

Plans for Distributed Sensor Network Security

1 Jan 2000 thru 30 Sep 2000

NAI Labs, the Security Research Division of Network Associates, Inc.

Background

This plan is based upon the tasking agreed upon by Dr. Kumar and NAI Labs at their meeting of 29 October 1999. This document provides a brief problem statement, research plan, and deliverables.

Problem Statement

Distributed sensor networks will employ communications among large numbers of sensors remotely deployed in irregular patterns to form ad hoc distributed processing networks that can produce high-quality information with minimized resource consumption. To reliably support coordinated control, management, and reporting functions, sensor networks must be self-organizing with both decentralized control and autonomous sensor behavior, resulting in a sophisticated processing capability. Sensor networks must be robust and survivable despite individual node failures and/or intermittent connectivity.

Providing confidentiality and authentication is critical to preventing an adversary from compromising the security of a distributed sensor network. However, providing key management for confidentiality and group level authentication is difficult due to the ad hoc nature, intermittent connectivity, and resource limitations of the distributed sensor network environment. Our research will address this problem by developing a security architecture and cryptographic mechanisms that efficiently provide integrity, authentication, and confidentiality security services.

Research Plan

To solve the problem described above, our research will investigate the use of three innovative ideas: attribute-based keying, developing groups through interactive challenge protocols, and the use of symmetric key certificates.

We will research the use of distinguishing characteristics or attributes (e.g., location and/or sensor capabilities) of nodes plus the use of device and mission keys to develop new keying methods to determine an ad hoc group key. Attribute-based keying uses one-way functions in a manner similar to Clueless Agents, where only nodes that have attributes matching a sender's query would be capable of decrypting a given message. We will determine the conditions where attribute-based keying provide cryptographically significant protection. We will analyze the effectiveness of attribute-based keying in a variety of scenarios, including a mapping of its effectiveness to the SensIT demonstration architecture.

We will research and develop an interactive challenge protocol where attribute information is exchanged between two mutually suspicious entities. This type of protocol allows members unknown to each other to develop a sense of trust that each should be part of the ad hoc group. The development of trust grows will grow from pairwise relationships to entire groups, possibly by leveraging the use of symmetric key certificates.

Finally, we will research the use of symmetric key certificates in a distributed sensor network. We will examine the applicability of symmetric key certificates, identify suitable scenarios, and describe

the security assumptions necessary for their use. We will identify characteristics of a security architecture that incorporates symmetric key certificates.

Deliverables

Constraints and Approaches for Distributed Sensor Network Security (Draft) – This document will describe the various aspects of the identified problem, including the constraints of the distributed sensor network environment. Constraints include the ad hoc nature and intermittent connectivity of the sensor network, and the CPU and power resource limitations of the sensors themselves. We will describe the results of our research in solving the problem, including the use of attribute-based keying, developing groups through interactive challenge protocols, and the use of symmetric key certificates. **Delivery Date: 1 June 2000**

Constraints and Approaches for Distributed Sensor Network Security (Final) – Building off of the first deliverable, we will describe the tradeoffs of various approaches based on different characteristics of the distributed sensor network. We will specifically detail an approach appropriate for further examination via either simulation or participation in SensIT project demonstration/experiments. **Delivery Date: 1 September 2000.**