SYM-AM-16-042

PROCEEDINGS
OF THE
THIRTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Improving Security in Software Acquisition and Runtime Integration With Data Retention Specifications

Daniel Smullen, Research Assistant, Carnegie Mellon University
Travis Breaux, Assistant Professor, Carnegie Mellon University

Published April 30, 2016

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Panel 9. The Operational and Developmental Dimensions of Cybersecurity

Wednesday, May 4, 2016	
3:30 p.m. – 5:00 p.m.	**Chair: Rear Admiral David H. Lewis, USN,** Commander, Space and Naval Warfare Systems Command ***The Cybersecurity Challenge in Acquisition*** Sonia Kaestner, Adjunct Professor, McDonough School of Business, Georgetown University Craig Arndt, Professor, Defense Acquisition University Robin Dillon-Merrill, Professor, Georgetown University ***Improving Security in Software Acquisition and Runtime Integration With Data Retention Specifications*** Daniel Smullen, Research Assistant, Carnegie Mellon University Travis Breaux, Assistant Professor, Carnegie Mellon University ***Cybersecurity Figure of Merit*** CAPT Brian Erickson, USN, SPAWAR

Improving Security in Software Acquisition and Runtime Integration With Data Retention Specifications

Daniel Smullen—is a Research Assistant enrolled in the software engineering PhD program at Carnegie Mellon University. His research interests include privacy, security, software architecture, and regulatory compliance. [dsmullen@cs.cmu.edu]

Travis Breaux—is an Assistant Professor of Computer Science in the Institute for Software Research at Carnegie Mellon University (CMU). His research program searches for new methods and tools for developing correct software specifications and ensuring that software systems conform to those specifications in a transparent, reliable, and trustworthy manner. This includes compliance with privacy and security regulations, standards, and policies. Dr. Breaux is the Director of the CMU Requirements Engineering Lab and co-founder of the Requirements Engineering and Law Workshop, and he has several publications in ACM- and IEEE-sponsored journals and conference proceedings. [breaux@cs.cmu.edu]

Abstract

The Department of Defense (DoD) Risk Management Framework (RMF) for IT systems is aligned with the National Institute for Standards and Technology (NIST) guidance for federal IT architectures, including emergent mobile and cloud-based platforms. This guidance serves as a prescriptive lifecycle for IT engineers to recognize, understand, and mitigate security risks. However, integrators are left with the challenge—during acquisition and during runtime integration with external services—to reason about the actions on data inherent in their system designs that may have confidentiality risks. These risks may lead to data spills, loss of confidentiality for mission data, and/or revelations about private data related to service members and their families. Solutions are needed to assist acquisition professionals to align system data practices with the RMF and NIST guidance, as well as DoD IA directives—particularly with respect to the collection, usage, transfer, and retention of data. To provide support to this end, we extended our initial automation framework to support reasoning over data retention actions using a formal language. We propose an evaluation method for these extensions, carried out through simulations of real-world IT systems using imitation but statistically accurate synthetic data. Our language aims to address dynamically composable, multi-party systems that preserve security properties and address incipient data privacy concerns. Software developers and certification authorities can use these profiles expressed in first-order logic with an inference engine to advance the RMF, express data retention actions that promote confidentiality, and re-evaluate risk mitigation and compliance as IT systems evolve over time.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net