An Oracle White Paper
August 2010

Oracle Adaptive Access Manager 11g
Architecture & Technical Specifications
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Overview</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Moving Beyond Traditional Authentication</td>
<td>2</td>
</tr>
<tr>
<td>Flexibility</td>
<td>2</td>
</tr>
<tr>
<td>Cost-Effective Online Threat Protection</td>
<td>3</td>
</tr>
<tr>
<td>OAAM Risk Engine</td>
<td>4</td>
</tr>
<tr>
<td>Auto-Learning</td>
<td>4</td>
</tr>
<tr>
<td>Configurable Risk Engine</td>
<td>5</td>
</tr>
<tr>
<td>Universal Risk Snapshot</td>
<td>5</td>
</tr>
<tr>
<td>Universal Installation Option Reverse Proxy</td>
<td>10</td>
</tr>
<tr>
<td>Native Application Integration</td>
<td>10</td>
</tr>
<tr>
<td>Web Services Application Integration</td>
<td>10</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>11</td>
</tr>
</tbody>
</table>
Executive Overview

Businesses, institutions and end users face the growing threat of fraud and abuse. Failure to comply with industry security regulations can severely hurt the bottom line. As well, deploying an incomplete security solution can be very costly in the short and long terms. Security professionals need a strong, flexible and cost effective solution to meet their current needs and be able to scale to meet their future needs without breaking the bank. Oracle Adaptive Access Manager provides powerful, unique, transparent and flexible protection for organizations and their users through its core capabilities and deep integrations with the other Oracle Identity and Access Management suite. This white paper describes in detail the features and benefits Oracle Adaptive Access Manager provides customers.

Introduction

Users and organizations lose when fraud occurs. Increasing sophistication and speed of fraud attacks and expanding regulations require a new type of security solution with capabilities beyond narrow and outdated static and reactive methods. Such a solution must take a holistic view of each individual application, event, transaction, user and access request in real-time. It is no longer enough to simply authenticate users or passively detect fraud and abuse; they must be prevented before they can occur. An effective security solution must quickly evaluate risk and confirm identities by validating multiple types of data, all with minimal need for human intervention. Oracle Adaptive Access Manager captures profiles and processes the full context of a situation to determine the level of risk. The level of risk automatically determines what if any actions the system must take to prevent an incident. The ever changing variety of fraud attacks and corporate misuse requires a solution to have varied areas of functionality and flexibility to adapt to evolving threats quickly. Threats such as social engineering, phishing, malware, trojans, viruses, session hijacking, man-in-the-middle, man-in-the-browser and many others must be prevented and mitigated if a solution is to have real value. As well, insider fraud such as role abuse and fraudulent impersonation must be preventable. Oracle Adaptive Access Manager includes functionality to protect the entry and transmission of static authentication credentials, fingerprint devices used, profile user behavior, assess situational risk in real-time, challenge or block users based on the current level of risk, full audit, reporting and investigation capabilities.
Moving Beyond Traditional Authentication

Authentication processes have many weaknesses:

- It is not uncommon to transmit users’ credentials in clear text. Moving raw data over open channels increases the likelihood of credentials theft.

- Even with SSL in place, the credential data remains unencrypted from the moment user enters it until the encryption process gets invoked. When the user’s device/browser is compromised, SSL becomes useless.

- No matter how much security is in place, organizations can’t control the end users computer. Every day, consumer and business applications are being accessed from thousands of devices compromised by key-loggers and other types of malware.

- Even multi-factor authentication alone cannot prevent fraud from occurring. For example, session hijacking happens after primary authentication is successful.

- Over compensation by requiring users to re-authenticate in-session when there is little risk impacts employee productivity and infuriates customers.

- Insider fraud is not prevented by authentication alone since often the individual committing fraud is the valid user the enterprise provisioned the credential to.

Oracle Adaptive Access Manager was designed with the goal to overcome these limitations and to enable strong protection for the enterprise and its employees/partners/contractors/customers even if they are accessing from a compromised environment.

Flexibility

Oracle Adaptive Access Manager was architected from the beginning as a platform rather than a point solution. The OAAM design philosophy offers a unique set of flexible capabilities to our customers and partners. Customers have the choice to use the complete out of the box solution provided or develop a fully custom solution harnessing OAAM or a hybrid of the two. A highly configurable risk engine, customizable reporting, real-time, listener and batch based deployment options, powerful configurable actions to implement fully custom solutions without any core product change, as well as our all new shared libraries infrastructure and challenge processor framework allows almost unlimited deployment possibilities. As well, the highly configurable transaction monitoring, behavioral profiling,
risk evaluation and other policy management tasks are all exposed in a brand new intuitive 11g GUI for easy access by business users. Backing up all the flexible capabilities of OAAM is the strength and stability of the Oracle stack and infrastructure. Oracle Adaptive Access Manager upakes common Fusion Middleware components along with the other Identity and Access Management products so install, patching, upgrades, diagnostics, management, audit, logging, reporting, security, UI frameworks and support organization are all common. In other words, OAAM is a truly enterprise grade product complete and open enough to meet the needs of any organization.

