DirX Access

Risk-based Authentication

Evaluating contextual factors to estimate and mitigate risks related to access requests

DirX Access is a comprehensive access management and identity federation solution. Starting with version 8.5, the capabilities of DirX Access have been enhanced by adding risk-based authentication (RBA), also called adaptive authentication.

RBA has recently become a new must-have for IAM products like DirX Access that provide authentication and access management. DirX Access incorporates RBA into its main decision-making mechanism, making it readily available for use when evaluating any request.

From a technical standpoint, RBA evaluates the potential risks connected with every interaction between the user (also called an agent) and the system. These risks must be offset by a sufficient level of confidence – assurances – regarding the user's identity. If these assurances cannot be made, additional actions must be taken, such as advanced authentication, auditing or request denial.

Any resource can be assigned one or more risk conditions as well as a sensitivity level. The risk conditions evaluate the request data either generally or at a user-specific level. The general approach allows administrators to define risk factors like lists of malicious IP addresses and other static policies. The user-specific approach takes the user's behavior patterns into account and raises the risk level when it detects a behavioral inconsistency, such as a request from a different geolocation or at an unusual time of day. The resource sensitivity approach allows administrators to increase the assurances needed to access a particular resource.

Motivation

When speaking about securing any enterprise solution, identity verification is one of the main problems to solve. The process of identity verification must be secure, reliable and user-friendly.

Confidence Provided by Authentication Methods

The methods of authenticating a user to a system generally fall into three categories, or factors, depending on the type of information in use: knowledge (a password, a PIN or the answer to a challenge), possession (a smart card or a mobile phone), and inherence (a fingerprint or face).

Any authentication method achieves a level of confidence connected with its use; the particular levels are highly dependent on the method's factor. Security officers should be responsible for designing appropriate policies for evaluation of available authentication methods. The policies then determine the appropriate authentication methods for the intended use. This process results in assigning a number to each authentication method to represent the confidence for the purposes of processing with RBA. By combining multiple authentication methods, usually of different factors, the confidence in the combined solution can surpass its respective components. This approach is called multi-factor authentication.

Measuring Risks from User Data

Earlier, we mentioned each user's interaction is connected to risks evaluated according to the risk conditions. We can also look at this from the opposite point of view – the unfulfilled risks being the fulfilled assurances. We fix the amount and nature of the data that the user sends to the authentication system and then try to retrieve as much useful information from this data as possible. This process provides very good results thanks to the use of big data and machine-learning techniques. This represents the idea that authentication is in fact a machine-learning process. This idea emerged several years ago and is gaining popularity in the industry. The major market players have deployed the machine-learning approach to authentication into their IAM products, usually under the name of risk-based or adaptive authentication.

Bull
atos technologies

RBA: Benefits and Trade-offs

DirX Access RBA addresses the typical issues connected to the process of authentication of information system users:

- Achieving sufficient confidence in the claimed user's identity.
- Reducing the use of laborious methods of authentication.
- Preventing the necessity of costly solutions.

This is achieved by the built-in evaluation mechanism, when RBA collects all possible risks connected with a user request on the protected system and then compares them to the assurances given by the authentication methods. These risks have several different forms: risks known in advance (for example, a request from a malicious IP address), risks connected with unexpected data (user behavior), and risks connected with requesting a resource that demands a higher level of protection (resource sensitivity). This last form implies that the DirX Access solution is **resource-sensitive**.

Not only does the behavioral approach identify the risks; it also provides additional assurances regarding the claimed identity. In this way, RBA represents a supporting **continuous behavioral authentication method**. Some of the evaluations that RBA performs are truly based on a user's past behavior.

The behavioral data cannot be used to unambiguously identify a user; however, they increase the confidence in the claimed identity. By contrast, if the user deviates from the expected behavior, the confidence in the claimed identity decreases, and the system can challenge them with additional authentication directives. In this way, RBA enables an optimal trade-off between security and user friendliness.

RBA is able to utilize the information about the device used for interaction with the system for authentication purposes. If such a device is in the exclusive possession of the user, RBA might serve as the **possession authentication method**.

The basic part of the RBA mechanism is formed by general risk conditions that are user independent. These conditions can be used for **known threats prevention**. Examples include denying access from malicious IP addresses or at unexpected times.

Contrary to the static policies, such as minimal password length or official working hours, user-specific part of RBA represents a more dynamic way of evaluation. The enterprise security policies are applied here with respect to the assessment of statistical outcome. With this in mind, RBA informs the system administrator about, for example, the percentage of user requests that cause additional interaction (step-up authentication) between the user and system. Based on this assessment, the administrator can change the RBA policies to meet the enterprise goals.

One of the major advantages of RBA is that there are **no additional costs or actions on the user side**. For almost all authentication methods, some deployment action must be taken for any new user: the password must be memorized or the smartcard must be issued. And during the authentication process, some explicit action from the user is needed, resulting in a delay, a help desk call, and so on. With RBA, the only requirement is enough space and computational power. The mechanism is immediately applied to any user without any explicit interaction required.

