XDAS Update Project

Project Review and Future Plans

This document will provide a brief history of the X/Open Distributed Audit Service (XDAS) specification, explain why the Update Project has been on hold for some time, and propose future work in this area.

Historical Overview

In 1997, the XDAS v1 Preliminary Specification was published by The Open Group. This specification presented a classification of generic events, a common event format, and four APIs for submitting events, reading events, importing events, and for configuration. As best as we can determine, this specification was the first standards-based effort to attempt to define structured audit events for IT systems.

This effort never moved past the Preliminary Specification stage, primarily because very few implementations were actually attempted. In practical usage, most products were already doing something to generate audit events – if only to files – and the effort required to convert to XDAS was prohibitive. Furthermore, significant gaps in the standard, a lack of extensibility, and Unix-specific concepts embedded in the specification caused others to reject adoption for newer products seeking a way to express events.

Based on this feedback, the 2008 XDAS Update Project was kicked off with the goal of taking the best parts of XDAS v1, combining that with current industry best practices and input from experts in the field, and creating XDAS v2. One of the early decisions was to ditch the API dependencies inherent in the v1 specification, and focus on the classification of generic events and the event format. The intent was to allow any consumer to understand event audit data no matter how it was received – syslog, file, or a real API.

Of course, many vendors were and are currently using their own proprietary event formats, and we soon found that one prominent vendor, Arcsight, was proposing a similar project. Their intent was to take the proprietary 'Common Event Format' (CEF), find a standards body to polish it up into a real standard, and publish it. MITRE picked up that effort and soon had a solid community of industry experts involved in the creating of a standard they called 'Common Event Expression.' As this effort evolved the original CEF underpinnings started to disappear, however, and a real community standard started to emerge. The Open Group members involved in XDAS also joined the project in an effort to influence the direction of the work and ensure alignment with a future XDAS standard.

In early 2011, we discovered that the Distributed Management Task Force, under the aegis of the Cloud Management Working Group, had also realized that a common event auditing standard would be necessary for proper auditing of cloud activities. The resulting effort, called the Cloud Auditing Data Federation (CADF) group, had an almost direct overlap with the intended XDAS work in terms of the components that would be defined although focused at a different level in the architecture. As before, The Open Group members actively engaged with the DMTF project to influence the work.

By the end of 2011, there were three different event standards in development, and no clear differentiation between them. The Open Group's XDAS effort was furthest along, but did not have very many active participants; MITRE's CEE effort had strong vendor support and industry experts, but lacked true standards-body clout; and the DMTF CADF group also had strong participation but was in its very early stages.

Given the state of affairs, the decision was made to pause the XDAS efforts within The Open Group and throw our resources behind the DMTF CADF effort. The reasoning here was two-fold: one, we felt that if multiple competing standards were promulgated, this would dilute the value of any standard; and two, some of the decisions made within the CEE standard did not align with the goals of the XDAS standard. Of course, we could not do anything to prevent MITRE from publishing a competing standard, but we felt that by accelerating the CADF effort we may be in a better position in the end.

As of now, the DMTF CADF effort is a couple months away from publishing the first official standard, and the MITRE CEE effort has been halted. A lot of work has gone into the CADF specification to ensure that it will serve the needs of The Open Group members, either as is or by extension. It is now time to revisit the XDAS Update effort and evaluate whether it makes sense to proceed.

The Future of XDAS

Clearly, there are three distinct options with respect to the XDAS. We can:

1. Drop the specification entirely
2. Develop and release a new, independent specification
3. Develop a specification that is a companion to the new DMTF CADF specification.

With respect to option (1), there are a few reasons this path may not be the best choice. First, the CADF standard is entirely focused on problems related to cloud auditing – an important space to be sure, but as a result there are certain operating system-level (for example) event classes and resources that may not be completely represented. Second, there are a few existing implementations of XDAS v1, and providing a transition path for those implementations is desirable.

With respect to option (2), the downside to this approach is pretty obvious – we are unlikely to get much traction in the market if XDAS attempts to "compete" with CADF. There may be some niche areas where a very different (from CADF) standard makes sense, but in fact The Open Group members worked to influence the CADF standard to be reasonably close to something that would support the XDAS use cases as well.

Option (3) seems to be the most attractive at this time. The CADF standard is designed to be very extensible, and as mentioned there are some "gaps" below the cloud level that XDAS could serve an important role in filling. In practical terms, XDAS would become a "profile" of the CADF standard, and one that was specifically targeted at operating system and application-level auditing.

Proposal

The proposal here is to create an XDAS specification that is a profile of the CADF DMTF specification. This would define two core things:

- Extend the CADF spec to cover any missing resources, actions, and other information that was defined in XDAS v1 or that we believe is necessary to cover standard OS, application, and network device logging
- Define a method to translate XDAS v1 format messages into the CADF format.

As an ancillary goal, we'll also review more recent best practice efforts including the nascent-but-moribund CEE effort, and make sure that lessons learned during development of that specification are accounted for in this new specification.

Justification and Target

The rationale for developing event standards in general has been well vetted through various forums, including meetings going back to the 2008 Catalyst Conference, a well-attended panel on this topic at the 2009 RSA Conference, and the simple fact that three independent groups identified the market need at roughly the same time.

In terms of the market, increasing consolidation of corporations and the resulting need to federate data, including audit event data, is driving increased interest in work like this. Furthermore, stricter regulatory regimes are requiring ever more detailed audit reports, leaving auditees wondering why they can't simply query their log management system for "all authentication events" or other seemingly simple questions. Cloud providers are also attempting to create offerings based on multiple loosely-coupled federated services, and need to provide proper audit trails to their customers who may not even know (or care) which underlying products are in use.

Industry has responded with products that consume many types of event data and parse, normalize, and classify that data in consistent ways; these are called Log Management and Security Information and Event Management products. Such products provide immense cost savings to customers formerly forced to have experts manually review the source event logs; as a result, the SIEM market has consistently grown 10-15% YoY. Roughly 1/3 to ½ the cost of any SIEM solution, however, is embodied with the normalization logic – a task which Mary Ann Davidson, CSO at Oracle, compared to "translating from Latin to Greek."

Development of an industry-wide event standard would therefore benefit:

- Vendors authoring new products that recognize that customers will need to be able to audit internal product activity, and that these customer wish to do so at a low cost
- SIEM vendors that want to stop spending such a large portion of their development budget on such a low-value task
- Cloud service providers that need to be able to consolidate event data from multiple services within their clouds or from federated providers, and deliver segments of that data to their clients in a consistent way
- Consumers that want to be able to consolidate event data from many different sources, and be able to analyze and report on that data consistently.

The DMTF CADF effort has tackled a portion of these areas via their specification, but the primary focus of that effort has been on the cloud service providers and their clients. The XDAS effort would extend that work to provide better support for the individual product vendors that are currently developing products or willing to update existing products.

The obvious gap here is related to existing products with a pre-existing, proprietary event schema. Even if consumers start to demand that such vendors move toward an easily-consumable standard, there will be significant resistance due to the costs of switching. On the other hand, simple translators from the proprietary format to the standard format could be crowd-sourced on the open market, and once these have been created they could be used by all consumers regardless of which Log Management or SIEM product they use.