Oracle’s strategy with OAAM is to provide base policies and rules to meet the access security requirements of any application in any vertical for any type of user base. Each deployment then will have specific policies and rules configured based on the unique security needs of the specific applications and user groups. This configuration is either performed by customers using Oracle documentation or buy expert professional services or a combination of the two. In this way Oracle provides a flexible and effective fraud prevention solution that can meet the needs of any business regardless of vertical or market. Based on our competitive intelligence, this is a very complete and preferable option for many customers.

Cost-Effective Online Threat Protection

Oracle Adaptive Access Manager offers many diverse benefits with an exceptionally low cost of ownership. Considering that OAAM provides device fingerprinting, real-time behavioral profiling and risk analytics, risk-based authentication methods including Knowledge Based Authentication challenge infrastructure including Answer Logic, OTP Anywhere server generated one time password delivered out of band via SMS, email, IM or voice channels, real-time and batch based enterprise fraud detection in a single license. Also, that all of this includes out of the box integrations with the industries top identity management and web single sign on products. The value is especially striking when considering the collection of point products and integration effort that would be required to furnish similar functionality.

With Oracle Adaptive Access Manager, corporations can defend themselves and their end users against the most potent fraudulent attacks in a cost-effective manner.

<table>
<thead>
<tr>
<th>THREAT</th>
<th>OAAM DEFENSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>• A phishing site cannot easily replicate the user experience of the virtual devices (TextPad, QuestionPad, KeyPad, PinPad). As such, users will be tipped off and most likely not enter their password or PIN code.</td>
</tr>
<tr>
<td></td>
<td>• The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server. If the shared secret is not presented or presented incorrectly users can be tipped off.</td>
</tr>
<tr>
<td></td>
<td>• The “freshness” time-stamp displayed in the virtual devices shows an end user that it was created right then for their use. This makes re-presenting old virtual devices on a phishing site suspect to an end user.</td>
</tr>
<tr>
<td></td>
<td>• If a phishing exercise is successful in stealing users login credentials, real-time</td>
</tr>
</tbody>
</table>
risk analytics, behavioral profiling and risk-based challenge make using stolen credentials very difficult since the fraudster will most certainly not have exactly the same behavior as the valid user and therefore would be challenged or blocked by OAAM.

Malware
- The Virtual Authentication Devices combat key-loggers and many other forms of malware that attempt to steal a user’s authentication credentials.
- The KeyPad and PinPad allow a user to send a random string of numbers instead of their actual credential. As a result no sensitive data is entered or sent to the server so it is not easily compromised by automated means.
- The same technology can be used to protect any sensitive data point. For example, a user’s Social Security Number could be safely communicated to a server by entering it using the Virtual Devices.

Transaction Fraud
- Oracle Adaptive Access Manager performs both real-time and batch based risk analysis on session, transaction, event and contextual data.
- Possible outcomes of these evaluations include alerts, blocking, risk-based challenge or custom integration actions to affect other systems.
- Virtual Devices can be implemented to prevent automated navigation of transaction interfaces and data altering by malware programmed to hijack user sessions post login. For example, if a PinPad is used to enter the destination account number of a transaction malware cannot easily navigate this process and the random data entered and sent is not the actual account number so it cannot be altered for fraud.

Insider Fraud
- Oracle Adaptive Access Manager profiles user behavior and assesses the risk associated with an access request in real-time. If an employee/partner/contractor exhibits anomalous behavior alerts can be generated for security and compliance analysts to review.
- Risk-based KBA or OTP challenge can thwart fraudulent impersonation.

OAAM Risk Engine

Auto-Learning
Oracle Adaptive Access Manager employs unique real-time auto-learning technology to profile behavior and detect anomalies in real-time. Because of this OAAM can truly spot high risk and proactively take actions to prevent fraud and abuse. As well, since OAAM is evaluating and learning behaviors in real-time it is constantly learning what is “normal” for each individual user and for users as a whole.

A simple example would be the behavioral profiling and evaluation of access times for a nurse. If she works in a hospital she may work different shifts on occasion to fill in but she will most likely work one shift more than the others in any given month. As such OAAM will keep track of when she is at work accessing the medical records system. If this month she has been working mostly PM shifts and some graveyard shifts to fill in then seeing an access request from her between 10:00 am and 12:00 pm would be an anomaly. This of course does not mean fraud is occurring but the risk is elevated so
asking a challenge question would help confirm it's really her. As she makes more access requests during the day shift OAAM learns in real-time that this is normal for her. This however is a simplistic example of one data point in isolation when in reality OAAM is learning and cross referencing large numbers of data points for each request and evaluating them for anomalies.

