Demonstration of the Secure Wireless Agent Testbed (SWAT)

Gustave Anderson Andrew Burnheimer Vincent Cicirello David Dorsey
Saturnino Garcia Moshe Kam Joseph Kopena Kris Malfettone Andy Mroczkowski
Gaurav Naik Max Peysakhov William Regli Joshua Shaffer Evan Sultanik
Kenneth Tsang Leonardo Urbano Kyle Usbeck Jacob Warren

Department of Computer Science & Department of Electrical and Computer Engineering
College of Engineering
Drexel University
3141 Chestnut Street
Philadelphia, PA 19104

Abstract

We will demonstrate the Secure Wireless Agent Testbed (SWAT), a unique facility developed at Drexel University to study integration, networking and information assurance for next-generation wireless mobile agent systems. SWAT is an implemented system that fully integrates: (1) mobile agents, (2) wireless ad hoc multi-hop networks, and (3) security. The demonstration will show the functionality of a number of decentralized agent-based applications, including applications for authentication, collaboration, messaging, and remote sensor monitoring. The demonstration will take place on a live mobile ad hoc network consisting of approximately a dozen nodes (PDAs, tablet PCs, and laptops) and hundreds of mobile software agents.

The Secure Wireless Agent Testbed

The Secure Wireless Agent Testbed (SWAT) is a unique facility developed at Drexel University to study integration, networking and information assurance for next-generation wireless mobile agent systems [8]. It is the only implemented system that fully integrates: 1) mobile agents, 2) wireless ad hoc multi-hop networks, and 3) security.

In the SWAT, mobile agents manage keys, assess network traffic patterns, analyze host behaviors, revoke access rights for suspicious agents, users, or hosts, adaptively reroute traffic at the network layer to improve the information integrity of the system, and provide the implementation framework for decentralized user applications, including authentication, collaboration, messaging, and remote sensor monitoring. SWAT is able to support industrial-strength, fielded, mobile agent architectures that include, but are not limited to, the Extendable Mobile Agent Architecture (EMAA) from Lockheed Martin's Advanced Technology Laboratories [7] and Cougaar [5]. The agent-based applications of the SWAT currently include: a group display GUI that shows a list of all members in a user group, and tracks the creation, joining, and leaving of groups; a secure, multi-group whiteboard application that enables users to communicate notes and map annotations within their groups; an application that employs agents to carry secure audio communications similar to two-way radios; agent-based network and resource monitoring; among others.

SWAT enables agents to reason about and react to network dynamics [4]. It is implemented for ad hoc network environments, in which hosts have the ability to dynamically identify routes and forward packets between hosts that are not within direct wireless range of each other and which may require multi-hop ad hoc routes. In the SWAT framework, agents are able to modify the network state, make decisions about their itineraries based on network topology, and adapt their communication modalities to avoid network congestion. SWAT is not limited to any particular ad hoc routing protocol. Currently, there are few wireless ad hoc routing algorithms that have been deployed live; most have only been simulated. For this reason, SWAT has created the Topology-based Secure Ad hoc Routing (TSAR) Protocol which is an authenticated and encrypted, proactive routing protocol that supports secure multi-hop routes [3].

SWAT addresses the need for a mobile agent information assurance framework that includes cryptography and the ability for different groups of agents to generate secure communications channels within the overall agent community. Agents must be able to reason about security groups

and communications in a manner that allows them to adapt to a dynamic security environment in which hosts may become compromised, networks may get attacked, and malicious agents may need to be identified and contained. SWAT provides agents with secure multi-layer, agent-to-agent group communication on resource-constrained devices. The security framework uses a combination of symmetric and public-key cryptography to support encrypted communication at both the network and the agent application layers, including support for secure group communication. To accomplish this, established security technologies have been integrated into SWAT, including tools for key generation and management, secure group communication, user revocation through the use of a security mediator, and en/decryption of traffic on the network layer.

