EasyChair Preprint

№ 7161

Risk Comparative Analysis Based on SEI CERT Secure Coding Standard in C++ and Java Programming Languages

Andi Tambunan, Hermawan Setiawan and Yehezikha Beatrix

December 7, 2021

Risk Comparative Analysis Based on SEI CERT Secure Coding Standard in C++ and Java Programming Languages

Andi Parada Tambunan
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
andi.parada@student.poltekssn.ac.id

Hermawan Setiawan
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
hermawan.setiawan@poltekssn.ac.id

Yehezikha Beatrix
Crypto Software Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
yehezikha.beatrix@student.poltekssn.ac.id

***Abstract*— Writing programs with security in mind is essential in developing a secure computer system. Writing security programs can follow the standards that have been set based on previous research. In different programming languages, the standards used will be different. This standard difference is based on several factors, such as the way the program is written and the possibility of existing attacks. In this study, a comparison of program security standards in the C++ programming language and the Java programming language will be carried out. Comparisons are based on standards issued by SEI CERT. Comparisons are made by taking into account the similarities and differences in the standards used.**

Keywords—Standard, Secure Coding, Java, C++

I. INTRODUCTION

Security in computer systems has been a severe problem for decades [1]. Computer system security is essential so that work can be carried out in accordance with the objectives of the computer system. Computer system security can be started at the system development stage. System development that implements security factors in program writing can be one of the keys to computer system security. The concept of software security by implementing safe code writing is an essential part of developing secure software. Writing programming code is a preventive measure to close the vulnerabilities that exist in software development. Writing secure programming code is a concept in securing software developed based on attacks in previous research and experience. How to write secure code will differ depending on what attacks you want to avoid and address

Safe program writing can be done by referring to existing standards. Different programming languages will have different standards for writing safe programs as well. This difference is based on several factors, such as the way the program is written or the structure of the program writing, or is based on attacks that occur specifically in specific programming languages. In this study, the standard used is the standard issued by SEI CERT for the C++ language and the Java language. In this research, the author has conducted an experiment in writing safe code in the Java language based on the five rules contained in the standard issued by SEI CERT for the Java programming language. Experiments of the five rules that have been carried out on the Java language make broader research to be carried out. In this study, the overall standard of SEI CERT Java and C++ will be compared. Comparisons are made to find out the differences and similarities of the rules contained in the two standards.

Using the Java and C++ programming languages in comparing safe code writing standards is based on several things. Several things affect that the Java and C++ programming languages are object-based programming languages, and the C++ and Java programming languages are languages developed from the same base, namely the C language [2].

II. CODING STANDARDS

A. SEI CERT Oracle Coding Standard for Java [1]

This standard is a standard issued by SEI CERT to be a guide in writing safe code using the Java programming language. Writing safe code using the Java language aims to secure software that is developed based on Java, so it requires benchmarks to be a guide in seeing how likely a program is to be vulnerable. The principle that can be used in this case is the risk assessment in each rule according to the standards used. In this study, data collection is a union based on rules that have severity: high, likelihood: probable and likely, and remediation cost: high. The risk assessment table which is based on this standard is as follows:

TABLE I. SEI CERT JAVA RISK ASSESSMENT

Rule	*Number of Rules*	*Likelihood (%)*	*Severity (%)*	*Remedition Cost (%)*
00	11	81	54	18
01	3	0	0	0
02	7	71	0	14
03	13	61	0	7
04	5	20	0	0
05	13	91	23	23
06	14	64	7	28
07	10	70	0	40
08	6	83	0	0
09	12	100	0	16
10	6	66	0	0
11	5	100	0	40
12	4	100	0	50
13	15	60	6	12
14	13	92	30	46
15	8	62	87	12
16	7	100	85	0
17	5	100	40	40
49	8	62	25	25
50	27	92	51	7

Based on the existing risk assessment table, it is known that in software development using the Java programming language that follows the SEI CERT guidelines, some information is obtained. Software developers who use the Java programming language can pay more attention to each category's high percentage of rules. This attention can be done based on three rules with the highest percentage rating. Based on the likelihood risk assessment, it is necessary to pay attention to rule 09, rule 11, rule 12, rule 16, rule 17 section. Based on the severity risk assessment, paying attention to the rule 15, rule 16, rule 00 section is necessary. Based on the remediation cost risk assessment, it is required to pay attention to the risk assessment section rule 12, rule 14, rule 17, rule 11, rule 07.

