CATRENE
Cluster for Application and Technology Research in Europe on NanoElectronics

PROJECT PROFILE

CA208 | Data security and privacy protection will be enhanced on the mobile internet and mobile devices [MobiTrust]

As mobile devices evolved during the past decade, the number of mobile users exploded and many hardware and software platforms appeared on the market. This also meant that security and privacy issues needed to be addressed and necessary support tools developed. Enter MobiTrust.

Let's look at the facts. The number of mobile phones globally is expected to pass the 5 billion mark by 2019, and the number of mobile internet users is expected to grow from 400 million by end 2011, to about 3.5 billion by end 2015. This increase is a result of the rapid evolution of mobile devices, such as smartphones and tablets, as well as the availability of 3G and emerging 4G LTE networks.

However, directly linked to all of this, a new challenge is arising related to the explosion of potential threats linked to the risks associated with security and protection of private and professional user-data. According to the main security players, there is a high risk that mobile devices will be greatly exposed to massive attacks, such as botnets, (malicious software like Trojan horses and viruses) within 3-5 years. This trend already started to emerge in 2011 and even Apple has been repeatedly subjected to severe attacks (with over 600,000 devices attacked in 2012 by the Flashback Trojan horse).

In addition, in-depth analysis showed that mobile-piracy activities are on the rise, increasingly managed and organised in ways similar to sophisticated legitimate businesses. In fact, mobile piracy is one of the rising stars, with attacks (like mobile botnets) against mobile devices, Cloud-infrastructure hacking and VoIP (voice over internet protocol) abuse considered the most serious threats.

Now, security solutions are emerging but a consolidated cost-effective approach is not yet in sight. With all of this as a backdrop, action in the form of better and more-effective security, privacy-protection and related tools is called for, as well as a review of the main hardware (HW) and software (SW) mobile platforms.

Embedded framework enhancing mobile security and privacy-protection

The key objective of the MobiTrust project is to develop a complete and extensive embedded framework – HW, SW mechanisms and related management, and HW/SW forensics tools – aimed at enhancing security and privacy-protection of future mobile platforms, like smartphones and tablets running on open platforms.

In particular, MobiTrust will focus on:

- ARM/Android kernel technology;
- Technical solutions that will create optimal trade-offs between 'opposing' requirements: privacy-protection and ease of use; traceability of transactions in judicial or commercial litigation settlements; and high-level security requirements in open environments, such as Android for both smartphones and tablets;
- 'Isolation' of the five main 'stakeholder' domains – user, mobile-network operator, service provider, operating system and device manufacturer – in new-generation smartphones or tablets. This will enable seamless private/professional usage of mobile devices, and ensure global and consistent privacy-protection policies;
- Ability to control from the security and privacy-keeping standpoint, platforms which rely on off-the-shelf components. This will be achieved by adding critical HW or SW elements developed in the project, and aimed at enforcing security and protection of private and professional data;
- Improvement of the certification processes of new mobile platforms from a security and privacy-protection viewpoint;
- User-friendly interfaces to enable easy interaction with mobile platforms;
- Enabling the replacement of dedicated terminals for vertical applications with off-the-shelf platforms, thereby boosting the deployment of vertical markets and related ecosystems.

In-house European expertise

The project's complexity calls for a unique combination of expertise around HW security, system-level knowledge, advanced silicon-design, mobile-security software, smartcards and other security devices and storage systems. Furthermore, the wide scope of project development far exceeds the capability of a single company, thus requiring a collaborative effort. Fortunately,

PROJECT CONTRIBUTES TO

✓ Safety and security

PARTNERS

Gemalto
Teclib'
Cassidian Cybersecurity
Cryptolog
NXP Semiconductors
Trustonic
Trusted Labs
OneSource
Commissariat à l'Energie Atomique et aux Energies Alternatives
Instituto de Telecomunicações Aveiro
Instituto Politécnico de Castelo Branco

COUNTRIES INVOLVED

France
Portugal

PROJECT LEADER

Christian Dietrich
Gemalto

mobitrust.av.it.pt

KEY PROJECT DATES

01 December 2014 - 30 November 2017

MobiTrust's European partners are also key players with extensive knowledge of market requirements and security constraints. Crucially, key players also include innovative small- and medium-sized enterprises (SMEs), needed to ensure that a complete set of trusted components fit into coherent architecture models; with a coherent security implementation at all the layers of the mobile security value chain; and which are fully consistent with most off-the shelf mobile platforms (such as iOS or Android).

Focus on security, privacy-protection and ease of use

MobiTrust could be instrumental in developing a European approach to mobile security (including privacy-protection aspects based on the European Directive on Privacy, under development), hence reducing the dependency of European public and private sectors on IT-critical components. An effective interaction with European initiatives will also help promote mobile components, resulting in a lower dependency on off-the shelf mobile products. This project could also protect critical public and private IT infrastructure from severe disruption and financial damage due to piracy and malicious hacker-intrusions.

In addition, critical business or intellectual-property (IP) data exposed to malign business-intelligence groups or agencies will be protected, thanks to dedicated privacy forensics tools. What is more, the daily life of European citizens will be affected in a positive way through end-users adopting privacy-protecting technologies developed by MobiTrust.

Standardisation and good practice

To improve end-user trust and increase market adoption of the technologies addressed, MobiTrust will synchronise its efforts to establish a secure mobile framework, with work already being done in relevant standards bodies and regulators, including Global Platform, GSM-A, 3GPP, ETSI, W3C and Fido.

Furthermore, the consortium expects to promote the widest possible adoption of privacy-enhancing technologies (PETs) and practices by the security industry, thereby proactively anticipating the requirements set by the forthcoming European Union 95/46/EC directive. MobiTrust's PET demonstrations are also expected to illustrate how easily deployable PETS are, and subsequently drive the mobile-security industry to accelerate their standardisation.

Leadership in key areas

MobiTrust is also expected to deliver business and financial benefits. It will help European industry maintain its leadership in some high-value business areas – such as mobile/wireless chipsets, Trusted Execution Environment (a secure area of the main processor), Secure Element (a tamper-resistant platform) and near-field communication (NFC) applications – by taking key positions in all business areas where security requirements are becoming a critical concern. It will, through synergy, also help build an open SW industry. What is more, the results achieved in MobiTrust will be a key enablers for new products and services. In particular, the capabilities of a worldwide trust-module for mobile and other embedded platforms will enable the industrial project-partners to provide solutions for new market segments and application domains, thus creating a strong, market-leading position for trustworthy devices. And driving all of this is a healthy mobile-security market, which is expected to grow from US$1.5 billion in 2014, to US$5.75 billion by 2019, at an estimated compound annual growth rate (CAGR) of 30.7%, and benefiting the project consortium and other European suppliers alike.

CATRENE Office
44 rue Cambronne
F-75015 Paris - France
Tel. +33 1 40 64 45 60
Fax +33 1 40 64 45 89
Email catrene@catrene.org
www.catrene.org

CATRENE (E! 4140), the EUREKA Cluster for Application and Technology Research in Europe on NanoElectronics, will bring about technological leadership for a competitive European information and communications technology industry.

CATRENE focuses on delivering nano-/microelectronic solutions that respond to the needs of society at large, improving the economic prosperity of Europe and reinforcing the ability of its industry to be at the forefront of the global competition.