Using Program Analysis for Detecting Denial of Service (DoS) Vulnerabilities in Java Code

Shawn Rasheed (*S.Rasheed@massey.ac.nz*)

September 27, 2018

Recently, there has been an interest in understanding performance bugs in code that can be used to launch denial of service (DoS) attacks [2]. Unlike DoS attacks based on flooding an application with network requests or bugs that crash applications using vulnerabilities resulting from the violation of a programming language's semantics such as out-of-bounds access (e.g. buffer overflows), algorithmic complexity-based DoS attacks target the exhaustion of heap, stack memory or the processor by supplying inputs that cause worst-case performance behavior in a program. We present the use of program analysis to detect a class of performance bugs in Java code, and our experiences in discovering related vulnerabilities.

Some of the more well-known attacks based on algorithmic complexity vulnerabilities are regular expression DoS (*ReDoS*) that targets applications using regular expression parsers, hash functions in caching HTTP proxies, *billion laughs* that involves exponential XML entity expansion in applications that use XML parsers, and zip bombs. Performance bugs that can manifest as vulnerabilies have been studied by Crosby et al [2] and by Chang et al [1]. Some of these vulnerabilities are due to code that traverse data structures, especially collection classes in a redundant manner. In relation to this, Dietrich et al [3] have studied the characteristics of code in various programming languages that can lead to performance vulnerabilities. More specifically, composite patterns in combination with collection types and methods that traverse the structures recursively. We have built a static analysis to detect such classes and experimented with Java libraries, with results that have in turn been verified to cause real performance degrading behavior in Java libraries.

References

[1] Chang, R., Jiang, G., Ivancic, F., Sankaranarayanan, S., Shmatikov, V.: Inputs of coma: Static detection of denial-of-service vulnerabilities. In: Proceedings CSF'09. pp. 186–199. IEEE (2009)

[2] Crosby, S.A., Wallach, D.S.: Denial of service via algorithmic complexity attacks. In: Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12. pp. 3–3. SSYM'03, USENIX Association, Berkeley, CA, USA (2003), `http://dl.acm.org/citation.cfm?id=1251353.1251356`

[3] Dietrich, J., Jezek, K., Rasheed, S., Tahir, A., Potanin, A.: Evil pickles: Dos attacks based on object-graph engineering. In: ECOOP (2017)