Effect of Differences of Programming Languages on Information Security Software Quality

HYUNGSUB KIM, SANGGU BYUN, SEOKHA KOH

***Abstract*— Online information infringement has been increasingly diversified. As such infringement attacks have grown diversified, no single software written solely by one programming language is able to defend every attack completely. Although most developers use one language for several years but only few understand the language to a full extent. It is deemed that information protecting softwares can be improved with the advantages of object-oriented languages. Many South Korean companies producing many information security protection products, however, use C for software development. The most frequently utilized computer language is Java but when it comes to information security, especially, C is mostly employed. Some parts of information security softwares are better when dealt with Java. In this recognition, the present research seeks to compare the characteristics of OSO/ICE 9126, CC and information security softwares to come up with a more appropriate programming language.**

***Keywords*—** Programming language, Information Security software, IOS/IEC 9126, Software Evaluation, Information Security Software Features, CC

I. INTRODUCTION

A A part operated by hardware is controlled by software owing to fast computing speed. Accordingly, an advantage of improving flexibility and maintenance is brought. However, software largely depends on the expression and computing capability of programming language used in the development of software, and developer's experience and accumulated technology makes a big difference in performance. In particular, these days when a system becomes complex and distributed, a controversy about the stability of software system and the preciseness of programming language is largely aroused[1].

Programming languages has been developed in line with the purpose of a software and with existing languages, programs were developed differently according to operation systems.

However, as for Java, since identical programs are independent from platforms or, in other words, operable under different operation systems, Java has become the most used programs language now.

C language, however, is most utilized in information security products. When asked why language C is more used than Java, information security software developers could not give an accurate answer.

This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA(Korea Internet Security Agency)(H2101-13-1001)

Hyungsub Kim is with the Department of Information Security Management of Chungbuk National University, Chungbuk, South Korea (e-mail: khsub@ chungbuk.ac.kr).

SangGu Byun is with the From2 Information & Communication Co., Ltd., Daejeon, South Korea (e-mail: bsg@frm2.co.kr).

SeokHa Koh is with the Department of Management Information System, Chungbuk National University, 12 Gaeshin-dong, Heungduk-gu, Cheongju, ChungBuk 361-763, South Korea (corresponding author. phone: +82-43-261-3343; fax: +82-43-273-2355; e-mail : shkoh@chungbuk.ac.kr).

II. RELATED RESEARCH

This chapter will discuss an effect produced by programming language in developing information security software by checking ISO/IEC common criteria and security element among software evaluation model through comparing the characteristics of information security software and the characteristics of C and Java programming language.

A. Information Security Software

Korea Internet & Security Agency (2010) defines information security SW as software run in order to prevent information damage • alteration • leak and so on during the collection • processing • storage • search • transmission • reception of information. Information security emphasizes measures against information leak, destruction, and alteration intentionally made to occur by human being. Information protection is a comprehensive term that includes measures against infringement by a mistake of human being or a natural disaster that occurs by chance as well as intentional infringement. Information protection is defined in various forms according to each country, and it is defined as 'what is to devise managerial and technical means in order to prevent information damage • alteration • leak and so on during the collection • processing • storage • search • transmission • reception of information' in Article 2 of Framework Act on Informatization Promotion[12].

In case of information security software, the most important quality is security differently from general software. Features such as integration compatibility, maintainability, reliability,

usability, high performance that is performance element shall be considered [17].

(1) High performance

General software is run and used when necessary. However, information protection products shall be always run in order to protect assets inside operating environment [17].

(2) Usability

It shall be easy to understand a function, interface, message, and help, and so on and to learn a function in order that any user who uses information security software can easily and conveniently use information security products[17].

(3) Reliability

Information security software shall have its own response capability against a defect that makes the product down in using these or a defect that puts the product severely out of order so as to guarantee that it is always run. And it shall be capable of taking measures so that it can prevent a severe error that may occur due to being mishandled by user[17].

