Center for Information Systems Security Studies and Research (CISR)Faculty and Researcher Publications

2001-05-00

Managing Costs and Variability of Security Services

Spyropoulou, Evie

IEEE

Presentation to IEEE Symposium on Security and Privacy, Oakland, CA, May 2001

Managing Costs and Variability of Security Services

Evie Spyropoulou, Cynthia Irvine, Tim Levin and Bruce Allen
Center for INFOSEC Studies and Research
Naval Postgraduate School
[eviespy | irvine | levin | ballen] @cs.nps.navy.mil

When an application is submitted for execution in a network, where geographically distributed, heterogeneous resources are available, a Quality of Service (QoS) middleware mechanism can be used to intermediate and schedule the application for execution. In our research we are working on including security as a dimension of QoS. Quality of Security Service (QoSS) is enabled when users or network tasks are presented with variable levels of security services and requirements, from which the desired level for the security dimension can be selected.

Furthermore if a particular security mechanism is “fixed” (i.e., always applied) then the overhead for the mechanism is part of the normal cost of running the task and the normal costing mechanism used by the QoS control mechanism will suffice. For variant security mechanisms, however, the security overhead will vary, depending on the security vector of the user’s QoS request. The middleware must have access to detailed information about the resource costs for each variant security mechanism.

We are working on a QoSS costing demonstration. In this approach we use a model for tasks, that incorporates the ideas of variant security services and value ranges for the security attributes. We additionally take into account an operational mode parameter (e.g. normal, impacted, emergency), because network status could influence the security policy and security services applicable to the task: for example under certain conditions, a user or administrator may be willing to accept more (or less) security for a given application. Users are presented with a simplified abstraction of security, in the form of security level choices, such as “high”, “medium”, “low”, and these selections are mapped to detailed mechanism invocations via a translation matrix.

To quantify the costs related to a task’s security requests, we use a costing framework (based on a security service taxonomy) with cost expressions relative to every security service invoked by the task. Each service may access various resources, e.g. CPU, memory and bandwidth. We discriminate between start-up and streaming costs. The calculated costs can then be fed to a middleware QoS mechanism for use in its resource allocation and scheduling decisions.

Current research involves linking QoSS conditions to underlying security mechanisms. IPSec provides various choices for the characteristics of the Security Associations (SAs) that can be established between two entities that wish to communicate. As a proof of concept we are working with modulation of IPSec variables to supply QoSS. Using the IKE protocol and the KeyNote trust management system, we can regulate SA parameters like encryption and hash algorithms, key lengths, SA life times, based on policy decisions that account for the application, system operational mode, and desired security level. We plan to conduct experiments and measurements to help us understand the impact of QoSS on the performance of applications under various network operational modes and high level policies.