XACML for Export Control and Intellectual Property Protection

John Tolbert

Introduction:

The Boeing Company has adopted the OASIS eXtensible Access Control Markup Language (XACML) standard for authorization. The XACML standard will be a foundational component of our security services architecture. XACML is well-suited for handling a variety of authorization models, such as attribute-based access control (ABAC) and discretionary access control (DAC).

While there are many authorization use cases, this paper will detail 2 particular use cases for which I have developed XACML profiles to address: export compliance and intellectual property protection. These use cases are widely recognized as complex but essential elements for global organizations security architectures.

I have co-authored an XACML U.S. export control profile that contains a list of standard attributes used in making export control authorization decisions. The profile attributes are based on the Export Administration Regulations from the U.S. Department of Commerce and the International Traffic in Arms Regulations from the U.S. Department of State. I have also written an XACML profile for intellectual property controls, which is based on an international understanding of intellectual property laws and protection schemes.

I am also developing an OASIS Open Document Format (ODF) for Office Applications metadata specification that contains elements that correspond to the XACML profiles mentioned above. The goal is to provide a comprehensive approach to making export and intellectual property authorization decisions using OASIS standards.

Export control:

The export control profile is predicated upon the notion that any U.S. organization that ships goods, materials, software, and/or technical information may be subject to U.S. export control laws. Non-military products may be classified according to the U.S. Department of Commerce Commerce Control List. Non-military products which are subject to export controls are classified by Export Control Classification Number, or ECCN. ECCNs are 5 character alphanumeric codes which

describe various regulated technologies. ECCNs may be further defined by sub-paragraph classifications.

Military products are controlled according to the United States Munitions List (USML).

Destination countries are also classified by a variety of criteria. Even specific entities and individuals may have restrictions. The recipients U.S. person status, location, and organization must also be taken into account in these export control authorization decisions.

To facilitate interoperability between authorization systems, we have aggregated the minimum list of attributes required for this type of authorization decision.

The XACML EC-US profile attribute list:

Resource attributes
classification, ECCN, and USML.

Subject attributes
nationality, current nationality, location, organization, and US person.

While the EC-US profile is specific to U.S. export regulations, the principles embodied in this profile could be utilized to develop XACML profiles for other nations export regulations.

Intellectual property:

Intellectual property (IP) may be defined as legal property rights over mental creations. IP owners can receive exclusive rights to their creations if certain conditions are met. These exclusive rights can be exploited by the owner for profit, either directly through sales of products, or indirectly through licensing.

IP is an asset; perhaps the most valuable asset an organization has. IP can be licensed to other organizations in cases of outsourcing and/or to generate revenue from IP sharing arrangements.

IP value tends to increase when properly protected, though there are differing points of diminishing returns. IP protection doesnt guarantee security; it just provides a compensation mechanism for cases of unlawful exploitation. IP valuation and protection are often criteria for venture capital investors.

Broadly speaking, there are four main categories of intellectual property: copyrights, trademarks, trade secrets, and patents. Copyrights confer

time-limited exclusive rights of ownership and/or use to the creator of the work. A copyright is typically used to protect artistic works such as photographs, music, books, etc. Copyrights are internationally recognized, though there are differences in the terms and enforcement.

Trademarks are the IP protection scheme of names, logos, symbols, products, etc. For example, in the U.S. there are 2 main types:

- For general usage, or for not-yet-registered trademarks
- For trademarks registered with the USPTO

Trademarks are also internationally recognized through the Madrid system, which requires registration through the World Intellectual Property Organization (WIPO), a United Nations agency. The World Trade Organization also sets legal minimum standards for IP protection among member nations.

Patents are property rights granted to an inventor to prevent others from profiting from the invention for a limited time in exchange for public disclosure of the invention when the patent is granted. Patents apply to processes, machines, articles of manufacture, or composition of matter (including biological), or derived innovations. Patents require detailed disclosure of information, designs, processes, etc. Patents are administered in U.S. by the USPTO, and are internationally recognized by WTO TRIPS, WIPO, and European Patent Convention.

Trade secrets are IP protection of formulae, processes, designs, information, etc. that are not easily obtainable that a business uses for competitive advantage. They are often protected by legal contracts such as non-disclosure agreements, non-compete agreements, or proprietary information agreements. Trade secrets are the most common form of industrial IP protection, and therefore outnumber patents. However, trade secrets are often categorized as proprietary information, and may not be discovered as trade secrets unless litigated. They are not federally protected in the U.S., though most states have adopted the Uniform Trade Secrets Act. However, theft of trade secrets is prohibited by U.S. Economic Espionage Act of 1996. Trade secret status requires less disclosure than patents. Trade secrets are well protected by European Patent Convention as know how. No international treaties protect trade secrets, though WTO TRIPS, GATT, and NAFTA have provisions for trade secret protection.

To facilitate interoperability between authorization systems, I have aggregated the minimum list of intellectual property attributes that are needed for rendering access control decisions in the XACML IPC profile.

The intellectual property attribute list:

Resource attributes

- IPC-Type (copyright, patent, trademark, trade secret)
- IPC-Data (string data, such as patent number)
- IP-Owner (owner of the intellectual property)
- IP-Designee (designated custodian of licensed intellectual property)
- License (contract or statement of work to which the marked IP data pertains)

Subject attributes

nationality and organization.

Environment attribute

location.

Action attributes

storage, physical transmission, electronic transmission, encryption type, marking, disposal, and authority.

Data marking

Realizing that XACML policy and rule evaluation works optimally with consistent data- or resource-level marking, we have begun work to standardize resource-level attributes for export and intellectual property controls. The Open Document Format for Office Applications Document Controls profile that I am proposing has metadata elements that match the XACML profiles mentioned above.

The ODF Document Controls metadata element structure:

```
meta:document-controls
    export-control
        us:classification
        us:eccn
        us:usml
    ip-control
        ipc-type
        ipc-data
        ip-owner
        ip-designee
        license
```

Though the Document Controls profile currently contains markings for U.S. export controls and intellectual property controls, plans are underway to create elements for Transglobal Secure Collaboration Program (TSCP) tags as well as document sensitivity labeling.

I chose the ODF TC as the starting point for data marking standardization. The ODF format is currently supported by Microsoft Office, OpenOffice, StarOffice, Google Docs, and Adobe Buzzwords. It can potentially be extended to other line-of-business applications as well. Moreover, we recognize the need for data marking standards for structured data, and are beginning the work in that area presently.

Conclusion

The attributes and glossary terms defined in the profiles are not an exclusive or comprehensive list of all the attributes that may be required for rendering authorization decisions concerning export compliance or IP protection. For example, XACML PDPs may have to evaluate other entitlements, such as group membership, from XACML PIPs. The profiles are meant as points of reference for implementing controls, and may be extended as needed for organizational purposes. Software vendors who choose to implement these profiles should take the defined attributes as a framework for export and IP controls, but allow individual implementers some flexibility in constructing their own XACML-based authorization policies and PDPs.

The goal of these profiles is to create a framework of common export and IP-related attributes upon which authorization decisions can be rendered. These profiles will also provide application software developers and authorization policy administrators guidance on supporting export and IP control use cases.

The Boeing Company finds that the XACML standard is a sufficient means for performing access control decisions that meet our business needs, as detailed in the use cases and profiles documented above. The XACML policy schema provides a rich set of features for expressing policies in a platform independent way, and the XACML request/ response protocol provides an excellent mechanism to externalize authorization functions from applications.