This document is restricted for personal use of Michael BÃ¼rger
Downloaded from KuppingerCole on 30.11.2015 20:50

KuppingerCole Report

EXECUTIVE VIEW

by Graham Williamson | September 2015

Axiomatics – Beyond Database Security

Managing access to data held in databases is becoming increasingly important. We need a way to mask sensitive data from those who should not see it and deliver content those who should. We also need to do this dynamically, removing access on a real-time basis as user authorization changes.

by **Graham Williamson**
gw@kuppingercole.com
September 2015

Content

1 Introduction 2
2 Product Description 3
3 Strengths and Challenges 5
4 Copyright 5

Related Research Documents

Advisory Note: Information Security Predictions and Recommendations 2015 and beyond - 71045

Executive View: Axiomatics Policy Management Suite - 70895

Advisory Note: Database Governance - 70102

Technology Report: XACML – Extensible Access Control Markup Language

This document is restricted for personal use of Michael BÃ¼rger
Downloaded from KuppingerCole on 30.11.2015 20:50

1 Introduction

The need to provide access to corporate data is increasing rapidly these days. Corporations are realizing they have rich data repositories that they need to leverage for business processes and to drive business value. Many organizations have migrated from a CIO who looks after information technology (IT) to a CDO (Chief Digital Officer) who transcends IT, knows how data supports business processes and has the seniority to make change happen.

But therein lays a problem. As more people want access to more data from more places via more devices, the need to address data security increases exponentially. It is now more important than ever to know more about a request for data. In the past we could just check someone was in the right AD group and then grant them access to the data repository. Now we need to check their rating relative to the classification of the requested document, the location from which they are accessing the data, the state of the device they are using, their current job responsibilities and the time of day before deciding how much data to release.

Increasingly organizations are requiring certain data to be masked or redacted when granting access to a document. The need is to release as much information as possible without contravening data sovereignty regulation and corporate governance requirements.

In the past it would be necessary to deploy a complex solution to mask data, manage access tokens and complex data encryption to provide protection of shared data. It is now possible to achieve an unprecedented level of control using adaptive, policy-based access management. User access to data is granted, in real-time, via a set of policies that determine the level of access that a user should receive.

One company with an innovative solution for this requirement is Axiomatics.

Axiomatics are a long-time supplier of attribute-based access management software and a major player in the standards-setting that has driven the development of this industry sector.

Recently they have incorporated an innovative feature into their attribute-based access management solution that will intercept an SQL query and apply policies to the response that determines what can be displayed for the user and, more importantly, what must be masked or redacted.

Axiomatics Data Access Filter allows access to corporate information to be governed by corporate policies and government regulation rather than IT staff. Governance becomes centrally managed across all applications and data repositories, providing consistence and corporate control. These benefits are achieved without changes to the corporate databases or the addition of software to handle the interface to the authorization server.

2 Product Description

Axiomatics is a major player in the attribute-based access control market segment with their flagship Axiomatics Policy Server product that provides a standards-based policy authorization service for relying applications. It provides a way for business units within an organization to create and administer policies to manage access control to protected resources. For instance, if a user wants to access the organization's accounts payable ledger the Policy Server could be used to evaluate a policy that ensured access was only provided to staff in the Finance Department, who had a role of purchasing clerk, who was on the organization's internal network and was requesting access during business hours.

This functionality has been extended with the release of the Axiomatics Data Access Filter, which provides the same fine-grained access management to control access to database entries.

A typical configuration for web applications these days abstracts the presentation, application and backend layers in 3 (or more) tier arrangement. The webserver renders content and supports load balancing of user sessions, the application layer contains the application logic and performs the requested service, and the backend system provides database services and optimizes search and transaction functions:

