

Dynamic Security Perimeters for Virtual Collaborative Networks

Authors: Ivan Djordjevic
Theo Dimitrakos

Presented by: Ivan Djordjevic

iTrust Workshop, Imperial College, London, 17th September 2003.

Motivation

Virtual Organizations:

- Distributed
- Inter-organizational
- On-demand
- Dynamic
- Scalable
- Secure

Current Issues:

- Scalability of communication
- Limited functionality of IOIS
- Security
 - Inflexibility of firewalls
 - Centralised Management
 - Policy
- Interoperability

Ongoing Efforts

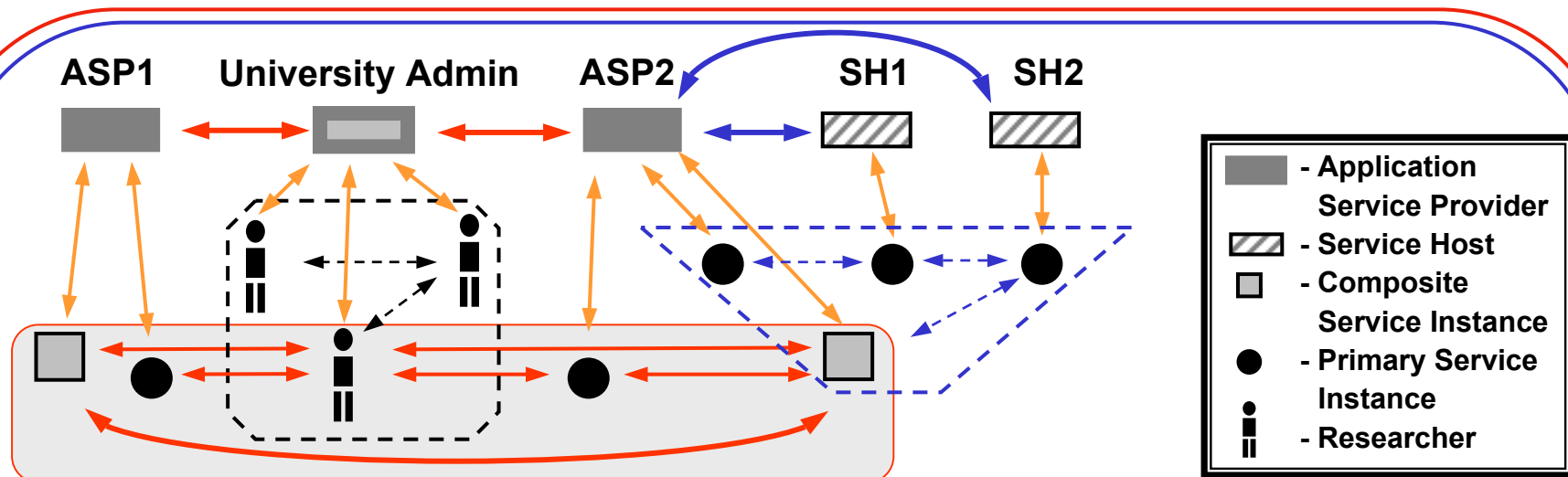
Architecture:

- IPv6 (IPSec) / Mobile IP
- VPN enhancements
- Peer-to-Peer (Groove, JXTA)
- Web Services
- Grid Services

Security:

- Distributed firewall (AT&T)
- Distributed/shared IDS
- Role-based policy
- WS security stack
- Grid security (e.g. Globus CAS)

