The Challenges of Protecting Trade Secrets

By John Tolbert and Crystal Hayes, The Boeing Company

Intellectual property (IP) is often a corporation's most valuable asset, and as computing security professionals, it's our responsibility to protect it. The loss of IP, whether by misappropriation or accidental leakage, can lead to loss of competitive advantage, loss of revenue, and potentially present national security risks. TSCP's objectives are to design and implement technical controls that facilitate the protection of IP via secure collaboration among our members. This paper will look at the challenges of protecting IP and trade secrets in particular and why it can be difficult.

TSCP provides a framework and specifications for secure collaboration among our members from the Defense sector, U.S. and European government agencies, and technology sector. Protecting TSCP members' IP is a key objective of secure collaboration, so the IP Working Group (IPWG) was launched recently to define a generic framework for the secure exchange of IP and proprietary information and the requirements that must be addressed through procedural and technical controls.

Intellectual Property is the primary target of cyber attacks in most industries today. The 2012 Verizon Data Breach Investigations Report counted 855 data breach incidents with more than 174 million records compromised, and states: *"Mainline cybercriminals continued to automate and streamline their method du jour of high-volume, low-risk attacks against weaker targets.* ***Much less frequent, but arguably more damaging, were continued attacks targeting trade secrets, classified information and other intellectual property.***"

What are Trade Secrets?

IP denotes certain legally protected expressions and mental creations. Trade secrets are a type of IP, but unlike copyrights, trademarks, patents and design rights, they are protected by *keeping* them secret. When creators take steps to protect their ownership and rights to their IP, for example, by registering the mental creation with government agencies, they may exploit those rights for monetary gain. Owners of copyrights, trademarks, patents and design rights can profit from their IP directly through the sale of products, or indirectly through licensing. All the above categories of IP are internationally recognized, but the terms of application, registration, and protection vary from country to country.

Typically, copyrights are granted for original literary and artistic works such as photographs, music and books as well as software. A copyright confers time-limited exclusive ownership or usage to the creator or creators of such works or software, and has effect at the time the work is placed in fixed, tangible form. In the Aerospace & Defense industry, copyrights most commonly protect software, drawings and manuals.

A trademark can be a name, logo, symbol, product, or in the case of a service, a servicemark. Both registered (®) and unregistered (™) trademarks are recognized in the United States and other common law countries; the former, registered with the United States Patent and Trademark Office (USPTO), provides the owner greater legal protection from infringement.

Patents are issued for invented processes, machines, tools, designs or derived innovations. A patent, as stated in U.S. statute, is "the right to exclude others from making, using, offering for sale, or selling the invention in the United States or importing the invention into the United States." Thus, the inventor has the exclusive right to financial gain from his invention for a limited period of time in exchange for public disclosure of

tion within that collaborative environment has an obligation to manage access to their partners' trade secrets as well as to their own. That can be especially challenging when we are collaborating on one program while competing for new business elsewhere.

Intellectual Property and trade secret protection is predicated upon controlling access to physical and electronic resources. The technical controls used to provide authorization services for business systems as well as high security / defense systems can be enhanced for better IP protection. Not to be confused with authentication, authorization is the granting of access rights to resources to principals (such as users and devices). Authentication is the verification that an entity, whether human or machine, is who or what they claim to be by validating their credentials.

Currently, many systems support OASIS XACML (e**X**tensible **A**ccess **C**ontrol **M**arkup **L**anguage), an XML-based standard language for making authorization decisions. XACML provides a storage schema for rules, policies, and policy sets and policy and rule combining algorithms. XACML also provides an abstraction layer that allows application developers to externalize authorization functions. XACML's request/response protocol can be used to create runtime authorization engines to govern access to IP resources. Furthermore, the XACML IP control (IPC) profile that specifies an industry standard list of attributes and attribute values has been created. This profile represents a common vocabulary that can be used to develop access control policies for IP resources. See https://www.oasis-open.org/committees/document.php?document_id=45915&wg_abbrev=xacml to view the complete specification.

TSCP's Information Labeling and Handling (ILH) specifications have defined standards for sharing and protecting members' trade secrets using OASIS XACML. The IPWG will develop more detailed business and technical requirements for ILH.

By leveraging the XACML standard, members can author policies for the protection of trade secrets that can be consumed by any XACML-conformant Policy Decision Point (PDP). Web-based applications can then defer access control decisions to authoritative PDPs.

TSCP is working with the XACML Technical Committee to establish a profile for the use of XACML, which supports the standardized metadata scheme used in the TSCP Business Authorization Identification and Labeling Scheme (BAILS) and Business Authorization Framework (BAF). This is intended to build on the work already in progress within the XACML Technical Committee on the Intellectual Property Controls profile. The utilization of these metadata standards will promote consistent enforcement of electronic access control policies over members' trade secrets as data moves between organizations in collaborative environments. Additionally, having standardized metadata and XACML-based policies can reduce trade secret leakage by integrating with Data Loss Prevention (DLP) technologies. Files tagged with metadata (for example, "Proprietary," "IP-Owner=Curtiss," and "Agreement-123") can then interact with DLP mechanisms that make policy-based access control decisions to limit data movement, and even prevent unintended disclosure. To expand upon the example, assume an engineer has authorized access to work on a technical drawing and wants to email it to an industry partner, but no license exists that authorizes that transfer. If the drawing file is properly tagged with metadata and the engineer's company is using XACML-based DLP, this transfer would be denied due to a lack of authorizing policy.

Some of the challenges to trade secret protection are specific to identification, metadata tagging, and integration of resource attribute evaluation into current and next-generation XACML-based authorization systems. Unstructured data must be correctly and consistently categorized and tagged with meaningful metadata. Practical methods must be developed to apply the same categories and attributes to structured data as well. Industry also faces challenges related to the acceptance and adoption of the aforementioned standards and protocols in software products.

In conclusion, despite these challenges and the fact that trade secrets are increasingly targets for cybercriminals, technologists are advancing standards and tools to mitigate the threats. TSCP is partnering with standards organizations and leading the way in developing solutions to protect the trade secrets of its members. We welcome and invite technical and legal experts from our membership to join us in these efforts; to contribute, contact the IPWG at ipwg@tscp.org.

TSCP is a government-industry partnership specifically focused on mitigating the risks related to compliance, complexity, cost and IT that are inherent in large-scale and collaborative programs that span national jurisdictions. For more information about TSCP and our initiatives, please visit www.tscp.org, where TSCP documents and specifications are available to the broader technology audience.