(4) Maintainability

A new weak point may always appear in information security software. And in case a new weak point appears, the information protection product shall be made to be capable of dealing with the new weak point by upgrading the information protection product[17].

(5) Integration compatibility

It shall be possible to be successfully installed and removed according to installation and removal procedure. And in case of upgrade, it shall be possible to use a function and data used in the previous version in the same way as before[17].

B. C language and java language features and comparison

language is used as the most popular programming language because the used instruction words are brief, and strong programming is possible. Besides, it takes firm hold as an important language because it faithfully follows a concept of structured programming, and can use an instruction word that can prepare a program corresponding to low-level language at the level of assembly language even though it is a high-level language at the same time[18].

Java programming language is based on C language and C++ language. However, Java language aims at purer object-oriented [7, 13] programming language than C++ language. And Java language doesn't include feature that is complex and may easily cause an error, which C++ language has. Java language syntax is comparatively simple, and has an aspect where the use of keyword is natural in comparison with C language or C++ language[5].

Table. 1 Compare C and Java language

Thing	C	Java
Type of language	function oriented	object oriented
basic programing unit	function	class = ADT
portability of compiled code	possible with discipline	yes
security	no, recompile for each architecture	yes, bytecode is "write once, run anywhere"
integer types	limited	built-in to language
floating point types	float usually 32 bit, double usually 64 bit	float is 32 bit IEEE 754 binary floating point, double is 64 bit IEEE 754
character type	char is usually 8 bit ASCII	char is 16 bit UNICODE
memory address	pointer	reference
ass-by-value	primitive data types, structs, and pointers are passed by value; array decays to pointer	all primitive data types and references (which includes arrays), are passed by value
allocating memory	malloc	new
de-allocating memory	free	automatic garbage collection
memory allocation of data structures and arrays	heap, stack, data, or bss	heap
buffer overflow	segmentation fault, core dump, unpredicatable program	checked run-time error exception
data hiding	opaque pointers and static	private
interface method	non-static function	public method
data type for generic item	void *	Object
polymorphism	union	inheritence
graphics	use external libraries	Java library support, use our standard drawing library
preprocessor	yes	no

Modified from http://introcs.cs.princeton.edu/java/faq/c2java.html)[13]

Security is in the process of software development, software development, developers mistakes, logical errors due to software vulnerabilities that can be nested to minimize the causes for the development of secure software means that security activities[9][20]. Source code can be generated from the information security software security issues should be considered when selecting a security weakness.

Table . 2 List of security weaknesses in C and Java languages

Table 2 presents commonly used programming languages, C and Java are compared. 58 security weaknesses in the C language, Java language has 79. The Java language has many security weaknesses more than C language. Table 2 shows that, except for the two languages were summarized in a common vulnerability. Java security weaknesses in this Table can be more.

Type	Security weaknesses		Type	Security weaknesses	
Language	C	JAVA	Language	C	JAVA
The data validation and expression	Stack-based Buffer Overflow	Unrestricted Upload of File with Dangerous Type	Code Error	Signed to Unsigned Conversion Error	Code Correctness: Call to notify()
	Heap-based Buffer Overflow	URL Redirection to Untrusted Site, Open Redirect		Type Mismatch: Integer to Character	Code Correctness: Incorrect serialPersistentFields Modifier
	Buffer Underwrite, Buffer Underflow	Failure to Sanitize Data within XQuery Expressions, XQuery injection		Return of Stack Variable Address	Code Correctness: Call to Thread.run()
	Out-of-Bounds Read	Failure to Sanitize Data within XPath Expressions, XPath injection		Code Correctness: Macro Misuse	Code Correctness: Non-Synchronized Method Overrides Synchronized Method
	Improper Validation of Array Index	Cross-Site Request Forgery		Code Correctness : Memory Free on Stack Variable	
	Improper Null Termination	Improper Neutralization of CRLF Sequences in HTTP Headers, HTTP Response Splitting		Code Correctness: Premature thread Termination	
	Unexpected Sign Extension	SQL Injection: JDO	Encapsulation		Exposure of Data Element to Wrong Session
	Unsigned to Signed Conversion Error	SQL Injection: Persistence			Private Array-Typed Field Returned From A Public Method
		SQL Injection: mybatis Data Map			Public Data Assigned to Private Array-Typed Field
		Improper Neutralization of Script-Related HTML Tags in a Web Page , DOM			Use of Inner Class Containing Sensitive Data
		Improper Neutralization of Directives in Dynamically Evaluated Code, Eval Injection			Critical Public Variable Without Final Modifier

