Aspire

Advanced Software Protection: Integration, Research and Exploitation

www.aspire-fp7.eu

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

Mission of Aspire

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Motivation

Recent trends in consumer electronics increase the demand from end-users to use their mobile devices for a variety of applications that were in the past limited to secured devices such as set-top boxes, secure online license servers, and desktops.

The zoo of mobile devices makes it impossible to require additional, application-specific security hardware; all offerings need to work on top of any (open) platform the user wants to use. Scalable technologies that can guarantee secure execution of the applications are therefore desperately needed.

For that reason, traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, have challenges on mobile devices like smartphones and tablets.

Software-based software protection is therefore utterly important. It can be a maker and a breaker in domains like multi-screen mobile TV, software licensing, and credentials and sensitive data stored on mobile devices. To protect their assets, many stakeholders in mobile devices need trustworthy, easy to afford software-based security solutions, and more value for the money they spend on software security.

One category of stakeholders consists of service, software, and content providers. From their perspective, mobile devices and their users have to be considered not trustworthy because the users can engage in so-called Man-At-The-End (MATE) attacks on the software and credentials installed to access the services or content. The providers need to protect their assets against these attacks. However, current software-based protection techniques to protect those assets can often only be deployed by subject matter experts. Their deployment therefore often increases the software's time-to-market and the developer's market entry ticket price.

While Europe currently leads in hardware-based protection, urgent action is required in the domain of software-based protection to extend that leading position in digital security into the dominating market of mobile devices.

Objectives

In the ASPIRE project, three market leaders in security ICT solutions and four academic institutions join forces to protect the assets of service, software and content providers.

The core objective of ASPIRE is to develop an integrated software security framework that allows developers to add effective software protection to applications automatically. The goal is to establish trustworthy execution of software on mobile client devices that lack generic and open security hardware elements to be exploited, but that have a (persistent or occasional) network connection to a trusted entity at their disposal. With the ASPIRE solutions, we want mobile software security to become

- **trustworthy** by leveraging the available network connections and developing a layered security approach of strong protections;
- **measurable** by developing practical metrics based on validated attack and protection models;
- **cheaper** by integrating support for the protections into an industrial-strength ASPIRE Framework;
- **more valuable** by enabling shorter time-to-markets;
- **more productive** by being more widely applicable.

Whereas Europe currently leads in hardware protection, the ASPIRE project will allow it to remain competitive in the rapidly growing global mobile economy and society by allowing its mobile service providers to embrace software protection.

Technical Approach and Outcomes

1. The Aspire software protection techniques will combine five lines of defence.

A single monolithic protection technique that solves all threats is impossible to design and to engineer. Instead, a series of techniques needs to be deployed, each with a specific purpose. The approach we therefore conceive in this project is the layered software security approach, where several lines of defence are deployed under the coordination of a decision support system. We envision five principle lines of defence. (Figure 1)

These five lines of defence protect different types of assets and against different types of attacks. Most importantly, they not only protect assets in the original application, but they also cover each other's weaknesses.

In ASPIRE, we will push the state of the art regarding these five lines of defence. **Data hiding** encompasses white-box cryptography as well as data obfuscation and data flow obfuscation. **Algorithm hiding** includes control flow obfuscation, and the replacement of static binary code on a client-side device by bytecode executed in a protected virtual machine or by code delivered at run time by a trusted server. **Anti-tampering** includes code guards, anti-debugging techniques, and protections against the use of tampered external libraries. With respect to **remote attestation**, ASPIRE will exploit network capabilities to enable remote run-time code integrity verification and diagnostics. Last but not least, **renewability** will be supported to diversify application code as well as protection code over time as well as over different users and devices.

Figure 1: ASPIRE's five lines of defence

2. The Aspire project will develop an automatic software protection framework.

In order to free the application developer from the complex task of adding the software protection manually to the application, we will develop a software protection tool chain. Steered by a decision support system that helps the developer in choosing the appropriate protections, this tool chain will apply protections to the application automatically and compute the security metrics for the protected application, i.e., the estimated level of protection achieved. The tool chain will support a convenient method for developers to annotate and to identify the sensitive assets in their software, to which the security techniques will then be applied automatically once the software is debugged and ready to be validated and shipped to the customer. That way, the software protection can be cleanly separated from the logic of the software application. This approach has many advantages with regard to the separation of concerns, privacy protection, decision support, time-to-market, tuning capabilities, and exploitation.

The tool chain will incorporate both source-level and binary-code-level protection techniques to integrate all lines of defence. (Figure 2)

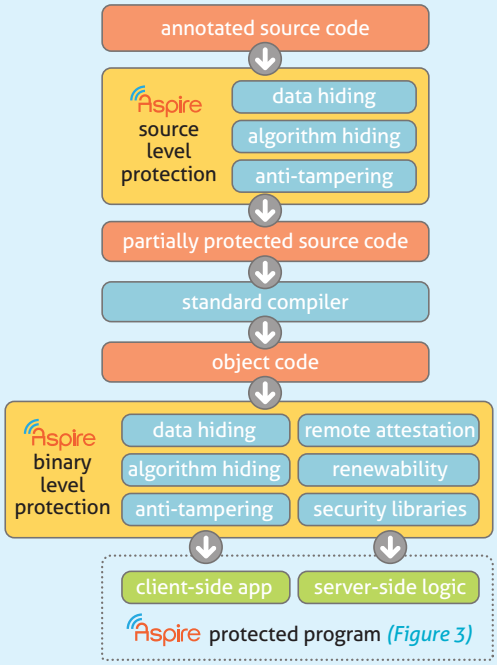

Figure 2: ASPIRE tool chain

The tool chain's output will be a protected application split into an untrusted, monitored client-side application and (trusted) server-side logic according to an ASPIRE-designed reference architecture. (Figure 3)

3. The Aspire project will develop security metrics to evaluate software protection.

ASPIRE will develop new metrics to assess software protection levels, with the ambition of making them the future gold standard of software protection.

