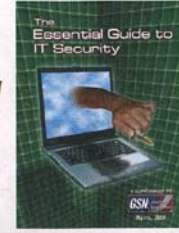


Presenting our 3rd annual buyer's directory



GSN's latest Essential Guide to IT Security

Begins after Page 7



# Authentication best practices: It's all about the data



By Nick Atalla

One of the major concerns in an organization's overall security strategy is how best to address protection of its valuable intellectual properties. Current trends indicate that encryption is widely used to protect digital

information at various stages, such as in transit or at rest.

Public key encryption schemas ensure only permitted users have access to sensitive con-

tent. Passwords can be added to protect files and encryption schemas to protect information as it travels across the Internet to end-users.

However, what happens when that protected digital file is received by the end user and opened in a common application, like Microsoft Word? How do you ensure that the information will be handled properly and not misused, whether intentionally or accidentally?

According to a 2007 Datamonitor report, 77 percent of data leakage is non-malicious. How do you insure that the end-user cannot copy or print a file or, for example, forward a

file to another user whom the content owner did not intend to have access – even if the content owner had non-malicious intentions?

Microsoft Windows Rights Management Services (RMS) is a Web-based technology that provides persistent and diverse protection to digital information while in storage, in transit and, most importantly, while in use. RMS technology can enhance and complete an organization's overall security strategies around digital information.

Microsoft Windows RMS is an information protection technology that works with RMS-enabled applications to help enforce policies

about how information is handled by end-users. The technology is more than just encryption – it's encryption plus the ability to define access and use policies for individual users or groups. Applying Federal Information Processing Standard (FIPS) 140-2, in multiple end-user licenses, an individual's authorization to access information he has rights to are issued to each piece of content, creating individualized barriers to prevent leakage. This means that if a protected email or document was attained with malicious intent, the single email or document may be compromised but the entire system would remain intact and secure.

For example, a policy can be applied to a Word document that would restrict a recipient's ability to print the document. The recipient may be able to view the document and even email it, but would be unable to print a hard copy. Likewise, a policy may be applied to an email message restricting the recipient from forwarding the message to another individual. These policies are referred to as "usage" policies, and with the Microsoft solution the usage policies are bound to the actual file – a persistent protection.

Each usage policy is enforced by the RMS-enabled application requiring that the identity of the recipient be trusted. Trusting identities on the Internet is far more complex than the common notion of trust between two individuals. Trusting the identity of the individual attempting to access RMS-protected content is critical to the overall integrity of the RMS environment.

Windows RMS works cohesively with Active Directory in establishing trusted identities and servicing requests from users. Establishing a trusted identity is accomplished through an individual's membership in Active Directory. Service requests, such as end-user licensing, are made by the RM-enabled application on behalf of the user. Once an individual is authenticated and certified with the Active Directory RMS service, RMS automatically provisions the individual with a set of certificates that uniquely identify that individual to the RMS subsystem.

Once provisioned with the proper certificates, RM-enabled applications will use the individual's Right's Account Certificates (RAC) to ensure the identity of the person requesting to open protected content. If the usage policy bound to the email or document does not define usage rights for the requester to open the email or document, the application will deny access.

The authentication process can range from simple, single-factor username and password authentication to a more secure, two-factor authentication, employing smart-card/bio-factor plus username/password mechanisms.

The integrity of the RAC is key – once issued to a particular user on a particular platform, the RAC is secure against attack because it is linked through a series of digital signatures to the user on a particular platform. It's also very easy to provision the same user on multiple platforms, as RMS stores copies of each user's unique certificate in the configuration database for the program.

Rights Management is also transformative and can be extended to third-party solutions. In RMS, a construct called "templates" is used to apply policies to content. A template predefines usage policies, such as time limitations and renewal policies for the content, and is used to define usage rights for individuals and groups. If a template is used to protect a document or email, the template can be transformed over time, concurrently altering the usage policies for content already delivered to users to match.

Additionally, although Rights Management as a core technology is strictly a Microsoft platform solution, third parties, such as GigaTrust, not only extend RMS to non-Windows platforms, the BlackBerry mobile platform, and non-Office document types like PDF, but also extend RMS to non-Active Directory authentication schemas.

In terms of an organization's overall security strategy, RMS is a must-have technology because it provides protection and policy enforcement for an organization's valuable digital intellectual properties and can ensure regulatory compliance across multiple industries. RMS protects information while at rest, in transit or in use and does so at the data level. After all, it is all about the data. ■

Nick Atalla, is VP, public sector services, GigaTrust.