department and the embedded system department must cooperate, sharing information and understanding to cope with any vulnerability detected.¹⁵

¹² CPNI is responsible for protecting UK’s important infrastructures. It collects and analyzes vulnerability information, and implements necessary measures to protect these infrastructures.

¹³ IPsec is a standard for securing Internet Protocol (IP) communications by encrypting and authenticating all IP packets.

¹⁴ NISCC Vulnerability Advisory 004033/IPSEC Vulnerability Issues with IPsec Configurations
<http://www.cpni.gov.uk/docs/re-20050509-00385.pdf?lang=en>

¹⁵ Ibid.

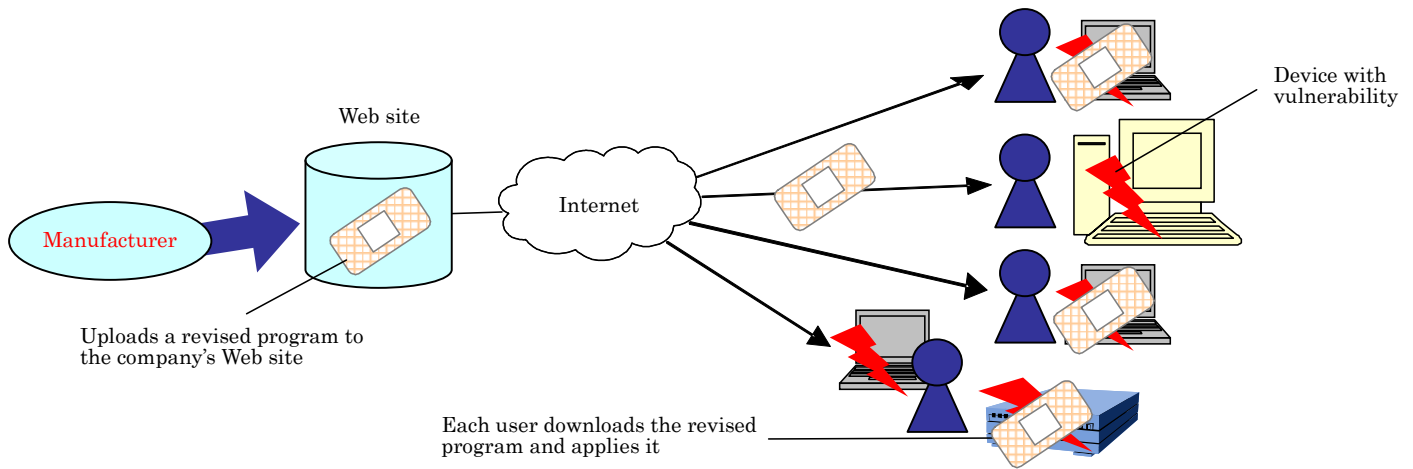


Figure 12 - How to Deal with Vulnerability in a Protocol that Can Significantly Affect Devices

5. Recommendations - Points Regarding IT Security Measures for Embedded Systems

The above information summarizes the results of research conducted this year by the GBDe Cyber Security Issue Group. Based on the group's findings and observations, it makes the following recommendations to promote IT security measures for embedded systems connected to a network. The recommendations are discussed in the context of product life cycle so that vulnerability can be prevented at all stages of product development.

5.1. Issues Covering the Entire Life Cycle

During the entire life cycle, an IT security specialist should be included in the audit process. He/she will review each phase of the embedded system development and check for any problems related to security measures.

IT security education should be provided to all embedded system development engineers and managers. The education should cover the latest terms used for IT security, the latest vulnerability information, and information on computer viruses and unauthorized computer access.

If some phases of the development process are outsourced to other companies, these companies may require the same level of enhancement in IT security technologies. They should adopt the same IT security measures and development framework to ensure that their company possesses the same level of IT security as the product's home company. Software development engineers in any company are encouraged to be certified by some sort of "IT Security, Technical Engineer" examination.

5.2. Issues Related to the Planning Phase

In the planning phase, any security-related requirements not originally included in the functional specifications of embedded systems should be clarified and documented. They can be defined by referring to the Common Criteria Ver3.0, or ISO/IEC15408.

It is important to prepare for cases where vulnerability may be detected after a product is launched on the market and to take appropriate countermeasures to guard against this risk.

On the technical side, companies should define all the possible risks, such as loss or leakage of confidential data, functional failures, or computer virus infection, and establish security policies for each risk defined. They should take into account any security-related risks associated with wrong operations or settings caused by users. The security policy established here will be referred to when deciding the specifications of the embedded systems.

Lastly, it is important to enable storage of security logs within the product. The log information will help users solve problems by making it easier to identify the cause. Also, a warning system that alerts users of any abnormal access attempt through the network is recommended.

5.3. Issues Related to the Design Phase

Information Technology security specialists should be involved in the embedded systems development process. They can review designed objects and documents from the security point of view. The results of their review should then be documented and reflected in the final design documents. The security review should also take place at the final stage of the design phase, including the check of externally installed or purchased software and of the use of Internet applications, from selection and operation settings to examination.

5.4. Issues Related to the Implementation Phase

It is recommended to perform a penetration test on all interfaces connected to the network. The test items should be chosen from the perspective of IT security and coordinated by the IT security specialist. The purpose of this testing is to ensure that confidential information does not leak out under any circumstances. The testing phase consists of unit testing, linkage testing and integration testing.

5.5. Issues Related to the Operation Phase

When vulnerabilities are detected, it is important to respond to the situation immediately and take appropriate actions. Companies and organizations need a framework to enable them to take appropriate measures against threats. One approach is to establish an incident response team that handles such problems.

In addition, it is helpful to prepare for possible incidents by gathering and analyzing relevant

FINAL – SUBJECT TO BSC APPROVAL – November 8, 2007

information on vulnerabilities, exploit codes, and other latest information. Operating a call center for inquiries from users is another option, but an IT security specialist should be consulted before answering questions.

5.6. Issues Related to the Disposal Phase

In the disposal phase, information accumulated within the embedded systems by users during the operation phase must be erased. This means it is necessary to remove data stored in the memory or other storage media. For example, although IC cards, including credit cards, expire and become invalid, they can still be abused by a third person. To avoid this, users need to cut up those cards. With mobile phones and other information devices, even though some users erase personal information and private contents by themselves when they buy a new product, upgrade to new model, or terminate use for some other reason, there still might be some data left in the memory or other storage media. Caution is essential if information protected during the operation phase is to remain securely protected during the disposal phase.

5.7. Other Points for Consideration (Manuals, Product Catalogs, Packages and User Interfaces)

Manuals and other documents should be provided that clearly state the emergency response procedures and measures to be taken for security incidents that occur via the network (such as how to disconnect the device causing the problem from the network).

In addition, manuals or other documents should specify confidential data disposal procedures for individual users and any other practical points for securely connecting embedded systems to a network.

Contributions were provided by the following Issue Group members: Hitachi, Japan; Institute for Information Industry (III), Taiwan; and CyberSecurity, Malaysia.