Domenico Argenziano

Tutor: Alessandro Cilardo

co-Tutor: Clemente Galdi

XXX Cycle - II year presentation

TEE-based Secure Storage and cryptographic hardware acceleration

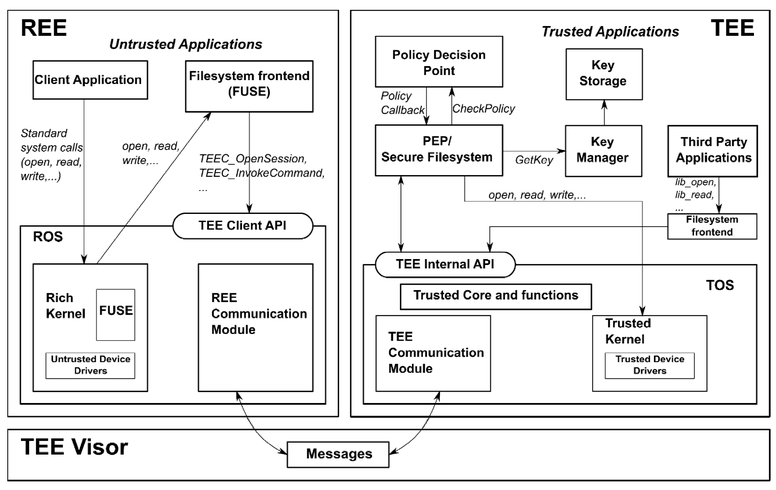
Today's spread of computational capabilities over a wide variety of different devices and the high degree of their interconnection, in order to exchange data and cooperate in data processing, pose a serious challenge with respect to data protection and access control within distributed application scenarios. Moreover, during the last years cloud computing has emerged as an important paradigm shift for a large class of applications and security is a major concern in the cloud setting, since user data is moved to an external server and processed at a remote site. The increasing demand for privacy and security against illicit data manipulation can be partially met using traditional cryptographic techniques (symmetric and asymmetric encryption, digital signature, etc…) but more advanced security primitives and protocols are needed for secure computing in distributed scenarios: users can encrypt their data and send them to the cloud, but, beside storing such data, remote nodes cannot perform computations on them. Moreover, encrypting data still poses the problem of cryptographic keys management and protection.
Therefore, my research activity has focused on a recent technology for data protection and workload isolation, *Trusted Execution Environment*, a virtualization infrastructure for Trusted Computing on embedded systems. On the other side, I studied hardware acceleration facilities and software for both standard and advanced cryptographic operations, based on a SIMD/GPU approach.

Secure Storage on Trusted Execution Environments

The concept of *Trusted Computing* implies that a computing system will always behave in the expected way and such behaviour is enforced by software and hardware facilities. Such a system is then considered *trusted*, in the sense that it can be relied upon in order to enforce a specified security policy.

A trusted system have to fulfill various properties (*Isolated Execution, Secure Storage, Remote Attestation, etc…), but* virtualization technologies have emerged as the glue which can bring together such building blocks. *GlobalPlatform* consortium has issued a set of standard specifications for a secure virtualization infrastructure, specially intended for mobile and embedded applications. Such platform puts side by side a *Trusted Execution Environment (TEE)* and a *Rich Execution Environment (REE)*. The TEE hosts a trusted OS and trusted applications which provide access to privileged resources.

Based on such framework, we designed a fine-grained secure file system running on the TrustOS, that features:

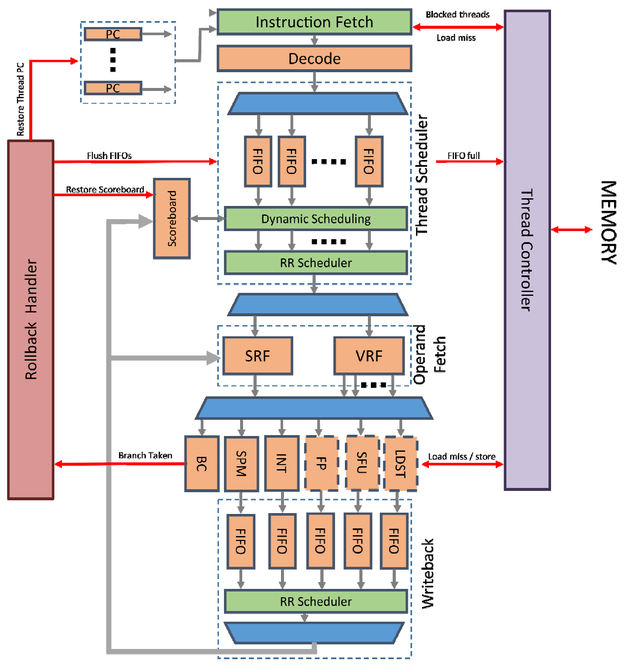


- Data confidentiality, integrity and authenticity
- Per file encryption with key stored along with the file
- Arbitrary access policies based on RBAC model
- Roles assigned to trusted applications, not users/owners
- Each role is assigned a keypair, kept by KeyStore, that encrypts file keys

No particular constraint is put on access control policies, and we support both geospatial and temporal conditions, which are of special interest on mobile devices. A full working prototype has been developed based on an open-source TEE emulation framework: *Open-TEE*.

GP-GPU acceleration for cryptographic operations

The increasing demand for information security in current distributed scenarios has led to an increasing adoption of cryptograhic operations which, in turn, implies an increased computational overhead. Besides, new advanced protocols have been proposed in the scientific literature among which, of particular interest in the cloud setting are those that allow computations to be carried out directly on encrypted data. One of the main class of such protocols is that of*Secure Function Evaluation* (or *Secure Multi-Party Computation*), which allows two or more parties to compute a public function supplying their own private inputs without disclosing any information about such inputs besides what can be deduced from the function result.



Despite their interesting properties, such techniques incur in a high computational complexity. Noticeble research effort has been put in devising faster algorithms, but they can surely benefit from advanced hardware architectures.
In the last years, GPU and especially *General Purpose GPU* (*GPU*) have merged as successful solution for high-throughput vectorial computing, combining two approaches: *Single Instruction Multiple Data (SIMD)* and multi-threading.

My research work has focused on designing cryptographic acceleration facilies based on the vectorial/GPU, to be integrated in the overall work of my research group for a highly customizable GP-GPU, *Nu+*. I worked on support for standard primitives (RSA, AES) as well as more advanced protocols, such as *Garbled Circuits*, invented by Yao, for Secure Function Evaluation.

Progetto di Ricerca e Sviluppo
Interventi di potenziamento di Sistema e di Filiera della R&S di cui al D.D. n. 52 del 26/06/2014
(Filiera WISCH, Work Into Shaping Campanias Home) - CUP n. B68C14000270007
Soggetto Proponente : CONSORZIO TECNEVA TECNologie EVolutive per sistemi Avionici

Future work:

- Analysis of the most relevant performance bottlenecks
- Full support for arbitrary spatio-temporal policies
- Asynchronous policy evaluation mechanism
- Arbitrary file encryption cipher
- Directory encryption
- Performance improvement through caching
- Extending and improving cryptographic support inside *Nu+* GPU: full support for RSA, AES, DES, Galois multiplication and hashing operations
- Latency oriented optimizations
- Support for *Secure Function Evaluation*: hardware facilities, languages for description, synthesis and compiling tools, libraries.