B. *SEI CERT C++ Coding Standard* [3]

This standard is a standard issued by SEI CERT to guide writing safe code using the C++ programming language. Writing safe code using the C++ language aims to secure software developed based on C++ so that it requires benchmarks that serve as a guide in seeing how likely a program is to be vulnerable. In this case, the guide that can be used is the risk assessment contained in each rule by the standards used. In this study, data collection is a union based on rules that have severity: high, likelihood: probable and likely, and remediation cost: high. The risk assessment table which is based on this standard is as follows:

TABLE II. SEI CERT C++ RISK ASSESSMENT

Rule	*Number of Rules*	*Likelihood (%)*	*Severity (%)*	*Remedition Cost (%)*
01	11	27	27	18
02	14	57	35	21
03	1	0	0	0
04	9	100	66	66
05	4	75	100	25
06	8	87	87	0
07	2	50	0	0
08	13	70	14	7
09	9	77	22	33
10	7	57	0	28
49	5	6	20	20

Based on the existing risk assessment table, it is known that in software development using the C++ programming language that follows the SEI CERT guidelines, some information is obtained. Software developers who use the C++ programming language can pay more attention to the high percentage of rules in each category. This attention can be done based on three rules with the highest percentage rating. Based on the likelihood risk assessment, it is paying attention to the rule 04, rule 06, and rule 09 sections. Based on the severity risk assessment, it is necessary to pay attention to the rule 05, rule 06, and rule 04 sections. Based on the remediation cost risk assessment, it must pay attention to the rule 04 section, rule 09, and rules 10.

III. COMPARISON METHOD

After getting the programming language risk assessment data based on the SEI CERT guidelines, in this study, a comparison will be made between the Java programming language and the C++ programming language. Comparisons were made based on risk assessment using SEI CERT guidelines. This study uses a comparative method to obtain conclusions. Nazir in [4] explains that comparative research is a kind of descriptive research that wants to find answers fundamentally about cause and effect by analyzing the factors that cause the occurrence or emergence of a specific phenomenon. Comparative research is a kind of descriptive research that seeks to fundamentally answer cause and effect by analyzing the factors that cause the occurrence or emergence of a specific phenomenon. In other words, comparative research examines the differences between two or more groups in one variable

In meeting the requirements for comparisons to be made on one variable, this comparison will only take the rules that exist in both programming language standards. The comparison is made by taking the existing rule similarities between the SEI CERT standard for the Java programming language and the C++ programming language. There are five similar rules between the Java and C++ programming languages which are shown in the following table:

TABLE III. FUNCTIONAL REQUIREMENTS

Rule	Java	C++
Declarations and Initialization (DCL)	Rule 01	Rule 01
Expressions (EXP)	Rule 02	Rule 02
Input Output (FIO)	Rule 13	Rule 07
Exceptions and Error Handling (ERR)	Rule 07	Rule 08
Miscellaneous (MSC)	Rule 49	Rule 49

The comparisons made in this study are based on the risk assessment of severity: high, likelihood: probable and likely, and remediation cost: high. The comparison uses a 100% scaled percentage value. This is because there are differences in the number of rules contained in one group of rules. The comparison will pay attention to the number of rules contained in each standard. The number of rules compared is 43 in the Java programming language and 53 in the C++ programming language. The comparison of the number of rules used will be visualized on the diagram as follows:

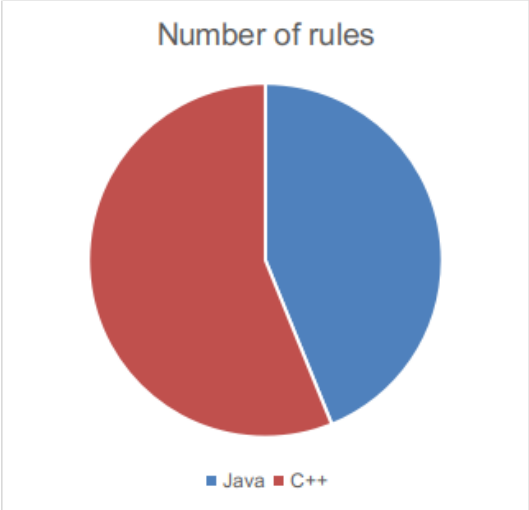

Fig. 1. Number of Rules Chart

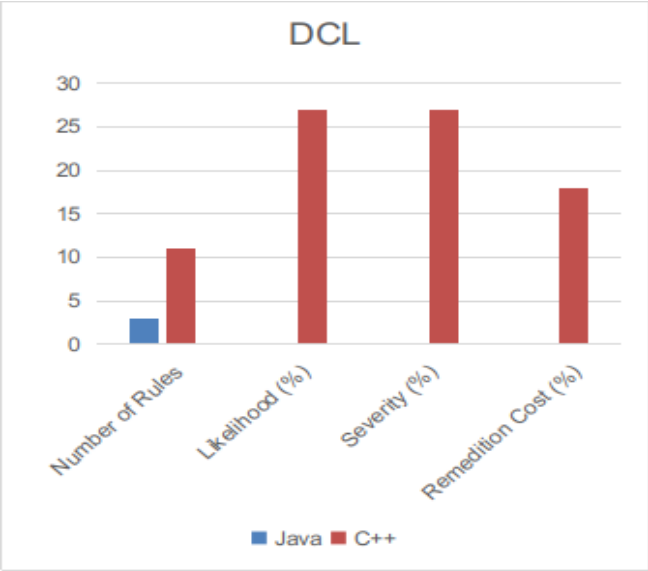

Fig. 2. DCL Comparison Chart

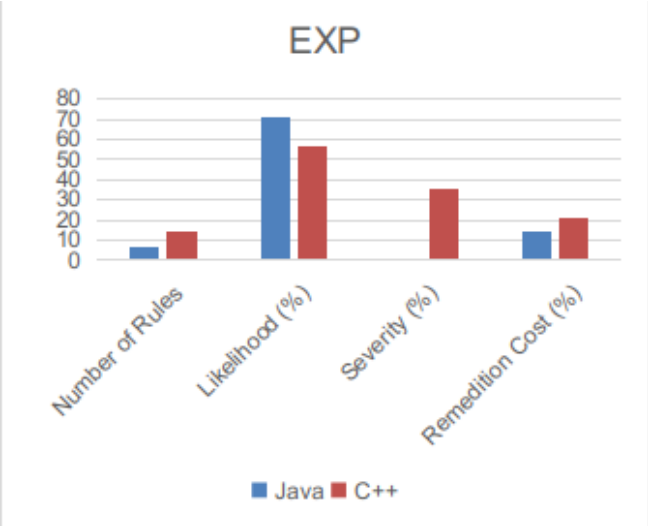

Fig. 3. EXP Comparison Chart

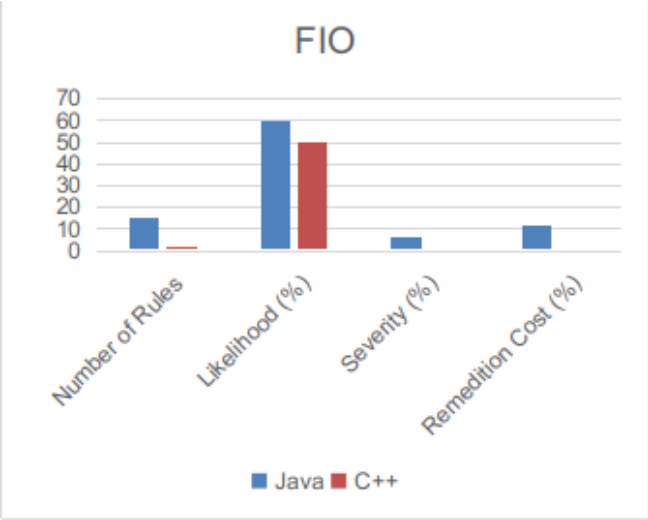

Fig. 4. FIO Comparison Chart

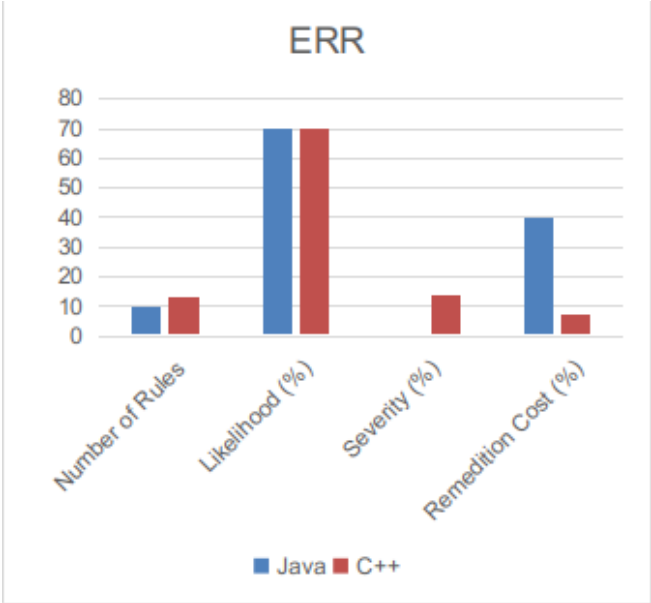

Fig. 5. ERR Comparison Chart

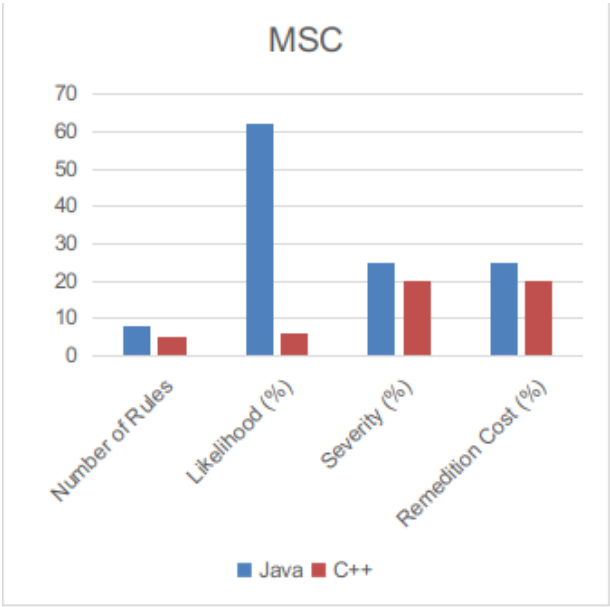

Fig. 6. MSC Comparison Chart

Based on the comparisons that have been made, the data shows that:

1. In the DCL rule, the risk of the C++ programming language is greater than that of the Java programming language.
2. In the EXP rule, the risk based on the likelihood assessment of the Java programming language is higher, while the severity and remediation cost assessment of the C++ programming language has a higher rating than the Java programming language.
3. In the FIO rule, the risk of the Java programming language is greater than the C++ programming language
4. In the ERR rule, the risk based on the severity of the C++ programming language is higher than the Java programming language. As for the assessment of remediation costs, the Java programming language has a higher risk than the C++ language. Based on likelihood, both languages have the same risk assessment.

5. In the MSC rule, the risk of the Java programming language is greater than the C++ programming language.
6. The number of FIO and MSC rules is more in the Java programming language.
7. The number of DCL, EXP, and ERR rules is more in the C++ programming language.

The results of the comparison that has been done based on the risk assessment found that many types of attacks occur in the Java and C++ programming languages. A risk assessment can indicate that the Java or C++ programming languages have their respective vulnerabilities.

IV. Conclusion

The comparison results can be concluded that software development using the Java programming language should pay more attention to FIO and MSC rules than development using the C++ programming language. Meanwhile, in software development using C++, more attention should be paid to DCL rules than software development using the C++ programming language. The comparisons made in this study focused on risk assessment based on the SEI CERT guidelines. The author suggests that comparisons can be made on other factors such as the effectiveness of secure coding on each program's attacks, comparisons between guidelines issued by different parties, and comparisons made on other programming languages such as python and javascript.

References

[1] F. Long and D. Mohindra, *The CERT Oracle : Secure Coding Standard for Java*. Addison-Wesley Professional, 2011.

[2] Aayushi Johari, "What is the difference between C, C++ and Java?," *edureka*. https://www.edureka.co/blog/difference-between-c-c-and-java.

[3] A. Ballman, "SEI CERT C++ Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems in C++," p. 528, 2016.

[4] A. S. Hamdi and E. Bahruddin, *Metode Penelitian Kuantitatif Aplikasi dalam Pendidikan*. Deepublish, 2015.