CATRENE
Cluster for Application and Technology Research in Europe on NanoElectronics

PROJECT RESULTS

CA208 | Comprehensive toolset provides mobile devices and mobile internet with enhanced security and privacy protection [MobiTrust]

The next explosion of mobile devices (smartphones and tablets) and mobile-internet users will only make long-standing concerns over privacy, fraud, and security even more urgent. MobiTrust addressed these issues by developing a total framework containing elements that provide current and future mobile platforms with the necessary protection.

The last decade has seen smartphones and tablets became the preferred repository of personal and professional data. We are also witnessing a significant increase in mobile devices (smartphones and tablets) and mobile devices connected to the internet, a trend expected to continue. According to Statista, a statistics portal, mobile internet usage is affecting the daily life of smartphone and tablet users, enabling consumers to access and share information while on the go. There are signs of a promising future for mobile internet usage as global mobile-data traffic is projected to increase nearly sevenfold between 2016 and 2021. According to January 2018 data, the global mobile population stood at 3.7 billion unique users. And as of February 2017, mobile devices accounted for 49.7% of web page views worldwide. This means that mobile devices will be even more exposed to massive attacks (such as botnets, Trojan horses and viruses), as well as illegitimate piracy activities which are increasingly managed and organised in ways similar to sophisticated, legitimate businesses.

Crucially, this raises key technological and societal issues:

- Privacy protection: More and more users are concerned that they lack proper control over their personal data or assets in mobile environments. Little effort has been made to define guidelines;
- Mobile fraud: The global shift of interest from hacker and pirate communities and organisations is putting a higher risk on some high value-added businesses;
- Protection of vulnerable users: The mobile ecosystem is increasingly facing the same problems as the classical internet world, with the development of illegal or criminal activities such as violence and pornography. Little protection in the mobile environment is available for minors and other vulnerable users;
- New trust models and spaces for mobility: Trusted service managers are just emerging, but consumers lack the confidence to perform high-value transactions because these trusted third-parties do not address the mobility, simplicity and confidence requirements which end-users are seeking. Certification or official marks, such as labels, will help.

Building comprehensive mobile defences

Addressing these key issues, the main goal of MobiTrust was to develop a complete framework—including HW/SW (hardware/software) embedded bricks; remote credential lifecycle management tools; judiciary-proof HW/SW forensics tools—aimed at enhancing the security and privacy-protection of future mobile platforms (including smartphones and tablets) with a focus on ARM/Android kernel technology, but also covering more closed environments, such as Apple's iOS.

MobiTrust delivered complete mobile platforms which were based on commercially available off-the-shelf ones in which the project results are integrated in several scenarios. Importantly, existing certification methodology frameworks were extended accordingly to handle such concepts as privacy, compositional security and forensics, which were introduced in the project. These platforms were deployed as demonstrators aimed at validating their security and privacy-protecting nature, as well as their simplicity of use and ease of integration.

MobiTrust demonstrated more than eight security and privacy-protection scenarios, including:

- A fully integrated, real-life simulation of a firefighting-unit's command & control centre deploying technology bricks from the MobiTrust security framework. This scenario also demonstrated the use of private mobile radio (PMR) over LTE (long term evolution), a 4G mobile communications standard;
- BYOD (bring your own device, referring to company policy of permitting employees to bring personally owned devices to their workplace, and to use those devices for work;
- Using a mobile device as a PC to improve end-user mobility and security;
- Performing the necessary security checks to perform a qualified signature on documents stored a mobile device;
- New hardware to improve security and performance of mobile transactions;
- An open source device-management system and an improved secure mobile operating system.

PROJECT CONTRIBUTES TO

✓ Safety and security
✓ Digital lifestyle
✓ More than Moore

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

http://mobitrust.av.it.pt/

KEY PROJECT DATES

01 December 2014 - 30 November 2017

How MobiTrust will impact Europe

MobiTrust is expected to deliver key benefits in the following areas:

- European approach: MobiTrust participated in developing European mobile-technology bricks that led to several product and solution launches. It is commonly understood that mobile devices' high-end features are mostly developed outside Europe. Significantly, this European project has demonstrated how major elements of security technology can be designed and produced by European companies. The project will also be key to the development of a European approach to mobile security (including privacy-maintenance aspects). And through strong interaction with European initiatives, MobiTrust will also help promote the use of mobile components, thus reducing dependence on off-the shelf mobile products;
- Fraud: With the pervasiveness of IP-based networks for mobile internet, the risk of massive fraud is threatening the economy. This project will help protect critical public and private IT infrastructure from severe financial damage due to piracy and malicious hacker intrusions;
- Protecting critical information: A heavily computerised world is creating new opportunities for the exposure of critical data to malign business-intelligence groups or agencies. MobiTrust will help protect all critical business or intellectual property rights (IPR) of European public or private organisations from widespread disclosure of sensitive information, thanks to a dedicated privacy-maintaining forensics tool-chain;
- European leadership: This project will help Europe maintain its leadership in some high-value business areas—such as mobile/wireless chipsets; multiple secure elements, form factors and enclaves; optical storage and near-field communication (NFC) applications. It will also help European industry take a sound position in all business areas where security requirements are becoming a key concern. This includes building a sound, open SW industry, which will create new products and services. And the worldwide trust module for mobile and other embedded platforms will enable industrial project partners to provide solutions for new market segments and application domains. This, in turn, creates strong market-leadership in trustworthy devices.
- Guarding privacy: Entirely under the control of major European companies, critical technologies developed in MobiTrust should be adopted in an easier way by end-users, considering strict requirements made in the various reference architecture models to protect their privacy. These privacy requirements will be assessed by trusted European certification agencies. In addition, wide adoption of privacy-enhancing practices (PETs) by the security industry is anticipated. Among the expected outcomes of MobiTrust, demonstrating that PETs are in fact easily deployable to improve the experience of end-users, will act as an eye-opener in the mobile security industry, and will create some momentum around the standardisation of PETs.

Finally, a parting thought. With illegal and criminal activities, such as violence and pornography, impeded by MobiTrust, hopefully minors and other vulnerable mobile-users will also feel safer and more protected.

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.