Each host in the SWAT is an integration of the agent system, network, and security infrastructure. The agent framework contains mobile agents and static agents (services). The security components include group key management and group membership revocation, enforced by a security mediator. The agent framework is connected to the security components, enabling an agent (or the whole agent system) to join or leave a group, with the permission to join controlled by the security mediator. The network components enable secure point-to-point communication for the agent framework, as well as reliable group communication for the security components. Point-to-point communication is implemented using standard TCP/IP and is secured using IPSec. All network communication is routed using a multi-hop ad hoc routing protocol on a wireless network.

The SWAT infrastructure consists of PDAs (HP iPAQs), tablet PCs, and laptops on an 802.11b wireless network with ad hoc routing. SWAT is developed on the Familiar Linux distribution, using the Intel Strong Arm architecture of the HP iPAQ h3800 series PDAs. A similarly configured Linux environment exists for the x86 architecture, to incorporate other portable devices to the testbed such as laptop and tablet PCs. SWAT makes use of Cisco Systems' Aironet 350 series PCMCIA cards across all platforms. We have selected the Aironet cards based on empirical studies, demonstrating that the Aironet cards have the best performance in ad hoc mode compared to network cards of other brands.

Demonstration Scenarios

SWAT is currently being tested and validated in a number of practical scenarios. The main functional objective of SWAT is to provide users with tools for distributed, mobile, collaborative work and communication. There are many practical applications of such a system (e.g., police personnel at a sports event, medical personnel at an accident scene, emergency responders to a natural disaster). One possible SWAT application may be in the homeland security domain, where first-responders react to civil emergencies and "bring their own network." Using SWAT they will be able to communicate and transfer information more effectively, and in ways not possible with existing technologies.

A demonstration will begin with a set of hosts in the staging area, familiarizing the audience with the platforms. After a review of the equipment, we shall demonstrate the functionality of the SWAT. Certain SWAT demonstrators wielding wireless components will leave the area, and demonstrate use of the whiteboard application. Two-way radio communication features will be used to show coordination, and for demonstrating secure routing of messages according to group structure. Revocation functionality will be demonstrated through the revocation of agents and users both within the staging area, and away "in the field". Streaming video and audio will be sent from remote hosts to the staging area, and hosts may be "knocked out of commission" as they suffer power and network failures. Different host topologies will be demonstrated in order to impose network "stresses" on the routing protocol and on the network-aware reasoning agents.

References

[1] Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik. On the performance of group key agreement protocols. In *Proceedings of the 22nd IEEE International Conference on Distributed Computing Systems*, 6 2002. An extended version is available as Technical Report CNDS-2001-5.

[2] Y. Amir and J. Stanton. The spread wide area group communication system. Technical Report CNDS-98-4, The Center for Networking and Distributed Systems, John Hopkins University, 4 1998. http://www.cnds.jhu.edu/publications/.

[3] D. Artz, A. Burnheimer, W. Regli, and M. Kam. The topology-aware secure ad hoc routing protocol. Technical report, Department of Computer Science, Drexel University, 2003.

[4] D. Artz, M. Peysakhov, and W. Regli. Network meta-reasoning for information assurance in mobile agent systems. In *Proceedings of the Eighteenth International Joint Conference on Artificial Intelligence*, pages 1455–1457, August 2003.

[5] BBN Technologies. Cougaar architecture document. http://docs.cougaar.org, February 2003.

[6] D. Boneh, X. Ding, G. Tsudik, and M. Wong. A method for fast revocation of public key certificates and security capabilities. In *Proceedings of the 10th USENIX Security Symposium*, pages 297–308, August 2001.

[7] R. Lentini, G. P. Rao, J. N. Thies, and J. Kay. Emaa: An extendable mobile agent architecture. In *AAAI Workshop on Software Tools for Developing Agents*, July 1998.

[8] E. Sultanik, D. Artz, G. Anderson, M. Kam, W. Regli, M. Peysakhov, J. Sevy, N. Belov, N. Morizio, and A. Mroczkowski. Secure mobile agents on ad hoc wireless networks. In *Proceedings of the 15th Innovative Applications of Artificial Intelligence Conference (IAAI-03)*, pages 129–136, 2003.