Application Whitelists in Virtual Organisations

Cornelius Namiluko, Jun Ho Huh, John Lyle
and Andrew Martin

Oxford University Computing Laboratory
Parks Road, Oxford OX1 3QD, UK
Email: firstname.lastname@comlab.ox.ac.uk

Agenda

Introduction

Consensus View of a Trusted VO

Missing Components

New Components and Implementation Strategies

Conclusions & Future Work

Application Whitelists in VO

Introduction

- Whitelist - a repository of ‘known good’ software configurations
- Assumed in many trusted architectures during attestation to determine trustworthiness of a platform configuration
- Details on how this whitelist would be managed are rarely considered
- Conflicts will arise across multiple administrative domains
  - administrators respond differently to vulnerabilities
  - use different versions of software or apply different patches
- This may adversely affect service availability

Application Whitelists in VO

An Emergent Consensus View

- Grid Job Submission – users submit job to run on participant
- Integrity-based Access Control – preventing violation of user’s security requirements
- Attestation tokens – identity information and the public half of a TPM key whose private half sealed to the TPM
- Central Management – manage and distribute tokens

Application Whitelists in VO

An Emergent Consensus View

- Property-based Attestation – to simplify trust decisions based on platform configurations
- Job Delegation - allows recipient of a grid job to pass it on to other trustworthy nodes
- Minimised TCB – system trustworthiness depends on the size and complexity of the TCB
- Job Isolation - sandboxing, hardware or software virtualisation to isolate jobs

