한국항행학회 논문지 제11권 제3호 2007년 9월

# 임베디드 소프트웨어 개발현장보안에 관한 연구

# A Study on the Development Site Security for Embedded Software

여상수*, 김태훈**, 조성언***, 코우이치 사쿠라이*

Sang-Soo Yeo*, Tai-Hoon Kim**, Sung-Eon Cho***, and Kouich Sakurai*

## 요 약

유비쿼터스 컴퓨팅을 구현하기 위한 임베디드 시스템적 요소, 즉 각종 전자기기, 가전제품, 제어장치 들은 단순히 회로로만 구성되어 있는 것이 아니라 특정한 기능을 수행하도록 프로그램이 내장되어 있는데 이러한 시스템 제어역할을 수행하는 다양한 프로그램을 임베디드 소프트웨어라고 정의할 수 있다. 임베디드 소프트웨어는 시스템의 기능을 제어하는 핵심 요소이므로 내용이나 제어 구조가 공개되는 경우에는 심각한 영향을 받을 수 있다. 임베디드 소프트웨어의 보안은 크게 두 부분으로 나뉘어 고려될 수 있다. 첫 번째는 외부의 위협원이 내부로 침투하여 관련 정보를 유출하는 것이고, 두 번째는 내부 혹은 외부의 위협원이 임베디드 소프트웨어에 악성 코드를 삽입하는 등 불법적인 행동을 하는 것이다. 본 논문에서는 첫 번째 관점에서, 임베디드 소프트웨어를 개발하고 있는 개발 현장에 대한 보안 점검 요소들을 도출하고 제안하였다. 개발 현장에 대한 보안 점검을 통해 외부 위협원의 접근을 원천적으로 차단하는 동시에, 임베디드 소프트웨어의 비인가된 변형을 간접적으로 예방할 수 있을 것으로 기대된다.

## Abstract

Systematic components for implementing ubiquitous computing, for example, electronic devices, electric home appliances, and controllers, etc, are consist of not only circuits but also softwares expected to do some special system-controlling functions, and these softwares used to be called like as embedded software. Because embedded software is a core component controlling systems, the codes or control flows should be protected from being opened to the public or modified. Embedded software security can be divided into 2 parts: first is the unauthorized access to development site and embedded software, second is the unauthorized disclosure or modification. And this research is related to the first aspect of them.This paper proposes some security check requirements related to embedded software development site by analyzing the ALC_DVS.1 of the ISO/IEC 15408 and Base Practices (BPs) of the ISO/IEC 21827. By applying this research, we expect to protect unauthorized modification of embedded software indirectly.

Key words : Embeded Software, Threat Agents, Development Site Security

* 일본 큐슈대학교 시스템정보과학부(Dept. of Information and Systems Engineering, Kyushu University)
** 한남대학교 멀티미디어학부(Dept. of Multimedia Engineering, Hannam University)
*** 순천대학교 정보통신공학부(College of Information and Communication Eng. Sunchon National University)
· 제1저자 (First Author) : 여상수
· 교신저자 (Corresponding Author) : 조성언
· 접수일자 : 2007년 7월 16일

## I. Introduction

The importance and usability of embedded software can be proved indirectly by referencing Embedded Software Market Analysis Report. In 2003, the market of embedded software was 106.6 billion dollars and this was 17% of total software market share. But in 2007, the market of embedded software was expected to be 138.4 billion dollars [1].

Systematic components for implementing ubiquitous computing, for example, electronic devices, electric home appliances, and controllers, etc, are consist of not only circuits but also softwares expected to do some special system-controlling functions, and these softwares used to be called like as embedded software.

Because embedded software is a core component controlling systems, the codes or control flows should be protected from being opened to the public or modified. Embedded software security can be divided into 2 parts: first is the unauthorized access to development site and embedded software, second is the unauthorized disclosure or modification. And this research is related to the first aspect of them.