One of the main goals of automated anti-fraud solutions is to do away with unnecessary manual processes and remove much of the inconsistency and costs that can occur when humans are directly involved in evaluations. Oracle Adaptive Access Manager automates not only risk evaluations but as well keeps track of changing behaviors so humans don’t have to. Based on this dynamic risk evaluation proactive action is taken to prevent fraud with various forms of interdiction including blocking and challenge mechanisms. In this way OAAM prevents fraud with little or no need for human interaction.

Configurable Risk Engine

The Oracle Adaptive Access Manager risk engine utilizes a flexible architecture based on highly configurable components. Administrators can easily create, edit and delete security policies and related objects directly in the intuitive administration console. Non-technical users can administer OAAM policies, view dashboards and reports in the graphical user interface with little or no dependence on IT resources. Security rules are easily created by combining configurable rule conditions. Both access and transaction based rules are created from the library of conditions included out of the box. As well OAAM profiles behavior and evaluates risk using a fully transparent and auditable rules based process. This allows high performance, flexibility and complete visibility into how and why specific actions were or were not taken during a session. This is in stark contrast to opaque solutions that rely heavily on predictive technology where the exact cause of outcomes cannot be exactly determined. If a “black box” blocks access for an end user there is little way of knowing exactly why. In addition to transparent, self sufficient and flexible functionality OAAM customers also enjoy enthusiastic innovating product development teams, 24/7 global support and an active user community.

Universal Risk Snapshot

Change control is very important in an enterprise deployment, especially concerning mission critical security components. The new Universal Risk Snapshot feature allows an administrator a single operation to save off a full snapshot of all Oracle Adaptive Access policies, dependent components and configurations for backup, disaster recovery and migration. Snapshots can be saved to the database for fast recover or to a file for migration between environments and backup. Restoring a snapshot is an easy process that includes visibility into exactly what the delta is and what actions will be taken to resolve conflicts.

Device Fingerprinting

Oracle Adaptive Access Manager contains proprietary clientless technologies for fingerprinting and interrogating devices used during access requests and transactions. There is no client software or logic required which limits the burden on the end user and does not expose anything to be compromised. OAAM generates a unique single-use fingerprint and marks a device for each user session. It is replaced upon each subsequent fingerprinting process with another unique fingerprint. The
fingerprinting process can be run any number of times during a user session to allow detection of changes mid-session that can indicate session hijacking. OAAM monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted. The single-use capabilities combined with server-side logic defends against the fingerprint being stolen and reused on another machine to commit fraud.

Virtual Authentication Devices

Oracle Adaptive Access Manager includes unique functionality to protect end users while interacting with a protected web application. The Virtual Authentication Devices harden the process of entering and transmitting authentication credentials and provide end users with verification they are authenticating on the valid application. This is accomplished without any proprietary client-side software or hardware required. Only standard web technologies including HTML and simple JavaScript are used. This is because all logic is on the server not on the client where it is vulnerable to exploitation.

TextPad

TextPad is a personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing primarily. TextPad is often deployed as the default for all users in a large deployment then each user individually can upgrade to another device if they wish. The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server. If this shared secret is not presented or presented incorrectly users will notice.
PinPad & KeyPad fig. 2

PinPad and KeyPad are indirect authentication credential entry devices. They can be invoked at the time of login or in-session if required. A user navigates using their mouse to click on the visual “keys”. In reality the data entered is a string of random numbers that only the OAAM server can decode into the valid password/PIN/data. The PinPad and KeyPad are generally given as an optional upgrade users can choose to use or not. This flow ensures only users who really want the extra protection utilize it since there is a slight learning curve related to navigation.

QuestionPad fig. 3

QuestionPad is a specialized device only used to present KBA challenge questions to an end user. The question text is protected from screen scrapers since it is actually contained in the image file rather than HTML text.

KBA Answer Logic

Oracle Adaptive Access Manager includes a highly usable challenge method we call Knowledge Based Authentication (KBA). What makes KBA superior to other registered challenge question solutions is the usability provided by KBA Answer Logic. Administrators can easily configure the exact end user experience they require including individual question creation/editing, how many questions users register for, the variety of questions they can choose from and specific validations to be applied to the answers they give. Also, with KBA Answer Logic administrators adjust how exact the challenge answers given by end users must match the answers they gave at the time of registration. If the answer given by a user is fundamentally correct but there are minor variations such as typos, misspellings and typos they should pass. Answer Logic dramatically increases the usability of KBA which reduces or eliminates the need for unnecessary call center involvement in moderate risk situations and self service flows. KBA Answer Logic is a collection of multiple techniques detailed here.

