

Digital Rights Management & XML Security Protocols

Head-to-Head or Hand-in-Hand?

Holly Lynne McKinley, SSCP
Booz Allen Hamilton
McLean, VA

Introduction

Digital Rights Management brings to mind controversial issues such as software piracy, RIAA lawsuits for illegally downloaded music, and peer-to-peer (P2P) file-sharing programs. The protection of information, including creative rights, has become a hot topic with the emergence of programs like Napster and Kazaa. These programs have challenged the boundaries of both registered and perceived copyrights; and developed a new arena for the implementation of security measures.

Purpose and Scope

The purpose of this paper is to examine the DRM and XML's security protocols to determine if a synergy exists between DRM and XML protocols, and if so, can this synergy be used to further secure information. For each concept, this paper will discuss key features and applications. Since DRM is a controversial issue, a section of this appendix will broach these topics.

The application of digital rights to a program can be observed in the transmission of information from point to point. Some important security concentrations are:

- Identification & Authentication
- Authorization & Access Control
- Accountability
- Non-Repudiation
- Confidentiality
- Integrity
- Availability

These considerations provide a contextual foundation for the security discussions presented in this paper.

The scope of this paper is to examine DRM and XML security as they relate to web applications and web services. Peer to Peer DRM applications and the integration of privacy concerns are not fully examined; rather these issues are mentioned for the reader's note and further consideration.

It is important to remember that DRM is not a mature technology. Many court cases are being pursued to define copyright, intellectual property and privacy in this digital age.

Digital Rights Management Overview

Rights do not have simple definitions. Legislatures, courts and public forums have debated the definitions of privacy and property. Court cases are plentiful here, making this subject fairly prominent in the media and heated in public opinion. There is not yet a universal definition of *best practices* for rights management implementation; however, as the definition of rights is matured through court cases and legislation, these practices will become standardized. Additionally, digital content provides a complexity in that it is highly portable and transmittable.

DRM provides methods for ensuring the security of non-code content enroute to the end user. Because the content being secured is typically copyrightable works and intellectual property, it is important to understand the laws and policies impacting copyrights and intellectual property protection. The legal definition of copyright explains that an author's copyright covers works of literature, music, drama, pantomime/choreography, picture/graphic/sculpture, motion picture/ audiovisual, sound recording, and architecture. The definition of intellectual property is slightly different from that of copyright. Intellectual property is the ownership of ideas and control over the tangible or virtual representation of those ideas. The protection of intellectual property information is important to the prosperity of a business model and can be integrated into the architecture through implementation of DRM.

The *Digital Millennium Copyright Act of 1998* (DMCA) is a key policy (and controversy) that covers a broad range of content. The DMCA establishes United States legislation implementing two WIPO treaties: the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). These treaties are implemented by member nations, reinforcing the necessary global nature of intellectual property and copyright protection. *Title III: Computer Maintenance or Repair* and *Title IV: Miscellaneous Provisions* describe specific circumstances where strict copyright exemptions can be applied.

Key features:

First generation DRM methods established locks and limitations on content distribution. The current generation of DRM provides more flexibility in the development and dissemination processes by using Rights Expression Languages to wrap content or injecting tags throughout the protected content. These languages are establishing more efficient management of the rights holder's relationships with the content, and with the original author or copyright holder.

Content creation, usage, and management are three points that build the DRM framework that Renato Ianella has developed. In this framework, the creation and capture module support rights validation, rights creation and rights workflow. The management module supports storage/repository functions and trading functions. The usage model supports permissions and tracking management. These functions, once a common set of protocols and interfaces is developed, will allow DRM to be implemented across a system.

Several standards groups are addressing the lack of common DRM protocols. These groups are primarily the W3C, OASIS, IEEE and IETF. Open E-Book forum (OBEF) and MPEG group are heading the efforts from the media perspective. The IETF and W3C are reviewing several DRM standards. The following protocols have been reviewed, or are currently under revision.

- The **Open Digital Rights Language (ODRL)** is an open-source protocol established to provide the semantics for controls of digital content. ODRL provides expressions of “permissions, constraints, obligations, conditions, offers and agreements with rights holders.”¹ The security model of ODRL implements XML encryption and XML Digital Signature entities.
- **MPEG-21**, an open framework for multimedia resources management has initial portions standardized or at a draft-standard state. The initial parts of the MPEG-21 framework that have been finalized are: Digital Item Declaration DID, Digital Item Identification DII; those at draft standard status are: Digital Item Adaptation DIA or the Rights Expression Language REL and the Rights Data Dictionary RDD.
- The **DRM Specification V2.0** outlines the cryptographic protocol, messages, processing instructions and certificate profiles required to implement the specification. One of the required protocols is **Rights Object Acquisition Protocol (ROAP)**. A Rights Object expresses permissions and constraints that control how protected content can be used. ROAP controls these objects and allows the content to be viewed by users with appropriate rights objects.