The core of this new gold standard will be an evaluation of the extra cost (time and effort) that sophisticated attacks on a given application will incur due to the combination of applied protection techniques. To that extent, ASPIRE will develop new ways to model the interaction between attacks and protections, and conduct experiments involving human attackers to determine the protections' relation to attack time and effort.

4. The Aspire project will develop a decision support system for software protections.

Finally, ASPIRE will bring software protection to the next level by letting the framework assist the developer to decide how to best protect the assets in a particular client environment. The idea is that the programmer annotates the assets he wants to protect, and that a decision support system assists the developer in selecting the protections to apply. This system then instructs the ASPIRE tool chain to implement the protections, discharging the programmers from manually selecting the protections. The decision support system will contain expert knowledge to make such decisions. (Figure 4)

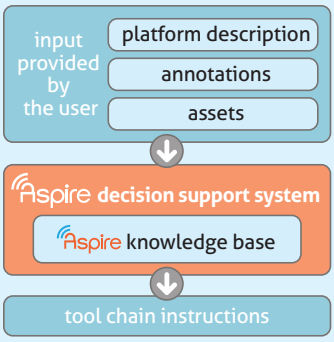

Figure 4: ASPIRE decision support system

5. Aspire will evaluate the framework on three real world use cases.

With three industrial partners, ASPIRE has access to real-life use cases, on which to evaluate and validate the whole ASPIRE Framework. These use cases are from the domains of secure DRM library integration, any end-point software licensing, and software-based security for credentials.

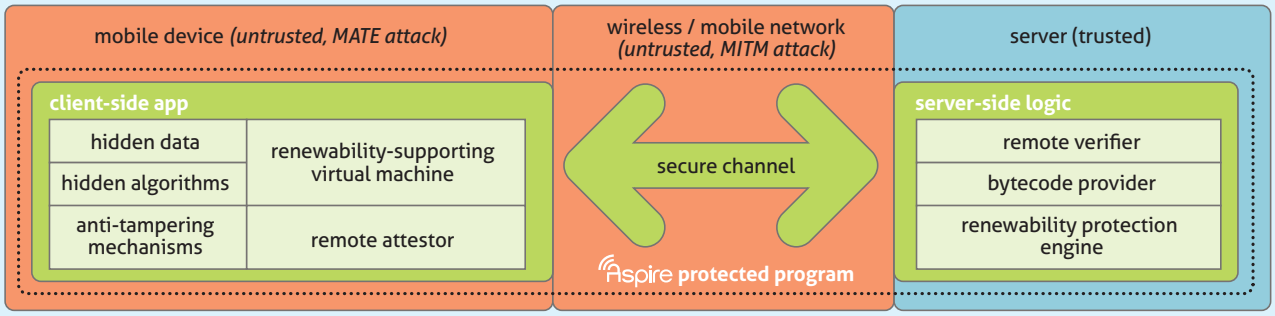

Figure 3: ASPIRE reference architecture for the protected application

Contact:

Project coordinator and technical leader: Prof. Dr. Bjorn De Sutter
Universiteit Gent • Sint-Pietersnieuwstraat 41 - 9000 Gent - Belgium
Tel.: +32 9 264 33 67 • Fax: +32 9 264 35 94
E-mail: coordinator@aspire-fp7.eu • Web: www.aspire-fp7.eu

Consortium:

ASPIRE is an FP7 collaborative research project that brings together three market leaders in security ICT solutions and four academic institutions from 6 European countries. Gemalto SA (FR) is the world leader in the smart card business. SafeNet is the world leader in token-based software licensing. Nagravision SA (CH) is the world's leading supplier of end-to-end security solutions for set-top box TV operators. Combined, these three companies understand the varying requirements of security solutions in the diverse markets that need such solutions. Ghent University, Politecnico di Torino, Fondazione Bruno Kessler and University of East London provide the necessary expertise in state-of-the-art software protection techniques and tool chains that cover offline as well as online techniques. They also provide extensive expertise in evaluation methodologies and metrics for software protection.

Universiteit Gent (Belgium, Gent)

Politecnico di Torino (Italy, Torino)

Nagravision SA (Switzerland, Cheseaux sur Lausanne)

Fondazione Bruno Kessler (Italy, Trento)

University of East London (United Kingdom, London)

SFNT Germany GmbH (Germany, Germering)

Gemalto SA (France, Meudon)

Project number: 609734
Project website: www.aspire-fp7.eu
Project start: November 1, 2013
Project duration: 3 years
Total costs: € 4.584.175
EC Contribution: € 2.949.977