A Multi-Agent System for Automatically Resolving Network Interoperability Problems

Joseph A. Giampapa
garof+@cs.cmu.edu

Katia Sycara
katia+@cs.cmu.edu

Austin Fath
jatf+@cs.cmu.edu

Aaron Steinfeld
astein+@cs.cmu.edu

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Daniel Siewiorek
dps+@cs.cmu.edu

Abstract

In this paper we present the Thistle *multi-agent system Help Desk application for helping an end user solve network interoperability problems on their own.*[1]

1. Introduction

As software applications become more distributed and interoperable with other network-based applications and services, it becomes more and more critical for the end user to become knowledgeable of technical data communications issues, such as how they are connected to the services and the speed and reliability of that connection, as well as policy-oriented considerations, such as whether or not they should have access to services given the way in which they are connected to the network or if they acquired the proper credentials. An examination of 528 trouble ticket cases from a 2.5 year period from the Carnegie Mellon University (CMU) School of Computer Science (SCS) confirmed that 50% of end user problems — not including requests for phone numbers and outliers such as trouble tickets used as memos — were related to obtaining the necessary user rights in order to perform a task. Many sources of the denied security access were due to conflicts with security policies, improper authentication, and the end user not understanding their *network security state* — the security rights and data protection mechanisms that derive from the means in which one is connected to the network — and what rights and protection mechanisms were required by CMU SCS security policies in order for them to obtain their desired network services [3]. The findings confirmed the hypothesis that the disconnect between the end users' awareness of their network security state and the administrative security policies was pronounced and spread across a wide range of security topics. Hence, our development of *Thistle*, a prototypical multi-agent system (MAS) Help Desk application, that seeks to enhance end user abilities to diagnose and remedy network interoperability problems, particularly those problems that stem from the enforcement of network security policies.

2. Thistle MAS Help Desk Application

Figure 1 illustrates the principal components of the Thistle MAS Help Desk application, the: *Thistle Task Agent*, *Thistle Interface Agent*, *DAML-S Matchmaker*, *Maude Evaluator*, *System Capability Repository*, *Local Policy Agent*, and a variety of wrapped network applications and diagnostic tools. These components reside on the end user's computer, which is intended for use in either a multi-zoned enterprise network or on a computer that is used for connecting to an enterprise network from a remote location, such as a home desktop or laptop.

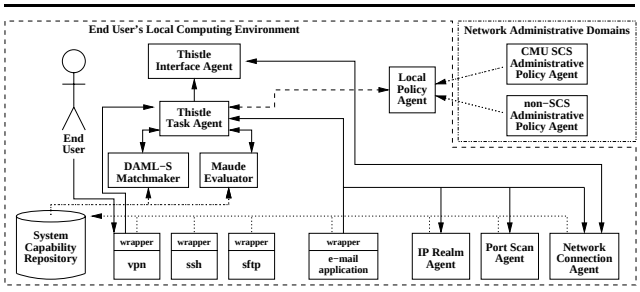

Figure 1. Thistle MAS Help Desk Application

1 This work was funded by ONR grant N00014-02-1-0499 and in part by the DAML program under AFRL contract F30602-00-2-0592.

AAMAS'04, July 19-23, 2004, New York, New York, USA.

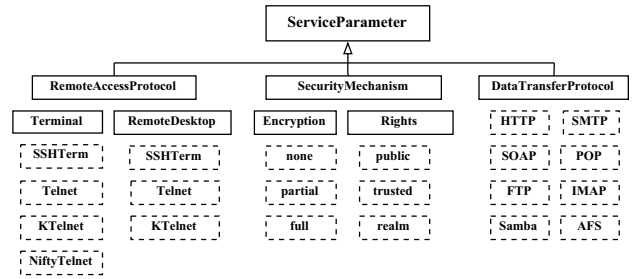

Figure 2. DAML-S Security Ontology

Figure 3. The Thistle Interface Agent

The only agent that needs to be active at all times is the Thistle Task Agent, which determines which agents and wrappers need to be invoked and queried. At startup, the Task Agent queries agents such as the IP Realm Agent to determine the administrative realm of which the user is a part. It also queries the Local Policy Agent for a description of the policies in effect for the administrative realms that the user could possibly join. When the user invokes a wrapped application, such as an e-mail client, the Task Agent receives a semantic description of the application's remote service dependencies and security requirements from the wrapper. The Task Agent then sends the descriptions of the application's requirements, and the policies for the administrative realms that the user will join in order to access their services, to the Maude Evaluator for evaluation.

The Maude Evaluator is an instance of a Maude [2] interpreter that was wrapped in the RETSINA Communicator so that other agents can communicate with it. Maude is a logical re-write rule inference engine that we programmed to reason about whether or not combinations of programs and network tools would satisfy specific administrative security policies. Its reasoning is based on modifications to the DAML-S security ontology described in [1], which are shown in Figure 2. Failing such verifications, Maude can be re-queried by the Task Agent to suggest alternative combinations of programs that the end user can invoke to achieve his goal. The Maude Evaluator was programmed to return an unlimited number of combinations of programs and tools, but no combination can involve more than 10 components, per our own estimation of a reasonable solution.

The Thistle Interface Agent, shown in Figure 3, is the only interface that the end user has to the Thistle Help Desk application. It appears on the user's desktop when the Task Agent determines that the user might not have sufficient security or connectivity to perform a task, and suggests to the user the current applications that the user might invoke to remedy the problem.

3. Evaluation and Discussions

The Thistle MAS Help Desk application has been tested extensively with different policies both on the CMU SCS campus network and on simulations of multi-zone networks. Firewalls were also used to selectively block specific application ports to simulate diverse actions of network policy enforcement. With the monitoring agents configured to check system state every 10 seconds, Thistle was able to detect changes in the configuration of network, application, and policy state in no more than 20 seconds of the events occurring. This is orders of magnitude shorter than the times required by the remote user or Help Desk personnel to perform similar debugging operations [3].

Thistle demonstrates abilities at proactive monitoring, problem avoidance, and proof-of-concept capabilities for collecting parameters and symptoms automatically through its monitoring agents. It can autonomously suggest to the end user what to do, and semi-autonomously act on the end user's behalf, thus empowering him with the ability to solve problems without the direct assistance of Help Desk staff. This is novel, and we are not aware of any work at this level of reasoning, complexity and execution. We believe that the modular and formal rule-based nature of the Thistle MAS Help Desk architecture allows for its extension to other tasks, such as providing assistance with file transfer and remote printing, or with helping a user configure complex parameters that impact quality of service and respond to network latency.

References

[1] G. Denker, L. Kagal, T. Finin, M. Paolucci, and K. Sycara. Security for DAML web services: Annotation and matchmaking. In *ISWC 2003*, 20–23 October 2003.

[2] The Maude system. `http://maude.cs.uiuc.edu/`.

[3] A. M. Steinfeld, R. Sanghi, J. A. Giampapa, D. Siewiorek, and K. Sycara. An examination of remote access help desk cases. Technical Report CMU-CS-03-190, Computer Science Department, Carnegie Mellon University, September 2003.

AAMAS'04, July 19-23, 2004, New York, New York, USA.