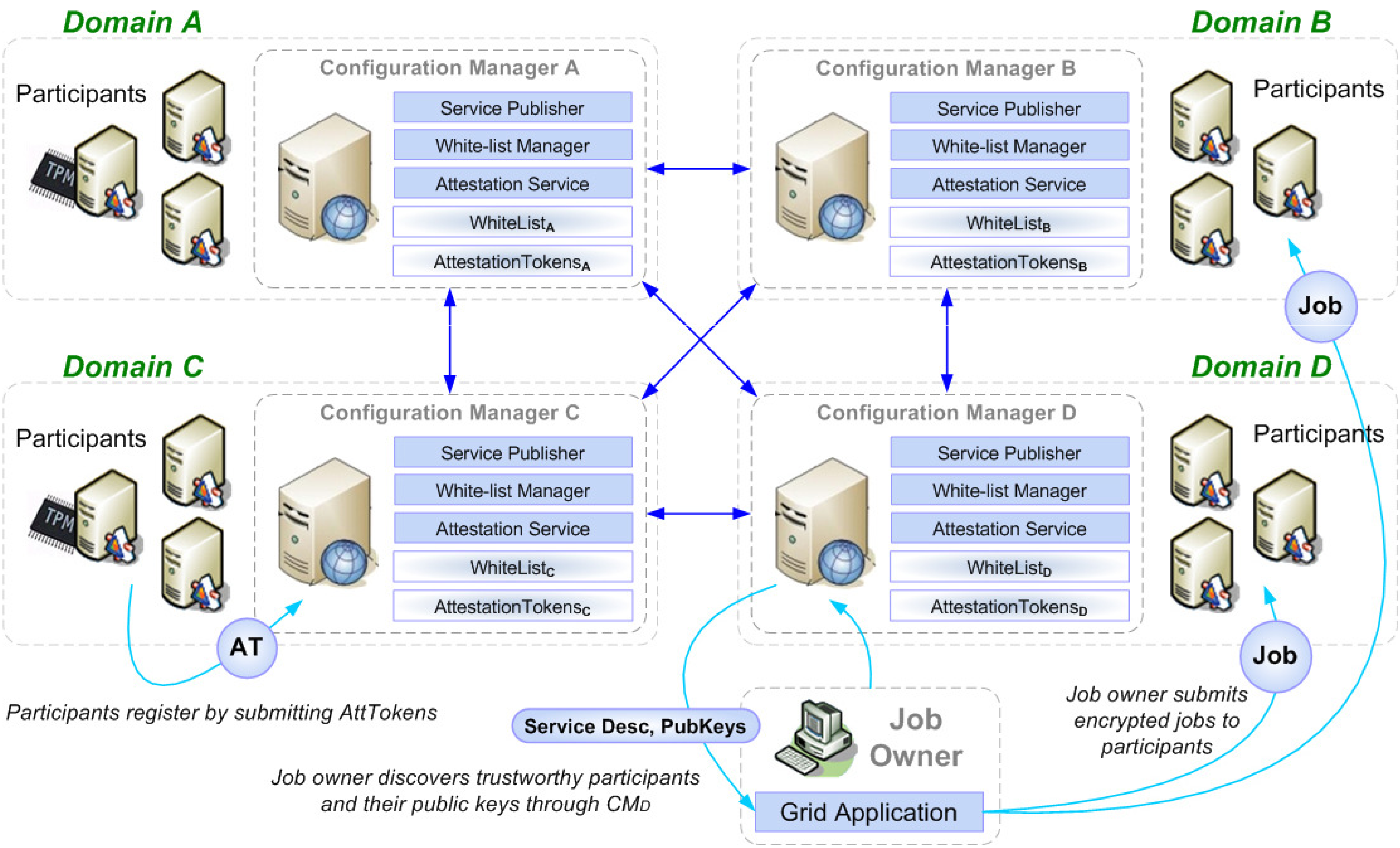
Application Whitelists in VO

Missing Components: Whitelist and Policy Management

- Users cannot manage whitelists - require constant modification and update
- Passing to trusted third party - no insight on how such a third party would operate
- TCG ‘s aggregation service face challenge for system spanning multiple administrative domains
  - institutions will have different selection of software
  - administrators only know software in their domain
  - some administrators will be more diligent in updating and revoking software patches than others
- No jobs can be distributed or integrity reporting is abandoned altogether

Application Whitelists in VO

Abstract View of a VO



Domain A

Participants

Configuration Manager A

Service Publisher

White-list Manager

Attestation Service

WhiteList$_A$

AttestationTokens$_A$

Domain B

Configuration Manager B

Service Publisher

White-list Manager

Attestation Service

WhiteList$_B$

AttestationTokens$_B$

Participants

Domain C

Participants

Configuration Manager C

Service Publisher

White-list Manager

Attestation Service

WhiteList$_C$

AttestationTokens$_C$

Domain D

Configuration Manager D

Service Publisher

White-list Manager

Attestation Service

WhiteList$_D$

AttestationTokens$_D$

Participants

Job

Job

AT

Service Desc, PubKeys

Job Owner

Grid Application

Participants register by submitting AttTokens

Job owner discovers trustworthy participants and their public keys through CM$_D$

Job owner submits encrypted jobs to participants

Application Whitelists in VO

New Components and Implementation Strategies

- Introducing the Configuration Manager (CM)
  - one per-domain
  - participants establish domain membership through CM
  - composed of attestation service, service publisher and whitelist manager
  - adds validation information to RIM – including tests carried out, vulnerability scans and results
- Inter-domain Communication using well established standards where possible to update other CMs about changes to domain. Message include:
  - RIM
  - Validation Information
  - Policy recommendation
  - grace period and meta-data

Application Whitelists in VO

New Components and Implementation Strategies

- Whitelist Manager
  - communicate to service publisher to indicate changes or updates required on the participants
  - whitelist entry updates
  - receives updates from other domains
  - validates change requests with domain administrator

Application Whitelists in VO

Conclusions & Future Work

- We argue that whitelist management should mandate inter-domain communication
- Propose a set of new components which would interoperable sharing of whitelist entries
- future trusted grid system can use our analysis to avoid potential availability and interoperability problems
- How application whitelisting can help solve the problem of untrustworthy job submitters?

Application Whitelists in VO

Acknowledgements

This work is partly funded by studentships from QinetiQ and the EPSRC, as well as a Rhodes Scholarship. We thank David Wallom, Steven Young and Matteo Turilli from Oxford eResearch Centre.

Application Whitelists in VO

Thank you for your attention!

Questions