		Use of Externally-Controlled Input to Select Classes or Code, Unsafe Reflection			Use of Dynamic Class Loading
		Download of Code Without Integrity Check	API misapplication	Use of Inherently Dangerous Function	J2EE Bad Practices: Direct Management of Connections
		SQL Injection: Hibernate		Creation of chroot Jail Without Change Working Directory	J2EE Bad Practices: Direct Use of Sockets
		Reliance on Untrusted Inputs in a Security Decision		Often Misused: String Management	J2EE Bad Practices：Use of System.exit()
Security functions	Incorrect Privilege Assignment	Missing Authentication for Critical Function		Use of getlogin() in Multithreaded Application	Missing Check for Null Parameter
	Least Privilege Violation	Weak Password Requirements			EJB Bad Practices: Use of Sockets
		Information Through Persistent Cookies			Object Model Violation: Just one of equals() and hashCode() Defined
		Sensitive Cookie in HTTPS Session without 'Secure' Attribute	Time and status	Uncontrolled Recursion	Uncontrolled Recursion
		Download of Code Without Integrity Check			Race Condition: Static Database Connection, dbconn
		Cross-Site Request Forgery, CSRF			Race Condition: Singleton Member Field
		Insufficient Session Expiration			J2EE Bad Practices：Direct Use of Threads
		Password Management: Heap Inspection			Double-Checked Locking
		Password Management: Password in Redirect	Error Handling		Weak Password Requirements

Source: Java secure coding guide and C secure coding guide

C. ISO/IEC 9126

The quality of software is a whole that indicates how much explicit requirement and implicit requirement is met in the function, performance, and satisfaction of software. Therefore, the quality of software product is established by meeting the various requirements according to the features of software product. ISO/IEC 9126 is international standard that stipulates software quality model, and becomes guidelines to establish and evaluate the quality of software. Software quality characteristic and subcharacteristic that is the core of quality evaluation is shown in table 3 , according to ISO/IEC 9126-1 revised in the year 2000[6].

Table . 3 The ISO 9126 quality attributes

Main Attribute	Sub Attribute
Funcutionality	suitability
	Accuracy
	Interoperability
	Security
	Functionality Compliance
Reliability	Maturity
	Fault Tolerance

	Recoverability
	Reliability Compliance
Usability	Understandability
	Learnability
	Operability
	Attractiveness
	Usability Compliance
Efficiency	Time Behaviour
	Resource Utilisation
	Efficiency Compliance
Maintainability	Analyzability
	Changeability
	Stability
	Testability
	Maintainability Compliance
Portability	Adaptability
	Installability
	Co-Existence
	Replaceability
	Portability Compliance

Source : ISO/IEC 9126

Quality characteristics presented like table 3 proposes a set of 120 metrics2 for measuring the various characteristics and subcharacteristics of software quality[2]. Because international standards like this have a lot of comprehensive and abstract part, standards suitable for the actual condition of their own country according to country are established and used with international standards as the center in order to apply the standards to a specific country[13].

D. Common Criteria (CC)

CC in the United States, Australia, New Zealand, Canada, France, Germany, Japan, Netherlands, Spain, the United Kingdom, with the support by the government has contributed to the development[3], and is a common structure and language that describes the guidance regarding information product or system security for the information system developers and assessors via Protection Profile (PP) and Security Target (ST)[11].

Common criteria are largely composed of 3 parts. Introduction and general model is presented in Part 1, and security functional requirements are included in Part 2, and security assurance requirements are included in Part3[3].

