Type of submission: Paper

Title: Intrusion Detection Inter-component Adaptive Negotiation

Topic categories: Adaptive IDS solutions (Innovative Approaches); IDS interoperability Standards and Standardization (IDS Integration); Large-scale IDS (IDS in High Performance Environments)

Speaker/first author: Richard Feiertag (feiertag@tis.com)

Contact information and other authors:

Richard Feiertag
(feiertag@tis.com)
TIS Labs at Network Associates Incorporated
3965 Freedom Circle
Santa Clara, CA 95054
(408) 346 – 3789

Stuart Staniford-Chen
(stuart@silicondefense.com)
Silicon Defense
791 Shirley Blvd
Arcata, CA 95521
(707) 822-4588

Karl Levitt, Mark Heckman, Dave Peticolas, Rick Crawford
({levitt, heckman, peticola, crawford}@cs.ucdavis.edu)
Department of Computer Science
UC Davis
Davis, CA 95616

Lee Benzinger, Sue Rho, Stephen Wu
(Lee_Benzinger@nai.com, {jsr, wu}@tislabs.com)
TIS Labs at Network Associates Incorporated
3965 Freedom Circle
Santa Clara, CA 95054

The IDS community is developing better techniques for collecting and analyzing data in order to handle intrusions in large, distributed environments. To take advantage of this on-going work, IDSs should be able to dynamically adapt to new and improved components and to changes in the environment. The Intrusion Detection Inter-component Adaptive Negotiation (IDIAN) project has developed a negotiation protocol to allow a distributed collection of heterogeneous ID components to inter-operate and reach agreement on each other's capabilities and needs -- i.e., the information that can be generated and processed. Moreover, the negotiation is dynamic, so the information generated and processed can evolve as the IDS evolves or the environment changes.

The IDIAN project leverages the Common Intrusion Detection Framework (CIDF), an effort by DARPA to develop a common language, protocols, and APIs that would allow intrusion detection components to inter-operate and share information. The IDIAN project has extended the CIDF language CISL (Common Intrusion Specification Language) with constructs useful for dynamic negotiation. One such

construct is the notion of a *filter* to specify sets of IDS messages. Filters are useful in negotiating, for example, what audit data will be transmitted. The IDIAN project also adopts the CIDF framework architecture that classifies ID components according to their function.

The negotiation protocol utilizes the notion of a contract -- an association between two ID components, a producer and a consumer -- which specifies one or more possible agreements between them. An agreement commits the producer to provide the consumer with a set of services. For example, a detection component (producer) might have a contract with an analysis component (consumer) to provide a specific set of audit data.

At any given time, at most one of the agreements in a contract is in effect, although the ID components may elect to switch to one of the alternatives dynamically. Furthermore, two components may have multiple contracts operating at the same time.

The primary function of the protocol is to allow ID components to dynamically negotiate new contracts/agreements and to change existing ones. The protocol is designed to ensure that negotiations eventually terminate, and to handle multiway, cascading, and hierarchical negotiations.

To facilitate choosing among several options, the protocol uses the notion of *cost* to capture the relative cost to a producer (resp., consumer) to provide (process) a specific set of resources. Services provided by producers use up a variety of system resources. A consumer may decide to use a particular service only if the resource cost is below a certain threshold. The absolute and relative amount of resources required to supply a particular service may vary over time, and the protocol allows producers and consumers to renegotiate when necessary.

In addition to the protocol, the IDIAN project has developed several scenarios that demonstrate specific situations in which an IDS must adapt to a changing environment. The scenarios can be divided into two general classes:

1. The acquisition of a new capability by the IDS. For example, an ID component may acquire a new attack signature. The IDS must adapt by incorporating the new signature into the overall system.

2. An overload of the IDS caused, for example, by faults in the IDS itself or by a flooding attack. The IDS could adapt by reducing the amount of information being gathered, or by cutting off the flow of data from the flooding source.

Finally, the IDIAN project is working on a demonstration of the protocol operating in the scenarios.