FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

Document title:	Security Work Plan		
Document number:	f-in-00084	**Document source:**	(see authors below)
Document status:	Input	**Date of this status:**	2002/12/20
Change history:			
2002/12/20	Submission of document to the FAB		

Stefan Poslad
stefan.poslad@elec.qmul.ac.uk

Monique Calisti
monique.calisti@epfl.ch

Problem Statement:

Application services and users have a basic requirement for security services to protect them. Conventional security safeguards that protect identified system assets are manually and statically configured to act against preconceived threats. For example, multiple parties such as providers and users most often use agreed, pre-configured security safeguards such as public key authentication and encryption-based secure channels to protect confidentiality and to verify identity. Safeguards range from the use of encryption-based confidentiality and authentication to the use of trust to minimize service disruption and to the uses of policies, legislation and anonymity to protect personal privacy. Safeguards may be under the control of management processes, the infrastructure, and they may be switched on and off under application control.

The manner in which one or more security safeguards may be represented, associated with security threats, advertised, agreed (bootstrapped?) and invoked, has not been standardized within the agent community. These must be agreed 'out of band' in order to achieve end-to-end security. Agent security has been represented at a number of different 'layers' in the ACL communication stack ranging from the use of secure transport protocols, new transport envelope fields, "content ontologies", new security ACL fields, new speech acts; to new security interaction protocols and security policies that incorporate privacy and trust. A key issue is whether or not a single core security representation, versus a more abstract representation that can map to multiple security representations, should be specified.

Further problems arise when statically configured safeguards that support both agent and non-agent services, such as supply-chains, nomadic users and service orchestration environments, operate across multiple heterogeneous domains. Different domains may support multiple security services and there may be no clear choice for an agreed single configuration for security services that is suitable for heterogeneous domains and applications. In addition, security may be breached because of the overwhelming choice, complexity and lack of an explicit model of the security configuration. For example, mutual authentication techniques that require manual checking of the provider by the client are often bypassed in practice because they are too complex to configure at the client end and because it is convenient to rely on the reputation of the provider and the security capabilities of a trusted 3rd party for authentication. Finally, dynamic relationships between assets, safeguards and threats often need to be supported in practice. For example, if the safeguards are configured to meet preconceived threats, these may change – threats may need to be monitored and reassessed and the safeguards may need to be reconfigured.

Agents can use shared explicit representations of security and mediation, coupled to autonomous reactive and proactive behaviors to help automate, facilitate, enhance and support dynamic security configurations. FIPA should address and lead the area of multi-domain multi-agent security. The benefits to FIPA for standardizing in this area are that

such specifications are crucial if multi-agents systems will be used to support service access within open multi-domain service infrastructures.

Objective:

There are three main objectives to this work-plan:

- To review existing agent and non-agent security abstractions and assess how different security representations and profiles of sets of safeguards can be used to support different security requirements. These security safeguards may range from conventional single-point control mechanisms such as access control to sophisticated distributed multi-point mechanisms such as delegated authentication, voting and reputation mechanisms.
- To develop a FIPA-based abstract security specification for MAMD (Multi-Agent Multi-Domain) systems that explicitly describes security that can be mapped to configurable levels of security safeguards and to one or more agent security representations.
- To reify the abstract FIPA security model to form an agent-based security service for deployment in one or more application domains such as eBanking or eTourism.

Technology:

The technological input for this work-plan will come from the review of security services from the W3C; IETF; from published multi-agent security papers and from the FIPA security white-paper published as [1] that includes an analysis of obsolete FIPA specifications that concerned security and outlined an abstract security model.

Specifications generated:

The specifications that are generated by this work plan are:

- An abstract security service specification for MAMD (Multi-Agent Multi-Domain) systems;
- An agent security service to support querying the available security and dyanmically setting security configurations.

If at all possible, revisions to existing FIPA specifications will be avoided, For example, security could be specified in terms of one or more optional security ontologies and services.

Plan for Work and Milestones:

The plan is for an 18 month activity that uses the following milestones:

- 2003/03 Start review of existing agent and non-agent security models for heterogeneous open service environments;
- 2003/07 Completion of review of existing open system security models and requirement specification for abstract security model. Begin work on developing a preliminary specification of an abstract FIPA Security Service Specification.
- 2003/11 Preliminary version of Abstract FIPA Security Service Specification completed.
- 2004/03 Experimental version of Abstract FIPA Security Service Specification completed. Begin work on reification of the abstract model to form a FIPA Security service
- 2004/07 Completion of preliminary version of the FIPA Security Service.
- 2004/11 Completion of an experimental version of the FIPA Security Service.

The project plan will be reviewed and revised, if and when necessary.

Dependencies:

- [FIPA00001] FIPA Abstract Architecture Specification
- [FIPA00023] FIPA Agent Management Specification

Support:

- Stefan Poslad (QMUL)
- Juan Jim Tan (QMUL)
- Leonid Titkov (QMUL)
- Monique Calisti (Whitestein)
- Margaret Lyell (Mitre)
- Nicolas Lhuillier (Motorola)
- Sergi Robles (UAB)

FAB Comments: