Quality of Service (QoS) support for Web services in military networks

Overview

The task is to build a prototype Web service based middleware with role based QoS support using existing standards where possible. As the network capacity is often the most limited resource in a military radio-based network, it is important to control access to this medium in order to be able to deliver acceptable service quality to all users. This focus of this assignment is to use existing Web Service standards to implement such a network access control mechanism. Relevant existing solutions to work with are DiffServ (network level QoS), and SAML, XACML, WS-Policy, WS-Security (all related to Web services policies, security, and roles) to express user roles and enforce access to the network. Current network resource state shall be taken into account when deciding/enforcing network access.

Motivation

Essential to Network Based Defense (NBD) is the concept of end-to-end QoS, which in turn requires employing cross-layer QoS signaling. This means that QoS must be considered at all layers of the OSI model, and that QoS information must traverse these layers. To achieve the end-to-end property needed in NBD, QoS information must also be allowed to cross both network and national boundaries. There already exist QoS mechanisms that can be used on the transport layer and below, and thus we focus our research efforts on the application layer and issues regarding cross-layer QoS signaling. Having IP as a common protocol and assuming DiffServ as the network level QoS framework, we focus on the application level solutions in this task (i.e., the middleware). The task is to provide for QoS at the application level, and map the demands to and from the Type-of-Service (TOS) field in the IP header, enabling cross layer QoS signaling. DiffServ provides coarse traffic shaping, so it is desirable to have finer grained control on the application level by taking user needs (role) and available resources (current network resource state) into account.

Technology

This task focuses on Web services as the middleware technology, as this has been identified by NATO to be the key enabling technology for network-centric operations. Currently, Web services are lacking standards for QoS, but there is a need for role based access control and prioritization of users and resources. Existing security standards can be employed to provide partial functionality:

- SAML is an XML-based framework for request/response exchanges of authentication and authorization information. SAML assertions describe the results of authentication actions that occurred previously. A single assertion might contain several different information items: authentication (identity), authorization decisions, credentials, group membership, etc. In this task, SAML should be used to identify the client's role.
- XACML defines a policy language for defining access control policies, and also provides an architectural model. A policy enforcement point (PEP) relies on a policy decision point (PDP) for deciding the outcome of a request, based on the policies applicable to the request. In the task, this could be used to implement application level role based access control.
- The WS-Security specification defines new SOAP extensions (message headers) bringing integrity and confidentiality to SOAP messages. It supports confidentiality (encryption), integrity (signatures), and protection against message replays. In the task, we're mostly interested in its capability to carry security tokens. Supported tokens are Username, Kerberos, X.509, XrML, and the above mentioned SAML.

The goal of the task is to build a prototype QoS framework for Web services utilizing relevant parts of existing Web services security related standards (and others). Evaluation will be performed using a realistic and representative networking environment (emulated or simulated).