Intelligent Systems Demonstration: The Secure Wireless Agent Testbed (SWAT)

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

Description of the SWAT

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 (Sultanik *et al.* 2003). 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 infrastructure, mobile agents manage keys, assess network traffic patterns, analyze host behaviors, revoke access rights for suspicious agents, users, or hosts, adaptively re-route traffic at the network layer to improve the information integrity of the overall system, and provide the implementation framework for a number of decentralized user applications, including authentication, collaboration, messaging, and remote sensor monitoring. SWAT is currently 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 (Lentini *et al.* 1998) and Cougaar (BBN Technologies 2003). 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 (Artz, Peysakhov, & Regli 2003). 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 (Artz *et al.* 2003).

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. SWAT is the first complete integration of 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. The cryptographic tools integrated in the current implementation of SWAT include: CLIQUES, the Tree Group Diffe-Hellman (TGDH) algorithm, Spread (Amir & Stanton

*Contact author: cicirello@cs.drexel.edu

1998), Secure Spread (Amir *et al.* 2002), a SEcurity Mediator (SEM) (Boneh *et al.* 2001), and IPSec.

Each host in the SWAT is an integration of the agent system, the network, and security infrastructure. The agent framework contains both mobile agents, and static agents (services). The security components of a host 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 through a multi-hop ad hoc routing protocol on a wireless network.

The SWAT infrastructure consists of PDAs (mostly 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 found within 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.

Throughout the conference Demo Program, SWAT will be demonstrated continuously. A demonstration will begin with a large set of hosts in the staging area, familiarizing the audience with the platforms. After a review of the equipment, we shall demonstrate group functionality through group creation and "join" and "leave" operations. Certain SWAT demonstrators wielding wireless components would leave the area, and demonstrate use of the whiteboard application. The whiteboard application will also show the integration of GPS as a backdrop for notations sent to group members (given adequate GPS radio signal reception inside the building). 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. A Sharp Zaurus handheld PDA will attempt to decipher transmissions and disturb operation of the secure SWAT network.

References

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

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

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

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

BBN Technologies. 2003. Cougaar architecture document. http://docs.cougaar.org.

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

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

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