

W3C Workshop on Transparency and Usability of Web Authentication

15-16 March 2006, New York, New York, USA

Position Paper

Abstract:

This paper is submitted to focus on the use of declarative rule languages to express trust attributes associated with websites and services in order to facilitate the expression and communication of meta-information regarding security in a manner that informs and empowers users and user agents to make more effective trust decisions. W3C new standards efforts in the area of rules and services can help provide a foundation towards technologies that will enable better global security and privacy support on the Web.

Statement of Issues: The conflict between the potential of Web Services and the inadequacy of web authentication is potentially best described as “a failure to communicate”. As enterprises extend and evolve into more dynamic, real-time facilities, central operations require the ability to express their security requirements in greater detail than can be currently enabled. Corporations must define and adhere to increasingly large directories of requirements in the management of their internal security controls; requiring compliance with those controls by participants in the extended enterprise is becoming essential.

Corporate operations increasingly distribute their computing and data processing requirements across a network of third party services, some of which are engaged and employed for controlled, finite sessions. But those third parties, for so long as they are processing data and functioning as part of the operating whole of the primary corporation, are being pressured to demonstrate their adherence to the security controls of their customers. This requirement is an expression of a requirement for trustworthiness—to be engaged as a part of the extended enterprise is to be trusted to perform in compliance with the applicable controls.

Traditionally, companies relied on the primary service agreements (non-web-enabled) to express requirements for the security of their trading partners and to describe appropriate means for verifying compliance with those requirements and, if necessary, imposing sanctions or remedies for non-compliance. However, the volume of requirements for security has handicapped the continued effectiveness of the contract as a functional tool for expressing security controls and enforcement. Quite simply, the varied nature of the requirements—focusing on security at the network, device, application and data level, as well as authentication itself—has overwhelmed the ability of the contract (and the contract drafters) to be effective as a governance tool that assures the integrity of the data being transported and processed.

Corporations have been placed under enormous strain to define, in a manner that is transparent and verifiable, their entire information security portfolio. Much of the

pressure for this activity has been from regulatory sources. Whether focused on the integrity of financial data, the reliability of patient data or the security of customer account records, the new requirements insist on considerable detail, structure and, perhaps most importantly, verifiability through audit. As one leading enforcement officer at the U.S. Securities and Exchange Commission recently observed, “Compliance must be capable of being demonstrated, to an objective reviewer, to have occurred *in fact*” (emphasis added).

Corporations have employed a variety of standards-based frameworks through which to develop their security infrastructure and to align their security controls toward structures that also enable extensibility—today, security must be capable of traveling across and binding networked systems that are partnered into the extended enterprise of a business. A frequent structure employed is ISO 17799; that standard, however, is currently lacking any structure through which third party certification can be provided (such as that available through the BS7799 counterpart). While current upgrades to 17799 are being developed to permit such certification, it is now foreseeable that, in negotiating either institutional partnerships (such as outsourcing or other shared data services) or individual sessions or transactions, companies will demand even further details—real-time confirmations of the current-state of the security services within a partner’s systems.

At the W3C Workshop on Rule Languages for Interoperability, 27-28 April, 2005, a paper was submitted calling for the prioritization of policy-based rule languages expressing information security controls [<http://www.w3.org/2004/12/rules/ws/paper/101>]. This paper proposes that, to achieve effective authentication, suitable mechanisms must be developed to capture and convey a more complete expression of the security credentials of the entire systems behind the webpage itself. Trust is inherently stronger when informed by greater information, and trust decisions, including by user agents, have the capacity to process and take into account a wider range of attributes than perhaps even the human user. Expressive web rule languages are key to help declaratively define, distribute, manage and use the information and evaluate the relevant criteria.

Thus, the mechanisms of authentication should be capable of being configured in order that:

- Policy-based rules that have been implemented for security can be expressed in a compact structure that can be referenced and reviewed by automated means. In this manner, the expression of requirements in a formal contract (which is both static and likely impossible to be referenced in real-time) can be replaced by a more dynamic, contemporaneous expression of the rule-based security controls.
- Mechanisms should exist to evaluate the expressed rule architecture as a means for authenticating not just the identity but the security structures and operations of a specific system or web service.
- User agents must be capable of expressing specific requirements that may be pre-conditions to any further evaluation of the trustworthiness of a proposed system and, in turn, the target system must be capable of expressing whether those requirements are satisfied.

- If necessary, performance history under the expression of policy-based rules can be queried and evaluated. While this concept may be highly controversial, the reality is that trust decisions functionally demand the same information as audits, compliance reviews or certifications—the only differences are measured by the frequency of the required evaluation. By contrast, restricting user access to data demonstrating that the described controls are, in fact, effective, betrays a lack of commitment to empowering effective trust decisions.
 - Note: performance history is a routine data capture in other trust decisions (e.g., e-bay ratings, etc.); this paper only proposes such data be automated and expressive in association with a larger inventory of policy-based rules expressing the operating information security controls.

XML Enabled Capability

Achieving the functionality of the proposed mechanisms enables more robust evaluation of the efficacy of security controls and, in turn, improved reliability in trust decisions. RuleML is proposed as an effective technology to be integrated into other mechanism, in order to permit the rapid, high-volume, processing required to enable these mechanisms and, as well, achieve other goals of interoperability, extensibility and security. A pilot that combines the earlier proposal for a rules language expression of ISO 17799 with the interoperability of communication proposed here would greatly contribute to a better understanding of trust decisions and improve the overall efficacy with which business relationships are structured.

Submitters

This paper is submitted by Jeffrey Ritter and Said Tabet.

Jeffrey B. Ritter: currently practices law, assisting clients in contractual implementations of information security controls and the production of compliance systems for various regulatory environments, both domestically within the United States and in Europe. This submission represents his personal views and is not the expression of the views of the law firm or its clients. Jeffrey B. Ritter, Kirkpatrick & Lockhart Nicholson Graham LLP;1601 K Street, NW;Washington, DC 20006-1600;1+202.778.9396;jritter@klng.com

Said Tabet: co-founder and co-Chair of the RuleML Initiative, involved in various key standards initiatives for the Web. Currently focus on standards-based public and enterprise policy and regulatory guidelines specification and management. Compliance is a key vertical topic that touches to all aspects of security and privacy particularly on the Web and in distributed systems. Said Tabet can be reached at stabet@ruleml.org