Integrated Enterprise Network Security Management

Technology #m07-096

“Lead Inventor: Angelos D. Keromytis, Ph.D.

Network Security Firewalls, User Password Protection Inadequate:
Current network security generally depends on a firewall to protect an internal network from the internet, coupled to user/password style security for each network service. A major problem within this framework is the independence of authentication: network services (e.g. database, web and file servers) perform authentication without consultation with each other or an overarching security broker. This leads to difficulty in identifying and controlling security threats from compromised intranet computers or external threats coming from distributed computers.

Network Security with Security Policies Across Network Services:
This technology provides a method to implement global, dynamic security policies across network services. The software is based on an event model, where network events are identified by sensor software, which informs a global security manager. The global policy broker determines the course of action, which is carried out by actuator software. This general architecture is broadly applicable to current networks, since only the sensor must be specialized for a particular network service. In more detail, the technology was developed in a event-listener model with the following components:

Sensors – software attached to network services which monitor activity and fire events under certain circumstances;
Events – announcements from sensors to a listener, which indicate network activity of interest has occurred;
Policy Engine – a central listener for a broad variety of events, which is able to make policy decisions for each network service and request for service;
Actuators – software which implements policy decisions, for example turning on logging of requests or blocking services.
With the focus on global security, this technology will protect networks which are currently veneric to internal, distributed or extremely slow attacks.

Applications:
• Enterprise network security
• Individual computers security

Advantages:
• Dynamic management of security
• Communication between services


Licensing Status: Available for Licensing and Sponsored Research Support
Inventors

Angelos D. Keromytis