

3 Publishable Summary

3.1 A summary description of the project objectives

Virtualised service platforms and cloud computing hold great promise for delivery of large applications in e-Government. However, to date, the fundamental shared-resource nature of virtualisation technologies has raised legitimate security concerns for Government and other organisations with duties to protect confidential data.

The PASSIVE project proposes an improved model of security for such virtualised systems to ensure that:

- adequate separation of concerns (e.g. policing, judiciary) can be achieved even in large scale deployments,
- threats from co-hosted operating systems are detected and dealt with;
- public trust in application providers is maintained even in a hosting environment where the underlying infrastructure is highly dynamic.

To achieve these aims, the consortium proposes:

- A policy-based Security architecture, to allow security provisions to be easily specified, and efficiently addressed.
- Fully virtualised resource access, with fine-grained control over device access, running on an ultra-lightweight Virtual Machine Manager.
- A lightweight, dynamic system for authentication of hosts and applications in a virtualised environment.

In particular PASSIVE project aims to:

1. Investigate the unique virtualisation requirements for e-Government applications.
2. Identify e-Government security requirements and propose solutions to security/privacy challenges that are hindering the adoption of virtualisation technologies by European governments and associated agencies.
3. Develop a framework for the secure deployment of virtualisation technology in e-Government scenarios, in consultation with an appropriately constituted advisory board.
4. Enhance the state-of-the-art in virtualisation security by designing and creating a prototype implementation of a policy-based hypervisor security management tool.

With a proven ability to reduce costs, energy consumption and greenhouse gas emissions through improved resource efficiency, it is not surprising that IT professionals have rapidly embraced virtualisation technology. Unfortunately, it is precisely the characteristic of shared access to physical resources which allows virtualisation to solve many complex IT problems that also makes it a foundation for potent new security threats. PASSIVE aims to counteract these new threats by providing virtualisation systems, with enhanced security features.

3.2 Description of the performed work since beginning of the project – Main results achieved so far

The main output of WP2 is:

- Review of the state-of-the-art relevant for security protection and management in a virtualised environment.
- Specification of 6 uses cases for sensitive information processing in virtualised environments, down-selected to 3 for use in the remainder of the project.
- Derivation of 17 key requirements for the security of virtualised environments, through analysis of state-of-the-art, the 6 use cases and legal and regulatory documents and standards from the EU and elsewhere.
- Identification of 32 research challenges for security protection and management in a virtualised environment.
- Involve in all the aforementioned tasks the Advisory Board.

The main output of WP3 is:

- Initial definition of security and access policy
- Initial architecture of PASSIVE system that include aspects of
 - Authentication and identity
 - Resource control
 - Dynamic security monitoring and enforcement
 - Metering and usage accounting
- The aforementioned output is designed to be coherent, feasible to implement and validate
- Involve in all the aforementioned tasks the Advisory Board.

The main output of WP4 is:

- Setup of the experimentation environment
- Setup of the resource virtualisation subsystem
- Based on the initial architecture involved partners commence working on the PASSIVE modules, their implementation and support tools, namely:
 - Policy engine and authentication module
 - Monitoring, metering, filtering and accounting modules
 - Compliance procedures and tools

The main output of WP5 is rather limited since it started on M11 and is limited to initial setting and discussion of the validation tools, in particular:

- Investigation on the usability of ETICS system not only to perform software integration and building, but also to execute automatic deployment testing in order to speed up the final deployment of the whole PASSIVE framework in the validation testbed
- Provision of an initial test-bed design
- Execution of first deployment test of NOVA in the local testbed

The main output of WP6 is:

- Web/Internet presence and dissemination of PASSIVE and the results within.
- Organisation of PASSIVE workshop.
- Participation in EC activities and clusters.

- Initial plan for standardisation and exploitation of PASSIVE.

3.3 Potential impact

The envisioned impacts of the PASSIVE project are in improved European industrial competitiveness in markets of trustworthy ICT, in particular:

- Facilitating economic conditions for wide take-up of results.
- Offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.
- Adequate support to users to make informed decisions on the trustworthiness of ICT.
- Increased trust in the use of ICT by EU citizens and businesses.
- Increased societal acceptance of ICT through understanding of legal and societal consequences.

The partners within PASSIVE gain invaluable competitive advantage by participating in this project. Virtualised computing represents the future of large-scale systems deployment, and is a foundation technology for other rising technologies such as cloud computing, large-scale distributed testbeds and grids. However, the possibility of “leakage” of sensitive data from one VM to another when both are on the same physical hardware has hindered the adoption of this technology in applications dealing with large quantities of sensitive data.

Improving the security mechanisms used on virtualised systems will lower the barriers to adoption of this technology in markets such as banking, fund management and government IT (both in citizen-facing and internal applications). The market potential for virtual computing in government IT alone makes a compelling case for any measure that will aid its adoption in this sphere.

The software implementation from the PASSIVE proposal will be used as the basis of a prototype VM security system by the consortium. This experimental prototype will serve as a proof-of-concept for incorporating the PASSIVE features into mainstream VM systems. The possibility of licensing one or more of the technologies employed in PASSIVE will be pursued in the course of WP6.

The PASSIVE project will provide the partners involved in the production and marketing of VM software with a competitive advantage in terms of the unique product features that PASSIVE will bring to their product line.

Hosting and infrastructure suppliers will gain advantages by offering the PASSIVE-equipped VM systems to sensitive government and financial customers. Similarly, organisations involved in supply of applications to these customers will be able to provide more competitive service delivery terms through greater use of virtualisation than is currently acceptable.

3.4 Project ID card


Acronym	PASSIVE
Title of the Project	Policy-Assessed system-level Security of Sensitive Information processing in Virtualised Environments
Proposal Number	ICT-2009.1.4-257644
Contract Number	257644
Starting date – End date	01/06/2010 – 31/05/2012
Duration (in months)	24
Total Budget	3,580,140.00 €
Total Manpower (PM)	351
Community Financial Contribution	2,349,982.00 €
Project Officer	Dirk Van-Rooy
Project Manager	Charalabos Skianis
Technical Manager	Panagiotis Rizomiliotis
Logo	
website	http://ict-passive.eu

Figure 1: PASSIVE Project ID card