Applications of Digital Rights Management

There are examples of DRM implementations in many areas of technology. CDs, DVDs and eBooks are commonly cited applications of DRM. Additionally, DRM is applied to streaming Internet video and evaluation versions of software through software metering. Digital envelopes and message authentication codes assist in the implementation of DRM.

ODRL is currently supported in 50 types of mobile handsets, an important first step into wider DRM applications. *mVideoGuard™* is a current implementation for ROAP, that also supports forward-lock, combined and separate delivery DRM.

The use cases provided by MPEG demonstrate that music distributions, streaming video and digital broadcasts are suggested applications of MPEG-21. Additionally, MPEG-21 can be cascaded to various rights levels.

Though DRM technologies can be challenged and hackers can find ways to “crack” DRM technologies, these technologies provide content protection from naïve users. DRM technology prevents inexperienced users from using software beyond fair use,

¹ ODRL Specification

deters illegal reproduction of copyrighted material, and protects the intellectual property rights of the author.

XML Security Overview

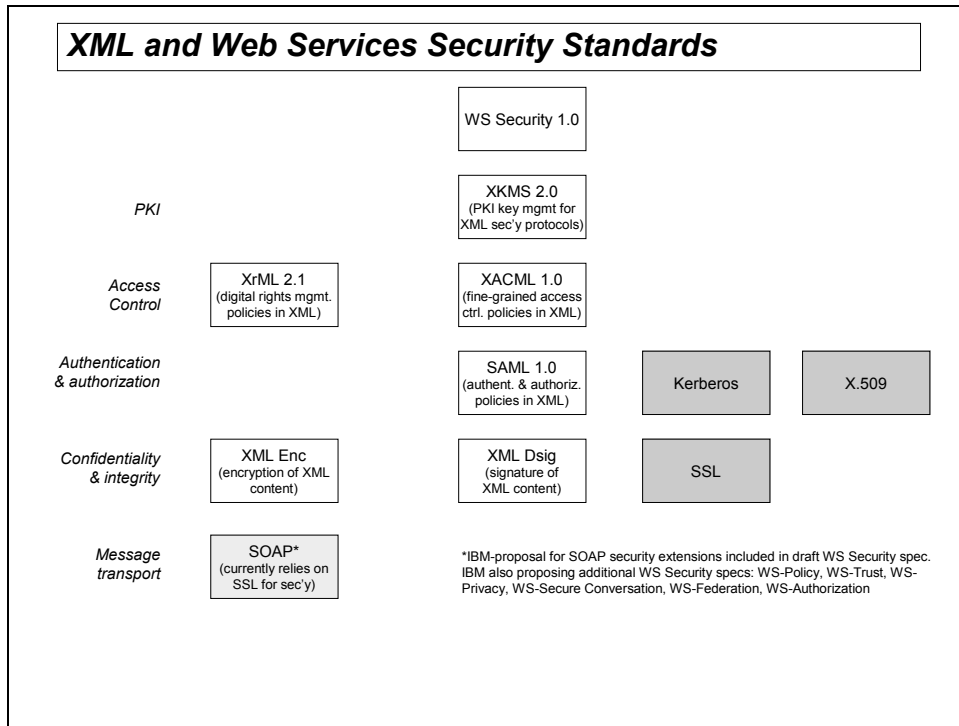
XML security options are available for providing authentication, authorization, access control, integrity, non-repudiation, confidentiality and auditing. The XML protocols used to mediate these security concerns are SAML, XKMS, XML Digital Signature, XACML, and XrML. Many of these protocols are explained in-depth in other portions of this Developer's Guide.

There are seven primary standards for establishing the framework for integrating security into XML-based applications. These standards are described below, including the standards body/organization responsible for defining them, and the status of each standard (draft, recommendation, etc.).

- XML Digital Signatures (XML DSig) – Allows portions of a document, or the whole document (as a file) to be signed. Most relevant for Workflow scenarios. STATUS: W3C recommendation, Feb 2002. IETF Draft Standard RFC 3275. RESPONSIBLE ORGANIZATION(S): W3C and IETF
- XML Encryption (XML Enc) – Defines the XML rule set for cryptographically protecting the confidentiality of XML and non-XML documents. Also allows for a part of the document, or the whole document to be encrypted. STATUS: W3C Recommendation since 2002. RESPONSIBLE ORGANIZATION(S): W3C
- Security Assertion Markup Language (SAML) – Allows for Single Sign-On (SSO) authentication to different systems and platforms. Nested assertions maintain user credentials as those credentials are passed to another application. STATUS: Version 1.1 approved Sept 2003. RESPONSIBLE ORGANIZATION(S): OASIS
- Extensible Access Control Markup Language (XACML) – Expresses access policies in XML documents. Enforces access rules and integrity of content being sent. STATUS: Version 1.0 approved February 2003. RESPONSIBLE ORGANIZATION(S): OASIS
- Extensible Rights Markup Language (XRML) (now MPEG REL)– Handles access rights/conditions within a document such as expiration times. XRML is a more specialized, digital rights management focused version of XACML, including specialized targets for media. STATUS: Version 2.1 submitted in May 2002. The OASIS group was disbanded in 2004, and the project was picked up by the MPEG. RESPONSIBLE ORGANIZATION(S): OASIS, now MPEG
- XML Key Management Specification (XKMS) – Web Services interface for PKI. Composed of two protocols: X-KISS (for retrieving/verifying public keys) and XKRSS (Defines service interfaces for registering/revoking/recovering keys from a key server). STATUS: Version 2.0 Working Draft April 2003. RESPONSIBLE ORGANIZATION(S): W3C
- WS-Security – A set of security standards defining new SOAP extensions for message authentication using XML Enc. WS-Security is a collaborative effort to

