Application Security: Loose-Coupling for Legacy Apps

Lori MacVittie, 2008-18-03

Last week we dove into the use of application delivery as a way to apply the SOA benefits of loose-coupling to "legacy" web applications. This week we'll dive into how to achieve similar benefits by applying loose-coupling to security for legacy applications.

Loose-coupling of security general requires the use of a service to apply - or enforce - security policies outside the application or service. At a minimum, the decoupling of security policies from actual services preserves the ability to reuse services in multiple applications, many of which may have different security needs. For example, applying authentication and authorization as a separate service means that a single service can be used in applications requiring active directory services as well as those that may use LDAP. While you could certainly write code to integrate both security mechanisms, this requires conditional coding that can hamper performance as well as longer development, testing, and deployment cycles. When introducing a new application, these requirements to support integrated security policies can potentially interrupt availability of existing applications making use of that service when they are tested and redeployed.

In a SOA, an intermediary can - and should - enforce security policies on services, and this should optimally be accomplished in a policy-based manner, through the use of meta-data, rather than hard-coded.

Loose-Coupling and Security for Legacy Apps

The benefits of reuse through loose-coupling can also be achieved for legacy web applications with the use of an external service, such as can be provided by an application firewall. In addition to the performance benefits of centralizing security duties, there are configuration and maintenance benefits that can be achieved by decoupling many security functions from applications.

First is ability to enforce corporate security policies across multiple applications without the need to modify existing applications or add code to support those policies. If your corporate security policy includes scanning for malicious content and attacks (if it doesn't, it certainly should!) then you can configure a web application firewall to provide that scanning duties for **all** applications. This reduces the number of entry points into the application that can potentially be exploited as well as number of touch points required to upgrade, update, or change the scanning mechanism. If a new attack is discovered, instead of updating multiple applications - which takes time and effort that translates into money - you only have to update a single device or application: the application firewall.

A second advantage is that by decoupling security policy from applications you decrease the potential for introducing new errors when modifying security code. While "cut-n-paste" methods can, if they are used carefully, reduce this potential as well, there is still the possibility that the original code being copied contains an error or vulnerability. If this occurs, then all applications that have been "updated" are now vulnerable and must be modified, tested, and redeployed - again.

Finally, decoupling security from applications allows you to enforce different security policies based on a number of parameters such as from where the user is accessing the application or whether the client is a person or a machine. Just as the flexibility of loose-coupling in a SOA aids in the ability to more easily integrate applications with partners and other applications, the same is true when security policies are decoupled from legacy web applications. For example, using an application delivery controller in conjunction with an application firewall you can require that all external clients must authenticate using a certificate while internal clients may be able to use a username and password. This flexibility and conditional access control can also be achieved through the deployment of an SSL VPN.

There are many options and product types available that can decouple security from legacy web applications in order to achieve benefits similar to that of loose-coupling within a SOA implementation. If you're looking for ways to loosen the ties that bind security tightly to your applications, consider the options and their benefits.

Imbibing: Water

Technorati tags: MacVittie, security, application delivery controller, application firewall, SSL VPN, loose-coupling, SOA, reuse

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com