(1) Part 1 : Introduction and general model

In this section, the common evaluation criteria are outlined and information security system evaluation principles and general ideas are defined. Standard constituting components are explained, terms and abbreviations used in the whole standards are defined along with the key ideas of evaluation targets, evaluation certification system and common evaluation criteria users, etc. Essential ideas are described such as protection profile, security requirement package, compliance declaration and evaluation result. Section 1 provides guidelines for making a security goal statement[3].

(2) Part 2 : Security functional components

Section CC 2 serves as the basis for expressing the security functional requirement described in the protection profile(PP) or security goal statement(ST). Such requirements are to explain TOE(Target of Evaluation) security behaviors and used to satisfy the security purposes described in protection profile/security goal statement. And these requirements explain security features such as users' recognition as a direct interaction with IT (input, output, etc.) or as an IT reaction [3].

Table. 4 CC Security functional requirements

Class name	Class title	Explanation
FAU	Security Audit	Detect, record, store and separate security activity-related information
FCO	Communication	Detect the identity of a user trying to exchange data.
FCS	Cryptographic Support	Manage and calculate encryption key.
FDP	User Data Pritection	Protect user data.
FIA	Identification & Authenticatio n	Check and authorize user identity
FMT	Security Management	Manage TSF(TOE Security Functionality) data, security attributes and security functions.
FPR	Privacy	Protect user privacy
FPT	Protection of Tusted Security Functions	Protect and manage TSF data
FRU	Resource Utillization	Secure available resources for TOE.
FTA	TOE Access	Protect user session in relation to TOE.
FTP	Trusted Path/ Channel	Secure safe communication channels between user and TSF or between TSFs.

Source: Jongmin Lee, 2006

(3) Part 3 : Security assurance components

This functions as the basis for expressing the assurance requirements stated in protection profile or security goal

statement. These requirements establish a standardized manner to express TOE assurance requirement. Common evaluation criteria section 3 is consisted of assurance component, family and class. This common evaluation criteria section 3 defines evaluation standard for protection profile/security goal statement and encompasses the evaluation assurance grades defined by the common evaluation criteria as TOE assurance levels. The application of the common evaluation criteria section 3 includes security IT product consumers, developers and evaluators [3].

Table. 5 CC Assurance requirements

Class name	Class Title	Explanation
APE/ASE	Protection Propile Evaluation/Security Target Evaluation	Conceptual security requirement on TOE
ADV	Development	Stability in TOE interface, design and structure
ALC	Life Cycle Support	Development procedure, development tool, negotiation management, development environment security, distribution
AGD	Guidance Documents	Safe installation to prevent inaccurate TOE structuring and safe management of TOE such as installation and operation
ATE	Tests	Test if TOE functions as designed
AVA	Valnerability Analysis	Check for any aspect vulnerable to abuse in the process of TOE development or operation
ACO	Composition	Evaluation between evaluated TOEs or between not=evaluated TOE and evaluated TOE

Source: Jongmin Lee, 2006

I. Quality Measurement

The table 6 organized ISO/IEC 9126 software quality items according to information security software requirements and programming languages C and Java.

Table. 6 Comparison between information security softwares' non-functional requirements and C language and Java's non-functional characteristics.

Type	Requirements	C	Java
Functionality	High	Low	High
Reliability	High	High	Low
Usability	Low	Low	High
Efficiency	High	High	Low
Maintainability	High	Low	High
Portability	High	High	Low

(1) Functionality

The most important quality of information security software is security thus facing higher requirements including security. Java delets previous language functions or adds new ideas during development to prevent and avoid security threats, thus gained higher recognition in security than C[10].

(2) Reliability

Information security software, if used to safeguard systems under operation, should be able to respond to product defects or malfunctions for itself as well as user's mal-operation for itself in advance. In this sense, information security software requires high reliability[17]. Java, however, is in an environment where viruses or Trojan horse can easily transmit and proliferate. Therefore Java was measured as having lower reliability[10].