develop an object-oriented approach to different aspects (“subjects”) of Web Services Security. These subjects are: WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation, and WS-Authorization. STATUS: Version 1.0 April 2003. RESPONSIBLE ORGANIZATION(S): Microsoft, VeriSign, IBM

The figure below illustrates the relationship between the Web Services security standards and the Security functions they are designed to perform or enable. Standards in the grey boxes are general security standards/mechanism that are used by the Web Services security standards. SOAP acts as the transport mechanism for the security data transferred. SOAP currently has no security standards of its own.



Key Features of XML Security Protocols

XML security protocols provide the implementation capabilities for DRM on various media. DRM, though available for years, has matured through the widespread implementation of XML, specifically through the increased investment in web services. Each of the researched DRM protocols is reinforced through the use XML Security protocols.

SOAP is an XML protocol primarily used to transport procedural calls between computers. It is currently implemented for Java, COM, Perl, C#, and Python. XACML, WSDL, Wireless Binary XML (WBXML) and MPEG REL (XrML) are the typical protocols that are used to support DRM. Additionally, the ability to bridge the

differences between ODRL and MPEG-21 licenses has been demonstrated using XSLT and XSL-FO.²

Applications of XML Security Protocols to DRM

XACML is currently implemented with PSS System's Enterprise DRM solution. WSDL's advanced failure mechanism has been suggested as an implementation of rights management. WBXML is required to implement for DRM Version 1.0

MPEG selected XrML Version 2 over other rights languages, modified the language slightly, and ratified it as MPEG REL, part of the MPEG-21 standards and it is now an ISO standard.

ODRL is an XML-based rights expression language free of licensing restrictions, providing a lightweight formal mechanism for specifying rights independently of the content type and transport mechanism. As previously mentioned, it is currently applied in mobile handsets.

XML schemas are provided for Rights Object Acquisition Protocol (ROAP) protocol data units, Rights Object Acquisition Protocol trigger media type, and the OMA DRM Rights Expression Language. The OMA DRM Rights Expression Language (REL) V2.0 is defined as a mobile profile of the Open Digital Rights Language (ODRL).

Controversial issues regarding DRM

The implementation of DRM stirs debate in many communities. Though copyright and intellectual property rights are readily understood by most users, there are several other issues that develop surrounding DRM.

Some of these issues are:

- Heavy lobbying of legislatures in order to preserve a business model, where content is attached to saleable goods
- Removal of exceptions to copyrights must be balanced with fairness to the end user (copies for fair use)
- DRM's technical integration with other DRM technologies and with current applications
- Distinguishing digital copies from original content
- Standardization of DRM across platforms

² <http://odrl.net/workshop2004/paper/odrl-polo-paper.pdf>

Head-To-Head or Hand-In-Hand?

A final important point is that DRM and XML can be used in concert to increase the protection of information in transit and storage. The technologies, when working together, create a strong security model for DRM while simultaneously maintaining strong models as separate entities.

In the context of application security, DRM and XML security mechanisms protect digital content, and support each other with a layering method. As seen in the table below, XML is a support structure for DRM technologies, and DRM supplies further content management capabilities to the XML security protocols.

Security Method	DRM Supported	XML Supported
Identification and Authentication		X
Authorization and Access Control	X	X
Non-Repudiation	X	X
Confidentiality		X
Integrity	X	X
Availability		X

The origin of attack against security measures is another key difference between standard DRM and XML security technologies. The typical user who attempts to defeat DRM measures attacks as the end user or recipient of specifically downloaded information. Alternately, the typical hacker who attempts to defeat XML security measures intercepts information (that may or may not be specifically targeted), and the information

The application of both DRM and XML mechanisms ensures that protected content is wrapped in layers of security, further establishing defense-in-depth for the message contents.

Conclusion:

From this research, it is conclusive that XML security protocols are essential for the success of DRM in a dynamic environment. DRM applications and XML security protocol implementations work together, as well as separately to secure the content of messages. As DRM technologies standardize and mature, it will be imperative that the developing XML protocols be maintained as well.

The controversial issues surrounding DRM will continue to be a legal and public debate. More court cases and legislation will develop, and the pace of technology will probably maintain its pace ahead of the legislation.