Common Abbreviations & Nicknames

This algorithm matches the words in the following pairs as equivalent. OAAM ships with a predefined list of word-pairs that cover common abbreviations, common nicknames and common acronyms. The list can be customized by updating properties.

- Street - St.
- Drive - Dr.
Date Format
When users answer a date related challenge question sometimes they use a different date format than they did when they registered the question. Answer Logic can translate from one format to another to allow variation in fundamentally correct answers. For example, the following would be seen as the same answer:

- 0713
- 713
- July 13th
- July 13

Common Misspellings
Phonetic Answer Logic can account for minor misspellings and regional spellings.

- elephant – elefant
- color – colour

Keyboard Fat Fingering
Fat Fingering Answer Logic accounts for typos due to the proximity of keys on a standard keyboard and transposed letters. The following are some common typos.

- Switching "w" and "e"
- Switching "u" and "i"
- Switching "t" and "r"
- Correct word: signature - Fat finger: signatire

OTP Anywhere
OTP Anywhere is cost effective risk-based challenge solution consisting of a server generated one time password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), eMail, instant messaging and voice. OTP Anywhere can be used to compliment KBA challenge or instead of KBA. As well both OTP Anywhere and KBA can be used alongside practically any other authentication type required in a deployment. Oracle Adaptive Access Manager also provides an innovative challenge processor framework. This framework can be used to implement custom risk-based challenge solutions combining third party authentication products or services with OAAM real-time risk evaluations. Both KBA and OTP Anywhere actually
utilize this same framework internally. Example authentication implementations are provided to customers as a starting point for developing custom implementations and integrations.

Oracle Adaptive Access Manager Architecture

Oracle Adaptive Access Manager is architected to provide a rich selection of capabilities with heterogeneous support for a variety of environments. Functionality is implemented to optimize resources and provide enterprise class scalability and redundancy.

High Availability

Oracle Adaptive Access Manager is architected to ensure dependable uptime performance in demanding deployments. The runtime components including the rules engine and end user UI flows are contained in one managed server while the administration console functionality is separated out into its own managed server. The administration console contains the customer service and security analyst case management functionality which must always be available to employees in potentially large call centers with high call volumes. The two managed servers do not communicate with each other as was the case in previous versions of the product. Depending on the deployment method used the topology changes slightly. Native application integration deployments embed the runtime components so the administration console is the only additional managed server added to the deployment. Oracle Adaptive Access Manager is also completely stateless and fully supports clustered deployments to meet high performance requirements. As well, all high availability features of the Oracle database are supported for use with Oracle Adaptive Access Manager.
Deployment Options

Oracle Adaptive Access Manager supports a number of deployment options to meet the specific needs of practically any deployment. The decision of which deployment type to employ is usually determined based on the use cases required and the applications being protected.

Single Sign-On Integration

Oracle Adaptive Access Manager has an out of the box integration with Oracle Access Manager to provide advanced login security including the virtual devices, device fingerprinting, real-time risk analysis and risk-based challenge. New to 11g there are two versions of the OAAM + OAM integration, basic and advanced. The “basic” integration embeds OAAM into the OAM runtime server. It includes many of the login security use cases available from OAAM and reduces the footprint. To gain advanced features and extensibility customers can deploy using the “advanced” integration. Features such as OTP anywhere, challenge processor framework, shared library framework and secure self-service password management flows require the advanced integration option. Oracle Adaptive Access Manager can also be integrated with third party single sign-on products via systems integrators if required.

Universal Installation Option Reverse Proxy

Oracle Adaptive Access Manager can be deployed using an Apache module to intercept login requests and provide advanced login security. The flows available are the same as for the advanced single sign-on integration option described above. The main benefit of the UIO proxy deployment is that there is no need to touch the protected applications and SSO is not required.

Native Application Integration

Oracle Adaptive Access Manager can be natively integrated with an application to provide extreme high performance and highly customizable security. A native integration embeds OAAM in-process inside the protected applications. Advanced transactional risk analysis requires this form of deployment. Deployments with many millions of end users and large volumes of transactions to be evaluated often choose this route.

Web Services Application Integration

Customers who have advanced requirements similar to native integration but who prefer to use SOAP web services instead of Java API integration directly can choose this option.
CONCLUSION

Oracle Adaptive Access Manager offers the unique and powerful advantages that you expect of the next generation of risk-based access management. The unique combination of truly real-time anti-fraud capabilities found in Oracle Adaptive Access Manager and the completeness of the Identity and Access suite offering will greatly benefit any customer. The flexibility and transparency of the solution help provide a good return on investment. And finally, the vision and support provided by Oracle ensures that customers do not have to worry about the longevity of the solution they choose.