Approved for Public Release; Distribution Unlimited
Case # 09-1034

MTR090056
MITRE TECHNICAL REPORT

Examining SOA Attribute-Based Security in Tactical Networks

A Web Services Security Engineering Initiative

Albuquerque, Ronald

(PI, ✉ ralbuquerque@mitre.org**)**

Jenkins, Adam

(✉ ajenkins@mitre.org**)**

April 2009

Sponsor: Dept. E121; Dept. E128
Dept. No.: E547
Contract No.: N/A
Project No.: 03X92AD0-JR; 03X92AE0-BM
Downgrade: N/A
Derived By: N/A
Declassify On: N/A

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

This document has been approved for public release.

©2009 The MITRE Corporation.
All Rights Reserved.

Abstract

Emerging net-centric warfare technologies will provide military decision support personnel with access to significant amounts of battlefield information that is real-time. These technologies offer the potential to significantly transform command and control in Battle Management. Effective, intuitive information sharing will be a key driver for that improvement.

The war-fighter operates in dynamic situations where human factors impact the security environment. Systems employing enterprise Service Oriented Architecture (SOA) must implement advanced security that reflects this context.

Current approaches to information sharing are largely coarse-grained and do not take environmental factors into account - this posture discourages effective information sharing. Assured Information Sharing (AIS) attempts to strike a balance between protecting information and enabling the sharing of that information.

This technical report presents findings on research into Assured Information Sharing. It examines the best practices in implementing Attribute-Based Access Control (ABAC) via security policies in an SOA. In order to better inform SOA development, the focus is on operations within an airborne tactical network environment. It explores how fine-grained security mechanisms perform when disconnected, intermittent, and low-bandwidth network characteristics are imposed. The primary objective is to gain insight into associated tradeoffs.

The following are key conclusions drawn as a result of our research:

- An Attribute-Based Access Control (ABAC) security capability can be provided with today’s COTS technologies.
- Fine grained IA capabilities enable context-specific security.
- Policy-Based Access Control (PBAC) results in a security capability that can enable closer alignment with operational realities.
- ABAC is not prohibitively hindered by tactical network considerations.