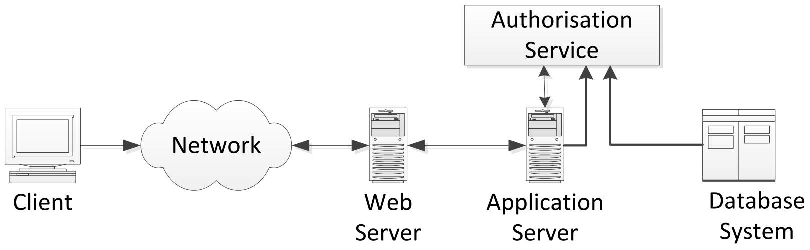


Figure 1 - 'N-tier" Configuration

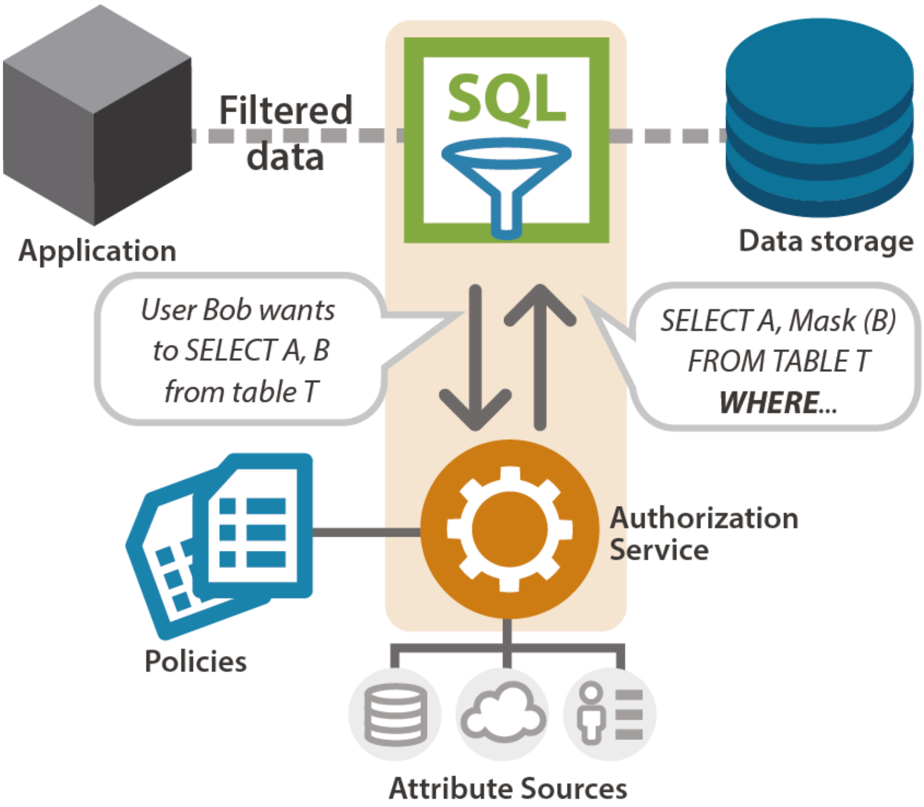
When a user requests access to the application they are typically authenticated to the web service i.e. are they in the correct AD group? If the application uses an authorization service the authorization step determines the user's permissions within the application i.e. are they the Finance Manager?

In an interesting extension to this functionality the Axiomatics Data Access Filter provides an authorization function to the database access management task. When a user requests access to a protected piece of data in a database it is now possible to evaluate a set of policy's to determine the level at which access should be granted. For instance a British Army corporal might have Defense Secret Network access in the USA but would not be able to see documents classified US eyes only. This would be achieved by the Authorisation server querying the user's "nationality" attribute before granting access to the protected document, or portion of the document.

The result of the request can be quite sophisticated. Access can be denied outright, access to certain rows can be restricted or data elements can be masked or redacted. For instance, the Regional HR Manager in Boston might only be allowed to see the salary levels of East Coast employees and his counterpart in Los Angeles would only see salaries of West Coast staff. While database entries for staff across the company can be displayed for both managers, salary details for staff not in their region can be redacted.

This document is restricted for personal use of Michael BÃ¼rger
Downloaded from KuppingerCole on 30.11.2015 20:50

Another useful application of this technology is adherence to privacy legislation. In many cases countries have rules governing the storage and display of data about their citizens in off-shore locations. For instance, Australia restricts storage of personally identifiable information (PII) on Australians in any jurisdiction that does not have similar privacy laws to Australia. That means that cloud storage on Singapore could be used but a storage service in Indonesia could not be used. If data was to be made available to an Indonesian call center restrictions on the data to be displayed would need to be enforced. The Axiomatic Data Filter could be used to enforce a policy whereby call center staff in Indonesia would not get access to a user's date-of-birth, for instance.



The system uses an "SQL intercept" method whereby each SQL query is forwarded to the Authorization server which evaluates and modifies the SQL statement in accordance with the applicable rules established by the policies.

The modified SQL statement is then sent to the database and only data the user is authorized to access is returned.

The modification of the SQL statement, policy evaluation and the associated attribute look-ups all happen in real-time.

This means that modification to a policy set, or a change to a user's attributes, will modify the next look-up and be reflected in the data returned when the user accesses the protected database.

3 Strengths and Challenges

The main strength of Axiomatics' Data Access Filter is at the business level. A way to unlock business value in an organization's data assets can directly improve productivity. The product can directly impact business processes significantly speeding up the velocity of business transactions.

Obvious benefits are the ability to make context-aware access decisions; if a user is using a mobile device, or accessing restricted data late at night, appropriate controls can be enforced.

The fact that the access decisions are made in real-time mean that as soon as a user's attributes are modified, decisions based on those attributes with reflect the changes.

Changes to in business rules are made once, and via a single administrative tool. Management can be distributed but policy management remains central. This means that other access control tools interfaced to the same policy store will be consistent.

Because the product follows the XACML standard – up to the current draft of 3.0 - very closely, it is very adaptive towards complex access control requirements.

The XACML policy language defines three top-level policy elements: Rule, Policy and

The two main components of the product: SQL Proxy Server and SQL Filter Server are supporting in both the Windows environment (2008, 2012) and LINUX (Redhat Enterprise V5 or 6). Currently supported databases are Oracle (11g, 12c), IBM DB2 (9.5, 9.7) and MS SQL (2008, 2012).

Strengths	**Challenges**
● Leverages the mature, Axiomatics Policy server technology. ● Significant experience in large XACML configurations. ● Global partner ecosystem with ability to deliver in most geographies. ● Support for the major enterprise database environment.	● DBA reticence to support a proxy server configuration ● Potential performance constraints in transactional environments ● Policy proliferation with data-masking and redaction features

4 Copyright

© 2015 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

This document is restricted for personal use of Michael BÃ¼rger
Downloaded from KuppingerCole on 30.11.2015 20:50

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com