PASSIVE

Policy based Security for the eGov Cloud

PoFI 2011, Pisa, Italy.

Eamonn Power

PASSIVE Clouds, Costs and Data

- Governments want to
  - Safely handle sensitive data
  - Reduce CAPEX & OPEX in doing so
    - Use Cloud Services to help
- So why not ? …

PASSIVE

Constraints

- The Law
  - EU Directives are pretty clear about how sensitive data should be handled
  - Member states have implemented legislation in the same spirit
- eDiscovery
  - Handling sensitive data is important
  - Providing reasonable access and proof of history to support law enforcement is also key
- Dishonest Minority
  - Individuals who seek to make personal gain from sensitive data outside of the frame in which it was provided
    - Government-gathered personal information
    - Medical databases, etc.

PASSIVE

EU Directives of Note

- EU 95/46 - Personal Data Treatment and Circulation
- EU 2002/58 - personal data and privacy (clarification of EU 95/46)
- EU 2006/24 - data retention directive

PASSIVE

Current Cloud Issues

- So what's wrong with Cloud Services
  - Guarantees are minimal
    - Security policies are generally for informational purposes
    - Costs of providing guarantees outweigh benefit of doing business

PASSIVE Current Cloud Issues (2)

- The risk of malicious or compromised hosts
- Hosts outside of premises may not be to your standard
- Current best practice (for sensitive data)
  - Don’t store data on general cloud instances
  - If you do, encrypt it before it leaves the premises
  - Don’t process it outside of your premises
- Negates most of the possible benefit of cloud?

Current Cloud Issues (3)

- Large Scale Compromise of Cloud Provider
  - Homogeneous Resources (many instances of the same machine specification)
- Risks
  - Compromise a singe virtual machine (through document low-level device driver attacks)
  - Compromise neighbouring virtual machines (by gaining access to the hypervisor)
  - Try to spread to other hypervisor hosts in the provider cluster
- Costly in Time and Reputation
  - (which for a service provider = €€€)

PASSIVE

What is PASSIVE trying to solve?

PASSIVE

Overview

- 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.

PASSIVE

Partners

- University of Aegean (PM)
- ANECT
- ATOS
- Engineering
- Thales Research and Technology UK
- Technical University of Dresden
- University of Malaga
- Waterford Institute of Technology - TSSG

Atos Origin

ANECT

TECHNISCHE UNIVERSITÄT DRESDEN

uma
UNIVERSIDAD DE MÁLAGA

THALES

Waterford Institute of Technology

TSSG

PASSIVE

Goals

- 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

PASSIVE

How?

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

PASSIVE

Current Work

- Completed analysis phase
- 1st phase of Design complete
- 1st phase of Implementation in Progress

PASSIVE

Thank You

- Questions?
  - http://ict-passive.eu
- Eamonn Power (Dissemination Lead – WP6)
  - epower@tssg.org