(3) Usability

Usability refers to a software product capacity to make users understand, learn and prefer it when the software is used in a proper, designated environment[16]. Information security software, as it is not directly used by users, was measured lower in usability.

Java is more sophisticated language than C and used in diverse areas such as business application, web application, etc[4] Java, therefore, was marked higher in usability than C.

.

(4) Maintainability

The ability to change a software product. Changes, here, include software modification, improvement and adaptation according to operational environment, requirement and functional specifications [15][16], . It is always possible to see a new vulnerability arises in information security softwares and if it occurs, the software should be upgraded to respond to potential vulnerabilities. If such upgrade takes more time, the software cannot keep itself safe in an operation environment. Therefore, it requires high maintenance efficiency.

Object-oriented language of Java has a strong point of easy maintenance and reuse. But procedure-oriented language C is difficult to maintain and repair.

(5) Portability

Portability refers to the possibility to operate a software in diverse environments[16]. Information security software should be possible to install and remove successfully by following installation and removal procedures. And if upgraded, still the software should be able to use the functions and data used before the upgrade[17] requiring high portability.

In consideration of software portability, C has more libraries

than Java in language process difference, compiler specification difference, library assistance and real field dependent library[8].C, for this reason, was evaluated higher than Java.

As the table shows, C has more items satisfying the requirements for information security software. Nevertheless, it does not mean C-based softwares are more appropriate. Functionality and easy maintenance are essential in information security software and here, Java is stronger than C.

II. Conclusion

In this thesis, we compared the object-oriented language, Java and procedure-oriented language C in information security software development to raise questions why only C has to be used for the development and examined related previous literatures in this context. We identified quality model characteristics such as ISO/IEC 9126, CC and information security software and presented a table 6 on it in consideration of programming language characteristics.

It was determined that the C language a language suitable for the quality characteristics of the protected software information requests via Table5. Then, as shown in Table 2, the security weakness that there are many in the software protection of information to be most in need of safety many Java also vulnerable is not good.

Made later than the C language, Java the language of the existing weaknesses of the security created by accenting.

However, it is possible to restore the code errors and serious breed of malware is easy, of security, which is most pronounced in information security software is weak. On the other hand, C language has a characteristic of high-level languages and low-level language. Processing speed is high, recovery of the code difficult than Java, it is used more.

In Java, developers learn easily, the probability of error occurs is are few, but in the case of the C language, and fall into a serious error developers that can be narrated entirely less, you must create a program to properly sometimes.

In this thesis, this point was lacking.

The reinforcement should be noted that this paper is as follows.

The authors of the present study applied ISO/IEC 9126's quality characteristics to information security softwares and compared C and Java. However, more accurate outcome can be expected if each comparison item is examined with item-specific weights

The authors believe that developing a program with multiple languages, rather than one single language, would be more effective. And the starting point of the research was the thought that in some parts object-oriented languages such as Java would be more appropriate in the situation where presently almost all part of development has been done with C.

In the table 6, Java demonstrated better performance in functionality and easy maintenance.

In the subsequent study, we plan to classify quality features according to their significance and weight and utilize experts' surveys. Broader comparison examination will be necessary by using other programming languages as well.

References

[1] Ki-Seok Bang ,Hee-Jun Yoo, Jin-Young Choi, "An Introduction to Formal Verification Methods for HW / SW System from a Programming Language Viewpoit", *Korea Information Science Society review*, Vol.21 No.1, pp. 29~39, 2003

[2] ALAIN ABRAN, RAFA E. AL-QUTAISH, JUAN J. CUADRADO-GALLEGO, "Investigation of the Metrology Concepts in ISO 9126 on Software Product Quality Evaluation", *Proceedings of the 10th WSEAS International Conference on COMPUTERS*,pp.864-872, 2006

[3] Common Criteria for Information Technology Security Evaluation(2012. September), Version 3.1 Release 4, Available:http://www.commoncriteriaportal.org/cc/

