2nd International Workshop on Software Protection (SPRO 2016)

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

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

ABSTRACT

Software Protection techniques aim to defend the confidentiality and integrity of software applications that are exposed to an adversary that shares the execution host and access privileges of the application. This scenario is often denoted as protection against MATE (Man-At-The-End) attacks. This is an area of growing importance. For industry, in many cases the deployment of such techniques is crucial to ensure business continuity. Following the first SPRO workshop co-located with ICSE 2015 in Florence, Italy, this second edition aims to establish a tradition where academics and industrial experts in software protection can meet to confront the challenges in designing stronger protections and in developing better support to deploy those protections and to make them compatible with industrial software development life cycle requirements.

Keywords

man-at-the-end attacks; software protection tools; protection evaluation methods; decision support; industrial deployment; software development life cycle; obfuscation; software tamper resistance

1. BACKGROUND AND MOTIVATION

The domain of computer and communications security comprises many different scenarios in which security guarantees like confidentiality, integrity, and availability need to be provided. The SPRO workshop specifically targets the scenarios involving Man-At-The-End (MATE) attacks. In such scenarios, attackers have full control over, and white-box access to, software and its assets (such as algorithms, keys, sensitive data). In many scenarios (e.g., on mobile, open computing platforms such as Android), no custom hardware protections are available to protect the confidentiality and integrity of the assets. In such scenarios, software-based protection becomes increasingly more important. One example of a rapidly emerging scenario is Host-Card Emulation.

While research on the domain of software protection goes back several decades, there are still many challenges to overcome. Academic solutions to prevent, e.g., reverse engineering and tampering support only fuzzy security guarantees; the domain lacks widely accepted evaluation methodologies; assumed attack models are often incomplete; users have to select combinations of protections manually rather than being able to rely on decision support systems; and to a large degree the academic state-of-the-art is incompatible with industrial software development life cycle requirements.

CCS'16, October 24-28, 2016, Vienna, Austria
ACM 978-1-4503-4139-4/16/10.
http://dx.doi.org/10.1145/2976749.2990486

2. SCOPE AND OBJECTIVES

The aim of the SPRO workshop is to bring together researchers and industrial practitioners both from software protection and the wider computer and communications security community to discuss software protection techniques, evaluation methodologies, and practical aspects such as tooling. The objective is to stimulate the community working in this growing area of security, and to increase the synergies between the research areas of software protection engineering and their practical deployment. Some of the questions that we aim to address include:

- What protection techniques can be designed to protect given assets in software applications?
- Which threats need to be considered, and how can we evaluate the robustness of protected applications with respect thereto?
- How can different protection techniques be efficiently combined and what do we gain?
- What can we learn from existing use cases?
- How can protection techniques be efficiently tooled and integrated into a build process?

These are only a few of the many questions that practitioners face recurrently. The topics to be discussed during the workshop therefore include the following:

Software Protection Techniques

- Code Obfuscation, Anti-reverse engineering
- Data obfuscation, White-box Cryptography
- Binary Rewriting, Binary Instrumentation
- Anti-Debugging
- Remote Attestation
- Code Virtualization, Software Dynamic Translation
- Software Tamper Resistance, Code Guards
- Software Diversity
- Software Renewability, Mobile Code
- Software Licensing, Watermarking, Fingerprinting
- Self-modifying Code

Software Evaluation

- Evaluation Methodologies
- Malware Analysis
- Tools for static and dynamic software analysis
- Threat modeling, Petri nets, attack graphs
- Empirical studies
- Metrics

Industry aspects

- Protection technique tooling and tool chains
- Architectures and build process integration
- IDEs and tools for integration and deployment
- Validation and certification
- Best practices from industrial use cases
- Software protection on heterogeneous devices

3. PROGRAM

Authors of research papers selected for presentation and publications by the program committee will present their work in multiple papers sections. The number of sessions will depend on the number of selected papers.

