Cyber-Security for Computational Grids and Virtual Supercomputers

RADIANT: Research And Development In Advanced Network Technology
http://www.lanl.gov/radiant

With our national security coming under increasing scrutiny, there is a heightened awareness of the importance of securing our cyber infrastructure. To this end, we propose an inter-realm infrastructure for security (IRIS) and active wardens to proactively protect against cyberattacks.

IRIS: Inter-Realm Infrastructure for Security

The rapid growth in high-speed networks and the ubiquity of computers have converged to enhance global interconnectivity and provide the foundation for a new kind of computing infrastructure—computational grids (also known as virtual supercomputers). These grids consist of computational nodes that are distributed throughout geographically dispersed areas and institutions and are interconnected through a reliable internetwork; they harvest significant processing power, memory, and resources by utilizing the capabilities offered at the end nodes.

Securing a computational grid (that may be accessed by tens, hundreds, or even thousands of users) will be critical to its future. To address this issue, we present a cyber-security infrastructure called *IRIS: Inter-Realm Infrastructure for Security* that provides highly customizable and dynamically reconfigurable services to proactively secure communications between these grid nodes.* And because the widespread deployment of computational grids involves using the Internet as the communication backbone, the cyber-security infrastructure must also seamlessly deal with the heterogeneous nature of the Internet.

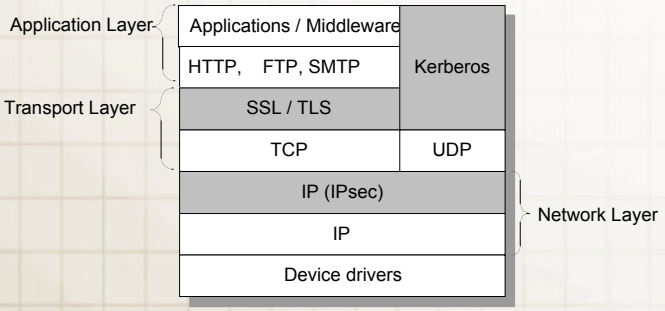

Figure 1: Relative Location of Security Mechanisms in the Protocol Stack

Background

Many security mechanisms have been devised to retrofit security into the Internet and existing distributed systems. While Kerberos, SSL, IPsec, and other similar technologies provide security services at various places in the protocol stack, as shown in the shaded boxes of Figure 1, many of these security services only offer security as an "all-or-nothing" option. Another common problem, particularly in the use of SSL and IPsec tunneling over different realms, is the introduction of *security gaps*.

While the current standard in grid security, the Grid Security Infrastructure (GSI), provides secure authentication and communication for grids, it does not discover middleboxes and negotiate security with them. As a result, security gaps could surface, particularly in

*Realms are areas with similar network characteristics e.g., a campus network. To handle this diversity between realms, *middleboxes* are introduced at the realm boundaries for mobility support, network address translation, packet filtering, firewalls, wireless gateways, etc.

cases where some grid resources and nodes exist in a local network behind a firewall. In addition, the adaptability of GSI may be limited because of the difficulty in porting it to lightweight devices (e.g., PDAs) in support of ubiquitous grid computing.

The Vision

We advocate a cyber-security infrastructure that incorporates greater flexibility, adaptability, and customizability. When it comes to security, one size does not fit all. Hence, the security architecture deployed must be able to adapt to environments with varying conditions. Further, with many different security technologies surfacing and being deployed, the assumption that a particular security mechanism will eventually prevail is flawed. For that reason, it is necessary to support multiple security mechanisms and negotiate security requirements. We also aim to reduce or eliminate security gaps.

To this end, we have implemented a prototype of the aforementioned cyber-security infrastructure called IRIS: Inter-Realm Infrastructure for Security. Our current implementation is in Java. We used Java for its cross-platform compatibility, which allows IRIS to be ported easily to the heterogeneous nodes that constitute a computational grid. Additionally, Java is gaining ground in the mobile world allowing IRIS to be ported to mobile devices, handheld computers and embedded devices in support of ubiquitous grid computing.

Active Wardens

Research in the area of steganography, as well as the state of the art for security systems, is dominated by a reactive paradigm of detection and response. However, by the time this reaction occurs, substantial damage may have already occurred. To proactively stifle steganography, covert channels, and other network attacks, the RADIANT team is developing "active warden" security systems. Using our model, all network traffic is routed through active wardens, which modify communications as to preserve overt communications, yet prevent the propagation of extraneous or ambiguous information that can be used for exploitation, such as covert channels, subliminal channels, and certain forms of intrusion detection and intrusion detection evasion. This is done by perturbing possible carriers to the level of their “Minimal Requisite Fidelity” (MRF), which represents the degree of signal fidelity that is both acceptable to end users but destructive to covert channels. For a class of “unstructured” carriers, MRF is defined by human perception, but for a class of “structured” carriers, well-known semantics give us high assurance that a warden can completely eliminate any subliminal or covert channels.

For future information on IRIS, please visit our team Web site at *http://www.lanl.gov/radiant.*

Contact Information

Send e-mail to: *radiant-info@lanl.gov.*

RADIANT: Research And Development in Advanced Network Technology
(http://www.lanl.gov/radiant)
Los Alamos National Laboratory
Los Alamos, NM 87545

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

November 2001

LALP-01-244

A US DEPARTMENT OF ENERGY LABORATORY

Los Alamos
NATIONAL LABORATORY
Los Alamos NM 87545