This paper proposes some security environments for embedded software development site by analyzing the ALC_DVS.1 of the ISO/IEC 15408 and Base Practices (BPs) of the ISO/IEC 21827.

## Ⅱ. Overview of Related Works

### 2-1 Common Criteria

The multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC is presented as a set of distinct but related parts as identified below [2].

Part 1, Introduction and general model, is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation.

Part 2, Security functional requirements, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Target of Evaluations). Part 2 catalogues the set of functional components, families, and classes.

Part 3, Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families and classes.

### 2-2 Protection Profile

A PP defines an implementation-independent set of IT security requirements for a category of Target of Evaluations (TOEs). Such TOEs are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific TOE.

The purpose of a PP is to state a security problem rigorously for a given collection of systems or products (known as the TOE) and to specify security requirements to address that problem without dictating how these requirements will be implemented. For this reason, a PP is said to provide an implementation-independent security description.

Research results of this paper can be applied to the development of PP very easily.

### 2-3 Security Requirements for Development Site

ALC_DVS.1 component consists of one developer action element, one evidence element, and two evaluator action elements.

Contents and presentation of evidence element of

ALC_DVS.1 component are described as like following (Requirements for content and presentation of evidence are identified by appending the letter 'C' to the element number):

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

But there was one more evidence element of ALC_DVS.1 component in CC version 2.1.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

And CC version 3.1 contains 2 more evidence element of ALC_DVS.2 component.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

In this paper, only one element, ALC_DVS.1.1C will be considered.

### 2-4 SSE-CMM

Modern statistical process control suggests that higher quality products can be produced more cost-effectively by emphasizing the quality of the processes that produce them, and the maturity of the organizational practices inherent in those processes.

More efficient processes are warranted, given the increasing cost and time required for the development of secure systems and trusted products. The operation and maintenance of secure systems relies on the processes that link the people and technologies. These interdependencies can be managed more cost effectively by emphasizing the quality of the processes being used, and the maturity of the organizational practices inherent in the processes [3].

The SSE-CMM model is a standard metric for security engineering practices covering:

· The entire life cycle, including development, operation, maintenance, and decommissioning activities

· The whole organization, including management, organizational, and engineering activities

· Concurrent interactions with other disciplines, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance

· Interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation

## Ⅲ. Threat Level for Development Site

There are many threats to development site. According to the importance and economical value of embedded software, the level of threat will be increased. If the level of threat were high, organizations should invest more resource to protect development site.

Threat Level can be decided by considering threat agents, motivation, tools and equipment, time, and so on. Working environment of each development is different, and therefore, sometimes organizations should consider relationships among some components. But this is very dependent on the characteristics of each site, so organizations can not consider all cases [4].

Easiest way to decide threat level is not considering the relationship among the components. And this method can be extended easily to specific site.

Next table 1 is the example of threat level. But in this

paper, we assumed Threat level 1 to derive basic security requirements and check point of embedded software development site. About the higher threat level, more specific researches are needed to find proper security requirements.

Table 1 Threat Level

| Threat Level | Description |
|---|---|
| TL1 | Security check and confirmation are needed |
| TL2 | Urgent security check and confirmation are needed |
| TL3 | Some disturbances may be happened |
| TL4 | Some difficulties may be happened |
| TL5 | Site may not secure sometimes |
| TL6 | Site is not secure |

## Ⅳ. Derivation of Check Points

### 4-1 Comparison in Process Area

The SSE-CMM has two dimensions, "domain" and "capability." The domain dimension is perhaps the easier of the two dimensions to understand. This dimension simply consists of all the practices that collectively define security engineering. These practices are called Base Practices (BPs).

The base practices have been organized into Process Areas (PAs) in a way that meets a broad spectrum of security engineering organizations. There are many ways to divide the security engineering domain into PAs. One might try to model the real world, creating process areas that match security engineering services. Other strategies attempt to identify conceptual areas that form fundamental security engineering building blocks. The SSE-CMM compromises between these competing goals in the current set of process areas.

