Aaron Powers

Tom Guenther

Matt Nuckolls

Problem Statement

XML provides a versatile way to store data. Data stored in an XML format can be published on the web for distribution purposes. This allows for a convenient method of distributing data to other individuals interested in the data. Naturally, some of this data may be sensitive or may only be intended for a certain individual to read. A secure method of publishing XML data is needed to prevent unauthorized access. The method of secure publishing should support the ability to verify a receiving individual’s allowance access as well as preventing the individual from seeing portions of the document they are not intended to see. Additional features that would be beneficial would be for the publisher to have the ability to publish only changes to an existing document instead of republishing the entire document as well as the receiving individual having the ability to only receive changes to the document relevant to the portions they are allowed to access instead of re-downloading the entirety of the document.

Analysis of the Problem

XML is a flexible markup language. It is intended to be both machine redable as well as human readable. Though it has a specific structure defined by tags, elements, attributes, etc. it has no specific format nor requirement for tag sets. This flexibility makes it versatile but also vulnerable.

Since XML simply a markup language, it has no intrinsic security mechanisms. Therefore, XML data storage and transmission security must be handled externally to the XML content. XML document encryption is necessary for secure storage and transmission. Furthermore, XML document access must also be handled externally. Again, XML has no intrinsic access controls.

Since access and transmission control must be handled externally to the XML document (implicitly: the XML parser), a “3rd party” application may be required to authorize access over a secure transmission protocol such as SSL (secure socket layer).

Possible Solutions

One possible solution is to implement a publish / subscriber middle layer that handles all transactions between the publisher (entity containing the data) and the subscriber. The middle layer would serve as a gateway to provide secure access to the stored XML data. At some level it will be assumed that the content provider who originates the data to be published will take reasonable precautions to ensure that the data is presented to the publisher in a secure way. The content provider will ensure that the middle layer is informed of any document access restrictions and constraints under which the publisher must act. At this point we don't have a clear picture of what this middle layer will look like. More effort will be spent on fleshing out the details. At the present time this is the solution we are exploring.

Review of Related Papers