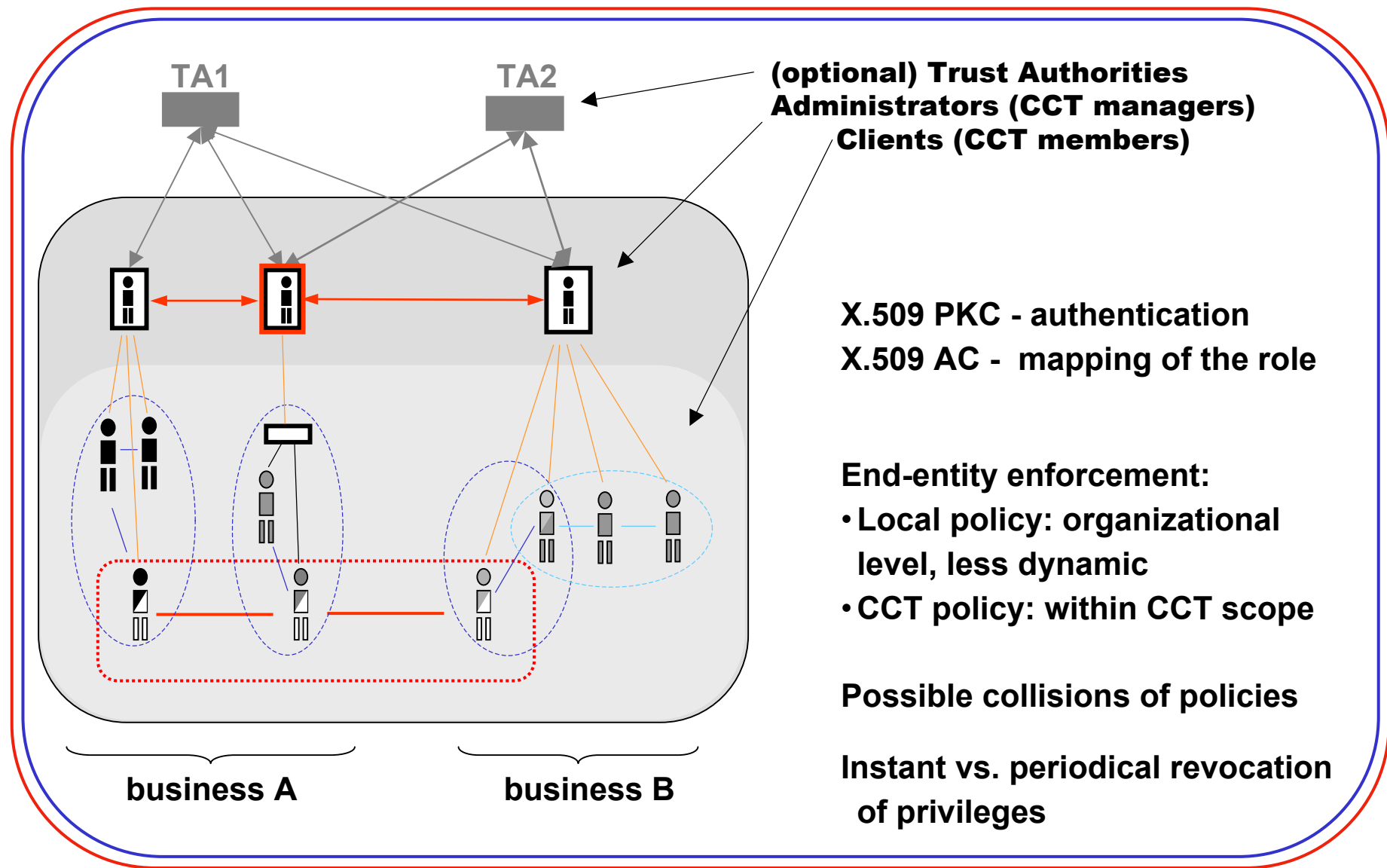
Illustrative Example



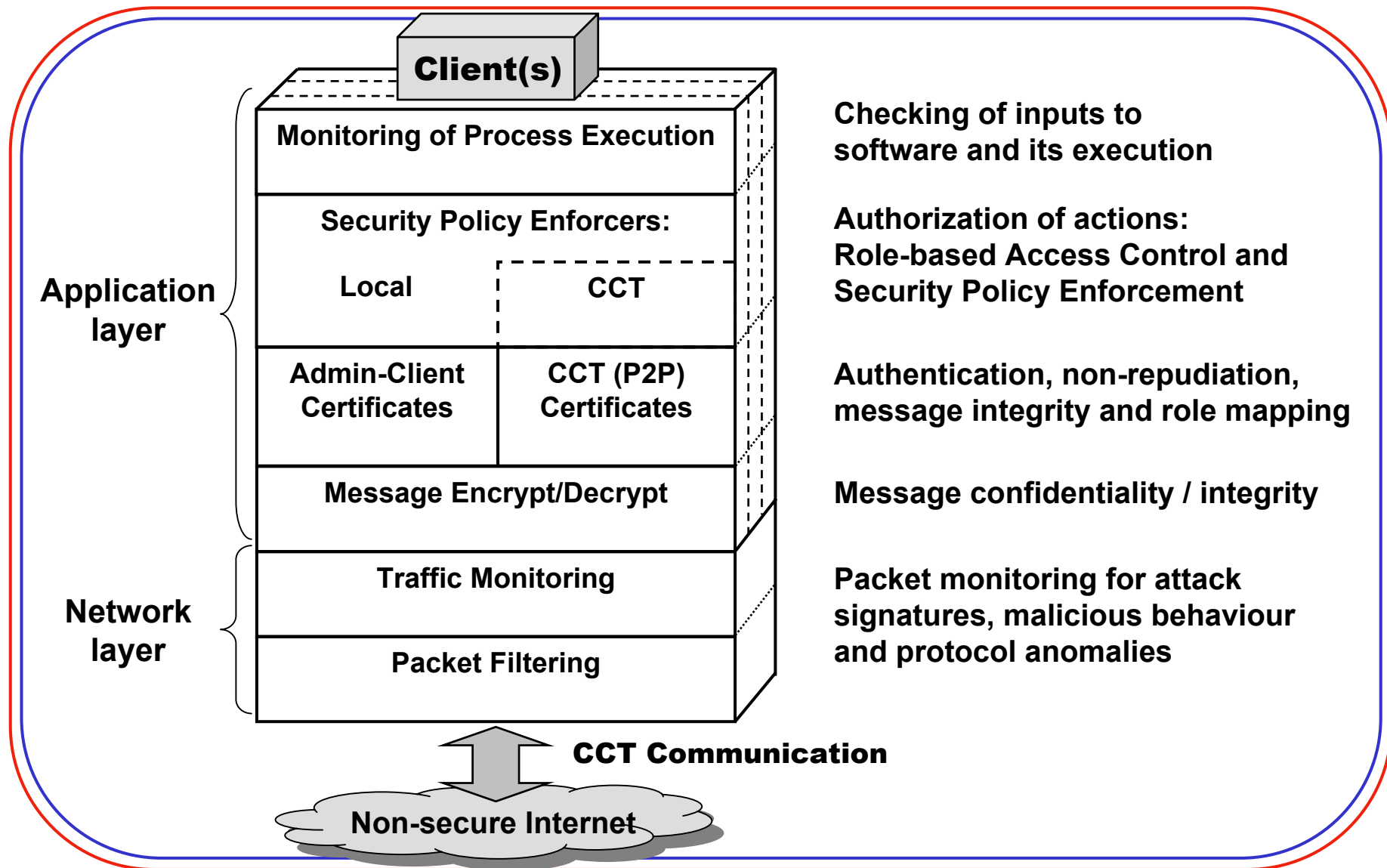
Features and Issues

- Resources are with different institutions → Different policies may apply
 - Same resources in several VOs → Different roles, (potentially) conflicting policies
 - No centralized administration of VO → Devolved policy management & distributed enforcement
 - Dynamic introduction of resources in VO → Real-time trust establishment on P2P basis
- Protection of resources & interactions within VO. Protection of VO from outsiders
 Complex trust relationships – within VO, and also for inter-organizational interactions

Architecture of Closed Collaboration Teams (CCT)



End-Entity Security Enforcement



Role of Trust

Motivation - To achieve additional flexibility and protection of the CCT perimeters

Approach - Assessing confidence in a network entity on the basis of evidence accumulated by observing behaviour in different CCTs.

Several Contexts of Trust:

- Performance execution of the CCT interactions
 - Opinions about CCT members (P2P interactions)
 - Opinions about Administrators (client-admin interactions)
 - Opinions about Administrators (P2P & 2nd-hand evidence from CCT)
 - Opinion about local clients (client-admin & 2nd-hand evidence from CCT)
- maintained by **clients**
- maintained by **administrators**
- Reputation of clients / administrators maintained by “reputation service” TTPs
(in some applications administrators may act as reputation services for their local clients)

Summary

Architecture for enabling scalable and secure VOs

- **Developed:**
 - Protocol for group management (simulation test-bed)
 - Architecture for end-entity enforcement of dynamic security perimeters
- **Considerations:**
 - Membership revocation scheme
 - Granularity of roles affects the complexity

Aspect of Trust – work in progress

- Used in several contexts
- Both Centralized and Distributed approach
- Considerations: calculating trust values / trust formation: deriving trust values from evidence, reputation & recommendations

Longer-term goal: Development of an operational implementation as a (Semantic) Web Development prototype or in the context of a or a larger Enterprise Computing infrastructure

Thank You!

Contact: ivan.djordjevic@elec.qmul.ac.uk
theo.dimitrakos@rl.ac.uk

Appendix:

Joining CCT: Management & P2P Messages

