XML Security

Author: Mihai Rotaru

Date: 10 Dec 2011

XML is becoming increasingly common, and therefore security issues are also having an increased importance. Given that XML is frequently used in e-commerce, businesses need ways to ensure that stored data is secure, and prevent unauthorized access. This is especially important due to the textual nature of XML - a simple text editor can be used to view the contents and extract sensitive data.

A number of security-related technologies have emerged, one of the most important ones being XACML - the eXtensible Access Control Markup Language. XACML allows for controlling access to information via rules and policies. Other significant initiatives are XML signature and XML encryption.

The concept of digital signatures is not new, and mature standards have been in place for quite some time. But existing technologies only allow signing individual files. Given the hierarchical nature of XML, more granularity is highly desirable - in other words, the ability to sign portions of an XML document. This is the role fulfilled by XML signature. The high-level algorithm is quite simple - the element to be signed is hashed, the hash being stored inside a `DigestValue` element. Another digest (usually a hash) is produced from this element and is cryptographically signed. The XML signature is then inserted in the `signature` element.

XML encryption operates on similar principles to XML signatures - it allows the encryption of XML documents with a high granularity, enabling the encryption of portions of a document. An additional advantage is that different encryption keys and algorithms can be used for each encrypted portion, allowing precise control over who can use which portions of the document.

XML encryption is especially important in a business environment. For example, a delivery company might define an XML document type which contains one element which contains information about the client, and billing information, and one element containing information about the contents of the delivered package. The driver will have the key for viewing the client information, while the client might be sent via email the key for him to be able to view information about the content and check if anything is missing.