[4] DĂNUł-OCTAVIAN SIMION, "Using Java in Business Applications", *Proceedings of the 4th EUROPEAN COMPUTING CONFERENCE*,pp.218-223, 2010

[5] Ho-seock Lee, "The data type of Java programming language", *The Journal of Research Institute for Engineering & Technology*, Vol.16 No.- [1997], pp. 463~479, 1997

[6] ISO/IEC 9126-1, "Software engineering-product quality-part1:Quality", 2000

[7] James Martin, "Principles of Object-Oriented Analysis and Design", Prentice-Hall Inc., 1993

[8] Jea-gi Lee, Sang-kwon Shin, Sang-sik Nam, Kwon-chul Park, "An Analysis of Software Portability and Productivity Evaluation", *Electronics and telecommunications trends*, Vol 14, No5, pp,16-27, 1999

[9] Jongmin Lee, "Investigation in Evaluation Matrix for Security Software Product", *Proceedings of Fall of The Korean Institute of Information Scientists and Engineers*,Vol.33 No.2C, pp. 427~432, 2006

[10] Kang-su Lee, "The Security threats and mechanisms of the Java environment", *Korea Information Science Society review*, Vol. 15 No. 7, pp48-56, 1997

[11] Kwo-Jean Farn, Shu-Kuo Lin, Chi-Chun Lo, "A Study on Information Security Evaluation Testing Laboratory Planning -- Illustration of PKI", *Proceedings of the 10th WSEAS International Conference on COMPUTERS*, pp.328-33, 2006

[12] Myeong-gil Choi, Eun-joo Park, "The research about increase of Information Security software maintenance rate", *Proceedings of Symposium of The Korea Society of Management information Systems* ,Vol.2010 NO.1, pp.403~408, 2010

[13] Rechard Wiener, "Lewis pinson, An Introduction to Object-Oriented Programming and C++", Addison-Wesley, 1998

[14] Robert Sedgewick, Kevin Wayne(2013. October 23), *Introduction to Programming in Java*, [Online], Available:http://introcs.cs.princeton.edu/java/faq/c2java.html

[15] RUSLI ABDULLAH, NAGHMEH MAHMOODIAN, "A Model of Managing Knowledge for Software Maintenance As a Service (SMaaS) in a Private Cloud Computing Environment", *Recent Advances in Knowledge Engineering and Systems Science*, pp.208-212, 2013

[16] Seok-ha koh, Jeong- you Hong, "Software Project Management", Saeng Neung Press, 2007

[17] Yeo-Wong Yun, "Risk-Based Metrics for Evaluating the Quality of Information Security Products", Department of Computer Science Graduate School, Chungbuk National University, 2010.02

[18] Yong-Tai Kim, Yun-su Jung, Gil-cheol Park, "C language understanding and application", Sungjin Media Co., 2012

[19] MINISTRY OF SECURITY AND PUBLIC ADMINISTRATION, Korea Internet & Security Agency, "C Secure Guide", Vol. 3, 2012

[20] MINISTRY OF SECURITY AND PUBLIC ADMINISTRATION, Korea Internet & Security Agency, "Java Secure Guide", Vol. 3, 2012

HyungSub Kim is a master course student at the Department of Management Information Systems at Chungbuk National University. He received his bachelor degree in Science in Business Administration from Chungbuk National University. His research areas include Software Engineering and Programming language in information security and business industry.

Sanggu Byun is working at From2 Information & Communications in South Korea as a managing director. He received Ph. D at the Department of Bio Information at Kongju National University.\

SeokHa Koh is a professor of the Department of Management Information Systems at Chung-Buk National University. He received a Ph.D. and Master of Management Science form the Korea Advanced Institute of Science and Technology. His research interests include software project management, software quality, business process modeling, object-oriented software development methodology, and IS education. Professor Koh is active in research, he has published several articles which have appeared in Information and Management, International Journal of Information Management, Journal of Global Information Management, Operation Research Letters, Journal of Optimization and Applications, Telecommunication Systems, Journal of Computer Information Systems, and Industrial Management and Data Systems among others