Each process area has a set of goals that represent the expected state of an organization that is successfully performing the PA. An organization that performs the BPs of the PA should also achieve its goals.

There are eleven PAs related to security in the SSE-CMM, and we found next three PAs which have compliance with ALC_DVS.1 component:

- PA01 Administer Security Controls
- PA08 Monitor Security Posture
- PA09 Provide Security Input

### 4-2 Comparison in Base Practice

All of the BPs in each PA mentioned earlier need not have compliance with the evidence elements of ALC_DVS.1. But if any BP included in the PA is excluded or failed when the evaluation is preceded, the PA itself is concluded as fail.

Evidence element ALC_DVS.1.1C requires that the development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. But ALC_DVS.1.1C dose not describe what are the physical, procedural, personnel, and other security measures. Evidence element ALC_DVS.1.2C requires that the development security documentation shall provide evidence that the security measures described in ALC_DVS.1.1C are followed during the development and maintenance of the TOE.

Some BPs contains examplework products, and work products are all the documents, reports, files, data, etc., generated in the course of performing any process. Rather than list individual work products for each process area, the SSE-CMM lists Example Work Products (EWPs)of a particular base practice, to elaborate further the intended scope of a BP. These lists are illustrative only and reflect a range of organizational and product contexts. As though they are not to be construed as mandatory work products, we can analysis

the compliance between ALC_DVS.1 component and BPs by comparing evidence elements with these work products. We categorized these example work products as eight parts:

1. Physical measures related to the security of development site and system.
2. Procedural measures related to the access to development site and system.
3. Procedural measures related to the configuration management and maintenance of development site and system.
4. Procedural measures (contain personnel measures) related to the selection, control, assignment and replacement of developers.
5. Procedural measures (contain personnel measures) related to the qualification, consciousness, training of developers.
6. Procedural measures related to the configuration management of the development work products.
7. Procedural measures related to the product development and incident response in the development environment.
8. Other security measures considered as need for security of development environment.

Categorized eight parts above we suggested are based on the contents of evidence requirement ALC_DVS.1.1C, and contains all types' measures mentioned in ALC_DVS.1.1C. But the eight parts we suggested may contain the possibility to be divided to more parts.

We can classify work products included in BPs according to eight parts category mentioned above. Next table 2 describes the result.

Table 2. Categorization of work products

| Number of category | Work Products | Related BP |
|---|---|---|
| 1 | control implementation | BP.01.02 |
| | sensitive media lists | BP.01.04 |
| 2 | control implementation | BP.01.02 |
| | control disposal | BP.01.02 |
| | sensitive media lists | BP.01.04 |
| | sanitization, downgrading, & disposal | BP.01.04 |
| | architecture recommendation | BP.09.05 |
| | implementation recommendation | BP.09.05 |
| | security architecture recommendation | BP.09.05 |
| | users manual | BP.09.06 |
| 3 | records of all software updates | BP.01.02 |
| | system security configuration | BP.01.02 |
| | system security configuration changes | BP.01.02 |
| | records of all confirmed software updates | BP.01.02 |
| | security changes to requirements | BP.01.02 |
| | security changes to design documentation | BP.01.02 |
| | control implementation | BP.01.02 |
| | security reviews | BP.01.02 |
| | control disposal | BP.01.02 |
| | maintenance and administrative logs | BP.01.04 |
| | periodic maintenance and administrative reviews | BP.01.04 |
| | administration and maintenance failure | BP.01.04 |
| | administration and maintenance exception | BP.01.04 |
| | sensitive media lists | BP.01.04 |
| | sanitization, downgrading, and disposal | BP.01.04 |
| | architecture recommendations | BP.09.05 |
| | implementation recommendations | BP.09.05 |
| | security architecture recommendations | BP.09.05 |
| | administrators manual | BP.09.06 |
| 4 | an organizational security structure chart | BP.01.01 |
| | documented security roles | BP.01.01 |
| | documented security accountabilities | BP.01.01 |
| | documented security authorizations | BP.01.01 |

