

European Specialists Team Up to Define Security Standards for Next-Generation Mobile Devices

Five partners from industry and academia have joined forces in a European research project, SEPIA (Secure Embedded Platform with advanced Process Isolation and Anonymity capabilities), to define security standards for next-generation mobile devices including high-end cell phones and tablet devices.

As financial services, such as banking and payment, become increasingly accessed from mobile devices, it becomes increasingly critical to provide secure, certified cell-phone platforms to ensure such sensitive applications are efficiently protected from security threats. The SEPIA research project brings together ARM, Brightsight, Giesecke & Devrient (G&D) and Infineon Technologies, and is coordinated by Graz University of Technology (Austria). The project is co-financed by the European Union's Seventh Framework Programme (FP7).

Mobile devices play an ever more critical role in our personal and professional lives today. They are increasingly used to access banking, location-based services, and social networking sites. Protecting people's security, privacy, and identity on these devices is therefore a mounting concern.

At present, however, there is no common security level across cell phone platforms and the technology varies widely. Set up to run for three years, the SEPIA research project aims to address this by developing new security enhancements and certification methodologies for mobile device platforms.

Herbert Reul, chair of the European Parliament committee on Industry, Research and Energy, confirms: "SEPIA addresses an ever more pressing security problem that is receiving increased attention on the European level, especially regarding mobile applications like eBanking." For the consumer, SEPIA should allow execution of security-critical applications such as electronic banking, location-based services, and social networking on cell phones, while ensuring that personal and confidential data such as usernames, passwords, location, and banking and payment details are stored and processed within a separate trusted environment.

The expected outcome of SEPIA is that these security-critical applications will run in a protected and isolated environment, alongside other services such as games and software downloads, without risk of being affected by viruses, Trojans, or other malicious software.

From a technical viewpoint, the SEPIA project will be based on a mobile platform combining ARM® TrustZone® technology, which creates a protected area in advanced systems-on-chip, and the high-security MobiCore© operating system developed by G&D. The interplay between TrustZone and MobiCore ensures that if online services incorporate security-sensitive functions - for instance payment

European Specialists Team Up to Define Security Standards for Next-Gener

Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

transactions - it is not possible for malware on the phone to manipulate username and password entries via the keypad or data output on the display.

Drawing on its expertise in hardware-based security, Infineon is contributing next-generation technology to allow secure storage of user credentials and passwords, thus adding further security to the new mobile platform.

BrightSight will develop novel and cost-effective certification methods that allow mobile platforms to be certified incrementally, thus achieving short time-to-market cycles.

The Institute for Applied Information Processing and Communications (IAIK) of Graz University of Technology is responsible for the scientific aspects of the project, including techniques to preserve anonymity and the development of security mechanisms for future cell phone processors.

The SEPIA project receives funding from the European Union's FP7 scheme. It supports Europe's foothold as a leading innovator in the sphere of mobile technology. SEPIA will make it easier to establish cross-platform, common security concepts and SEPIA's new approach to security evaluation will reduce time-to-market.

Source URL (retrieved on 05/06/2015 - 4:29am):

<http://www.wirelessdesignmag.com/news/2010/11/european-specialists-team-define-security-standards-next-generation-mobile-devices>