

The Future of Software Security Is Instrumentation (Keynote)

Jeff Williams
Contrast Security
USA

jeff.williams@contrastsecurity.com

ABSTRACT

Software is incredibly hard to secure because it's a black box. We've spent decades trying to verify properties of software by analyzing the source code, scanning, fuzzing, pentesting, etc. only to be continually outpaced by software complexity. Instrumentation is a powerful approach for measuring security directly from within running code. In this talk, you'll learn how to use the free and open source Java Observability Toolkit (JOT) project to easily create your own powerful runtime instrumentation without coding. You can use JOT to analyze security defenses, identify complex vulnerabilities, create custom sandboxes, and enforce policy at runtime. You can even create your own IAST tests and your own RASP defenses using JOT. Ultimately, we'll show that security instrumentation empowers development and security to work together in harmony.

CCS CONCEPTS

• Security and privacy → Web application security; Software security engineering.

KEYWORDS

Observability; appsec; instrumentation; jot; IAST; RASP

ACM Reference Format:

Jeff Williams. 2020. The Future of Software Security Is Instrumentation (Keynote). In *Proceedings of the 3rd ACM SIGSOFT International Workshop on Software Security from Design to Deployment (SEAD '20)*, November 9, 2020, Virtual, USA. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/3416507.3428117>

BIOGRAPHY

Jeff Williams brings more than 20 years of security leadership experience as co-founder and Chief Technology Officer of Contrast Security. He recently authored the DZone DevSecOps, IAST, and RASP refcards and speaks frequently at conferences including JavaOne (Java Rockstar), BlackHat, QCon, RSA, OWASP, Velocity, and PivotalOne. Jeff is also a founder and major contributor to OWASP, where he served as Global Chairman for 9 years, and created the OWASP Top 10, OWASP Enterprise Security API, OWASP Application Security Verification Standard, XSS Prevention Cheat Sheet, and many more popular open source projects. Jeff has a BA from Virginia, an MA from George Mason, and a JD from Georgetown. <https://www.linkedin.com/in/planetlevel/>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SEAD '20, November 9, 2020, Virtual, USA

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-8126-0/20/11.

<https://doi.org/10.1145/3416507.3428117>