| | | |
|---|---|---|
| | sanitization, downgrading, and disposal | BP.01.04 |
| 5 | user review of security training material | BP.01.03 |
| | logs of all awareness, training and education undertaken, and the results of that training | BP.01.03 |
| | periodic reassessments of the user community level of knowledge, awareness and training with regard to security | BP.01.03 |
| | records of training, awareness and educational material | BP.01.03 |
| 6 | documented security responsibilities | BP.01.01 |
| | records of all distribution problems | BP.01.02 |
| | periodic summaries of trusted software distribution | BP.01.02 |
| | sensitive information lists | BP.01.04 |
| | sanitization, downgrading, and disposal | BP.01.04 |
| 7 | periodic reassessments of the user community level of knowledge, awareness and training with regard to security | BP.01.03 |
| | design recommendations | BP.09.05 |
| | design standards, philosophies, principles | BP.09.05 |
| | coding standards | BP.09.05 |
| 8 | philosophy of protection | BP.09.05 |
| | security profile | BP.09.06 |
| | system configuration instructions | BP.09.06 |

From the table above, we can verify that some BPs of SSE-CMM may meet the requirements of ALC_DVS.1.1C by comparing the contents of evidence element with work products.

## Ⅴ. Conclusion and Future Work

This paper proposes some security environments and requirements for embedded software development site by analyzing the ALC_DVS.1 of the ISO/IEC 15408 and Base Practices (BPs) of the ISO/IEC 21827. And this research was done by considering threat level 1.

In these days, some security countermeasures are used to protect development site. But the security countermeasures should be considered with consideration of applicable threats and security solutions deployed to support appropriate security services and objectives. Maybe this is one of our future works.

## References

[1] Embedded Software Market Analysis Report, 2004~2005.

[2] ISO/IEC 15408-1, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

[3] ISO/IEC 21827, Information technology Systems Security Engineering Capability Maturity Model (SSE-CMM).

[4] 김태훈, 김석수, 박길철, 중요 정보시스템 위협원에 대한 분석, *한국항행학회 논문지*, 2007년 6월호.

## 여 상 수 (呂相壽)

1997년 : 중앙대학교 (공학사)
1999년 : 중앙대학교 (공학석사)
2005년 : 중앙대학교 (공학박사)
2006년 : 단국대학교 강의전임강사
2007년 ~ 현재 : 일본 큐슈대학교 방문연구원
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어

## 김 태 훈 (金泰勳)

1995년 : 성균관대학교 (공학사)
1997년 : 성균관대학교 (공학석사)
1999년 : (주)신도리코 기술연구소 연구원
2002년 : 성균관대학교 (공학박사)
2004년 : 한국정보보호진흥원 선임연구원
2006년 : 국군기무사령부 사무관
2007년 : 이화여자대학교 연구교수
2007년 ~ 현재 : 한남대학교 멀티미디어학부 조교수
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어

## 조 성 언(趙誠彦)

1989년 2월 : 한국항공대학교 항공통신정보공학과 (공학사)
1991년 8월 : 한국항공대학교 대학원 항공통신정보공학과 (공학석사)
1997년 2월 : 한국항공대학교 대학원 항공전자공학과 (공학박사)
1997년 3월 ~ 현 재 : 순천대학교 정보통신공학부 부교수
관심분야 : 무선통신시스템, Wireless USN

## 코우이치 사쿠라이(櫻井 幸一)

1986년 : 큐슈대학교 (이학사)
1988년 : 큐슈대학교 (이학석사)
1993년 : 큐슈대학교 (공학박사)
1994년 ~ 현재 : 큐슈대학교 시스템정보과학부 교수
관심분야 : 유비쿼터스 및 RFID보안, 임베디드 소프트웨어