Architectures for Split Execution of Copyright-Protected Applications

January 18, 2008

1 Context

Typically, applications are executed in a single-host, single-processor architecture. Parallelization environment and GRID architectures provide the means to parallelize the execution of applications in multi-host, single or multiprocessor architectures. The usual goal of splitting applications across multiple hosts and processors is only one: performance.

Another possible goal for splitting the execution of an application by more than one device is for ensuring copyright rights. Applications can be split in two parts, one for running in normal execution environments and another for running in a secure, tamperproof device (for instance, a smartcard). The first one can be freely copied to other hosts; the second one cannot be copied. This way, to execute the application each user/host must have an instance of the application that cannot be copied, which ensures copyright protection.

Spliting an application for executing in this novel architecture requires a different approach for deciding which instructions are interpreted in each device. The principal splitting criteria is to make the code running inside protected devices hard to guess by attackers. Nevertheless, other criteria are also relevant: shared memory accesses, performance, etc.

2 Goals

The goal of this work is to define policies and mechanisms (e.g. compilers) for splitting and application in at least two parts, one for executing in general-purpose running environments (e.g. Linux) and another for executing inside a protected, tamperproof device (e.g. smartcard). The split application should be as efficient as possible without compromising the secrecy of the protected part. The attacker model must assume that attackers may challenge the protected device with specially crafted inputs in order to learn the operation of the protected part.

3 Supervisor

André Zúquete (UA Assistant professor, IEETA researcher, IT collaborator)

4 Research Unit

IEETA (Instituto de Engenharia Electrónica e Telemática de Aveiro)