3.1 KEYNOTE

Matthias Schunter (Dr.-Ing, MBA, and the Chief Technologist of the Intel Collaborative Research Institute for Secure Computing and a Principal Engineer at Intel Labs) will deliver a keynote presentation of Intel® Software Guard Extensions (Intel® SGX) as well as innovative usages for building secure systems using security-enhanced hardware.

Intel SGX is an Intel technology for application developers who are seeking to protect select code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves, which are protected areas of execution. Security critical application code can be put into an enclave by special instructions and is then hardware protected from attacks by other potentially malicious software. An enclave can therefore be shielded against attacks by untrusted application parts, by other applications, and also against attacks by a compromised operating system.

3.2 TUTORIAL

The ASPIRE project consortium (www.aspire-fp7.eu) will present a tutorial on the software protection tool chain it has developed and on its decision support tools and methodology. The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

3.3 PANEL DISCUSSION

A panel discussion is considered regarding the transfer of academic results to industry, in particular the challenges ahead to make the deployment of advanced software protection techniques compatible with software development life cycle requirements commonly found in industry. We also wish to discuss with the panel how collaboration between academics and industry can be further strengthened.

4. PROGRAM COMMITTEE

We are thankful to the members of our program committee:

- Andrea Höller -TU Graz, Austria
- Arun Lakhotia – University of Louisiana at Lafayette, USA
- Babak Yadegari – University of Arizona, USA
- Bart Coppens – Ghent University, Belgium
- Cataldo Basile – Politecnico di Torino, Italy
- Christian Collberg – University of Arizona, USA
- Christian Mönch – Conax, Norway
- Clark Thomborson – University of Auckland, New Zealand
- Frank Piessens – KU Leuven, Belgium
- Jack Davidson – University of Virginia, USA
- Jerome d'Annoville – Gemalto, France
- Johannes Kinder – Royal Holloway University of London, UK
- Karine Heydemann – Université Pierre et Marie Curie, Paris
- Mariano Ceccato – Fondazione Bruno Kessler, Italy
- Michael Franz – University of California Irvine, USA
- Mila Dalla Preda – University of Verona, Italy
- Paolo Falcarin – University of East London, UK
- Pascal Junod – HEIG-VD, Switzerland
- Roberto Giacobazzi – University of Verona, Italy
- Yuan Gu, Irdeto – USA
- Wulf Harder – QuBalt GmbH, Germany

5. CHAIRS

General Chair: **Brecht Wyseur** is a cryptography expert and security architect at Nagravision S.A., a Kudelski Group company based near Lausanne, Switzerland. The Kudelski Group is a world leader in digital security and convergent media solutions for the delivery of digital and interactive content. Brecht has worked at Nagra for the past 7 years in end-to-end key management systems for Digital TV. He obtained his PhD in Cryptography in 2009 at the KU Leuven, Belgium, with is dissertation on white-box cryptography. His research interests include cryptography and software protection; and in the past few years he has been particularly focusing on turning 'academic' techniques into real-world practice. Brecht has served in more than 20 program committees, and has organized workshops as General and Program Chair before, in particular as Program Chair of SPRO 2015.

Program Chair: **Bjorn De Sutter** is an Associate Professor in the Computer Systems Lab, Ghent University, Belgium. He obtained his PhD in Computer Science in 2002. Since Nov 2013, he coordinates (incl. technical leadership) the EU FP7 project ASPIRE (Advanced Software Protection: Integration, Research, and Exploitation). His research interests include embedded systems, compilers, software protection, code generation, and virtualization. He (co-)authored more than 70 journal and conference papers (incl. ACM TOPLAS, ACM TECS, ACM TACO, IEEE TDSC, IEEE S&P, CACM, ACM OOPSLA, ACM CCS). He has served in more than 25 program committees. He chaired the PC of the 2011 ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES). In 2008, 2009, and 2010 he chaired the Design Automation Conference (DAC) Embedded Software Tools and Design Program Subcommittee. He has also reviewed numerous papers for 17 different journals. He served as guest editor for CACM and ACM TECS.