The ASPIRE Framework for Software Protection

Bjorn De Sutter
Universiteit Gent
Gent, Belgium
bjorn.desutter@ugent.be

Cataldo Basile
Politecnico di Torino
Torino, Italy
cataldo.basile@polito.it

Mariano Ceccato
Fondazione Bruno Kessler
Trento, Italy
ceccato@fbk.eu

Paolo Falcarin
University of East London
London, United Kingdom
falcarin@uel.ac.uk

Michael Zunke
SFNT Germany GmbH
München, Germany
michael.zunke@gemalto.com

Brecht Wyseur
Nagravision S.A.
Cheseaux-sur-Lausanne,
Switzerland
brecht.wyseur@nagra.com

Jerome d'Annoville
Gemalto S.A.
Paris, France
jerome.d-annoville@gemalto.com

ABSTRACT

In the ASPIRE research project, a software protection tool flow was designed and prototyped that targets native ARM Android code. This tool flow supports the deployment of a number of protections against man-at-the-end attacks. In this tutorial, an overview of the tool flow will be presented and attendants will participate to a hands-on demonstration. In addition, we will present an overview of the decision support systems developed in the project to facilitate the use of the protection tool flow.

Keywords

software protection tool chain; compilers; annotations; man-at-the-end attacks; decision support systems; software metrics; attack modeling

1. INTRODUCTION

ASPIRE (www.aspire-fp7.eu) stands for *Advanced Software Protection: Integration, Research, and Exploitation.* It was a European FP7 collaborative research project that brought together three market leaders in security ICT solutions. Gemalto SA is the world leader in the smart card business. SafeNet[1] is the world leader in token-based software licensing. NAGRA, the digital TV division of the Kudelski Group, provides security and multi-screen user experience solutions for the monetization of digital media. Together with four academic institutions, they developed software protections and tool support for mitigating man-at-the-end attacks on native mobile code. The academic partners were Universiteit Gent (coordinator), Politecnico di Torino, Fondazione Bruno Kessler, and University of East London. The project ran from November 2013 until October 2016.

In the project, a software protection tool flow was designed and prototyped that targets native ARM Android code. This tool flow supports the deployment of a number of protections against man-at-the-end attacks, including data and code obfuscations; a range of offline and online anti-tampering techniques such as code guards, remote attestation, and control flow tagging; instruction set virtualization; code mobility; self-debugging as an anti-debugging technique; client-server code splitting; white-box cryptography; diversity; and various forms of renewability.

Some of the techniques are applied in source-to-source transformation plug-ins; other protections are applied in the Diablo link-time binary code rewriting framework; and some techniques, such as remote attestation, involve both source-level and binary-level processing. In the ASPIRE tool flow, these protections are deployed in a manner that is compatible with "standard" compilers, such as LLVM and GCC. The convenient tool flow configuration is facilitated by means of JSON configuration files. The deployment of the protections on assets in the C software builds on software protection annotations designed in the project.

Besides the protection tool flow, the project also developed a software protection evaluation methodology based on software metrics and advanced attack modeling techniques. This methodology supports two prototype decision support systems. A first system, for full decision support, aims for automatically selecting the best combination of available protections given security requirement annotations in the source code. A second, lighter system aims at comparing selected combinations of protections and giving the user of the tool flow feedback about the weaknesses and strengths of the selected protection combinations.

2. TUTORIAL OVERVIEW

In this tutorial, an overview of the tool flow design and its APIs will be presented. This will include the deployed

[1]During the project, SafeNet was acquired by Gemalto.

SPRO'16 October 28-28 2016, Vienna, Austria

ACM ISBN 978-1-4503-4576-7/16/10.

DOI: http://dx.doi.org/10.1145/2995306.2995316

protections at both the source level and the binary code level. The source code annotations will be discussed, and attendants will participate to a hands-on demonstration of the tool flow, in which they will protect toy examples with the ASPIRE tool chain and its protection components as they will be open-sourced in the days following the tutorial. As part of the demonstration, the intermediate output of all protection plug-ins will be studied.

In addition, we will present an overview of the decision support systems we designed and implemented to facilitate the use of the protection tool flow. Also these systems will be demonstrated hands-on to the attendants, again using toy example programs.

3. INTENDED AUDIENCE

The primary intended audience of this tutorial consists of academics and industrial practitioners and researchers that want to use the upcoming, open-source ASPIRE protection framework for their research and for evaluating the added value of additional protection in combination with the existing protections developed in the ASPIRE project.

In addition, the intended audience includes all individuals interested in the major outcomes of the ASPIRE FP7 project.

The intended audience also consists of all researchers and practitioners interest in developing and discussing decision support for the protection of software against man-at-the-end attacks. In other words, all people that want to improve the usability of today's software protection tools, which are often very complex, expensive, and difficult to use well.

4. ACKNOWLEDGMENTS

The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

The design, development and prototyping demonstrated in this tutorial is the work of many contributors, incl. the authors of the paper and Alessandro Cabutto, Alessio Viticchié, Andrea Avancini, Andreas Weber, Bart Coppens, Bert Abrath, Christophe Tartary, Daniele Canavese, Elena Gómez-Martínez , Gaofeng Zhang, Jens Van den Broeck, Jeroen Van Cleemput, Leonardo Regano, Paolo Tonella, Patrice Angelini, Patrick Hachemane, Paul Gunawan Hariyanto, Rachid Ouchary, Roberto Tiella, Ronan Le Gallic, Sander Bogaert, and Shareeful Islam.