Accepted Manuscript

Title: Software systems at risk: an empirical study of cloned vulnerabilities in practice

Author: Seulbae Kim, Heejo Lee

PII: S0167-4048(18)30094-4
DOI: https://doi.org/10.1016/j.cose.2018.02.007
Reference: COSE 1292

To appear in: *Computers & Security*

Received date: 1-10-2017
Revised date: 10-2-2018
Accepted date: 12-2-2018

Please cite this article as: Seulbae Kim, Heejo Lee, Software systems at risk: an empirical study of cloned vulnerabilities in practice, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2018.02.007.

Software systems at risk: An empirical study of cloned vulnerabilities in practice

Seulbae Kim[a], Heejo Lee[a,*]

[a]*Department of Computer Science and Engineering, Korea University, Seoul 136-713, Republic of Korea*

Seulbae Kim received the B.S. degree in Computer Science and Engineering from Korea University, Seoul Korea, in 2016. Currently, he is a M.S. candidate in Department of Computer and Radio Communications Engineering, Korea University. His research interests include software security and vulnerability analysis.

Heejo Lee is a Professor in the Department of Computer Science and Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as the CTO from 2001 to 2003. From 2000 to 2001, he was a Post-doctorate Researcher at CERIAS Purdue University. In 2010, he was a visiting professor at CyLab/CMU. Dr. Lee received his B.S., M.S., and Ph.D. degree in Computer Science and Engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an Editor of the Journal of Communications and Networks, and the International Journal of Network Management. He has been working on the consultation of the cyber security in the Philippines (2006), Uzbekistan (2007), Vietnam (2009), Myanmar (2011), Costa Rica (2013) and Cambodia (2015). He is a recipient of the ISC^2 ISLA award of community service star in 2016.

Highlights

- A scalable and accurate approach for vulnerable code clone detection is proposed.
- It relies on function-level granularity and vulnerability-preserving abstraction.
- Cloned vulnerabilities require a considerable amount of time to be patched.
- The time lag expands the possible attack surface of various software systems.

Abstract

With the growth of open source software (OSS), code clones - code fragments that are copied and pasted within or between software systems - are proliferating. Although code cloning may expedite the process of software development, it often critically affects the security of software

*Corresponding author.