System Overview

The traditional authentication process is perceived as an initial action that provides us with the user's identity. The identity subsequently remains unquestioned until the end of the session.

Risk-based authentication is a new component of an authentication process that introduces two substantial improvements. The first is **decision set extension**: instead of providing only the authenticated/denied state, RBA outputs a relative measure of the risks connected with the trust in the resolved identity (which can also be seen as a confidence in the identity claim). The second improvement lies in the extension of its applicability to any user request: with RBA, authentication becomes a **continuous process** of recalibrating the risk level to respond to new important information about the user's behavior that may be contained in any new request.

Risk Evaluation

The compound estimation of the risks is **user-**, **request-**, and **resource-dependent**. For every resource, a set of conditions is defined and subsequently applied during the evaluation process. Each condition assesses relevant request- and user-related data and outputs a single number that represents the estimated risk. In DirX Access, the interval from which this number is drawn is configurable to reflect both the environment specifics and the enterprise security policy. The conditions are mutually **independent**, so they are evaluated separately and the outputs are summed into the final **risk level**.

Another RBA system variable is the **assurance level**. Every authentication method has its assurance level configured. The user's authenticated state contains the assurance level granted by the most secure authentication method used.

On each request, the assurance and risk level are compared. If the risk level is higher, additional authentication actions are invoked.

User Perspective

As mentioned earlier, RBA evaluation does not demand any explicit user interaction. If RBA determines that the authentication is insufficient, an action is taken depending on the system policy. By default, the request is **denied**. Optionally, DirX Access can employ the Authentication Application component to allow legitimate users to provide stronger evidence of their identity. Instead of a simple denial, the user is redirected to the Authentication Application and provided with all the authentication methods that have an assurance level that is high enough to balance the risks, a process called the **challenge** approach. All of the RBA mechanism's actions are also **logged**.

As we can clearly see here, an important part of the RBA-enabled system is a **wide range of authentication methods** that allow for the establishment of different levels of trust. DirX Access addresses this

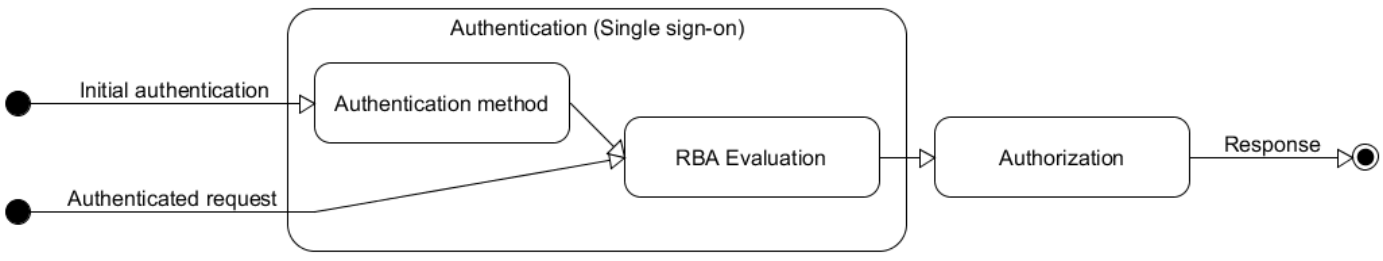

Figure 1: Risk-based authentication system in the context of request processing

issue by offering a large number of directly-implemented methods, including password-based (customizable form, basic), possession-based (X.509), one-time passwords (RFC2289, RFC4226, RFC6238) and more. The number of methods is even extended by the support of identity federation standards (SAML, OAuth) and the ability to wire any custom solution into the system using a dedicated customization interface.

General Risk Conditions

The general type of risk condition represents the evaluation that is **request-dependent** only. When targeted on one of the defined resources, the request data (being from an arbitrary user) are evaluated using the relevant condition. The condition is either satisfied or violated, with violation leading to the increase of the risk level by a defined value.

In addition to the built-in conditions, DirX Access allows including a custom condition solution, thanks to a customization interface.

Known Threats Prevention

Because general risk conditions are user-independent, they can be seen as prevention against known threats. DirX Access RBA can track three different features: **IP addresses**, **time ranges**, and **HTTP protocol headers**.

Tracking malicious IP addresses is a common approach to attack prevention. There are a number of publicly-accessible lists that can be easily included into the risk condition configuration. The administration tool DirX Access Manager allows the administrator to enter the addresses either directly or by ranges. When using ranges, RBA can also be used to privilege the well-known addresses (for example, from the corporate network).

Resource Sensitivity

As mentioned earlier, RBA demands a certain level of confidence (assurances) regarding the user's identity to balance the risks. The **resource sensitivity** type of risk condition can be used to explicitly increase the level of confidence needed to access particular resources.

Having in mind the purist approach to configuration of risk conditions, this is a very important risk condition type. Ideally, we would like to have all defined conditions applied when requesting any resource and the only resource-dependent setting would be achieved by this condition type. In practice, however, it's not important to evaluate all conditions in all cases, so some conditions can usually be omitted to improve performance.

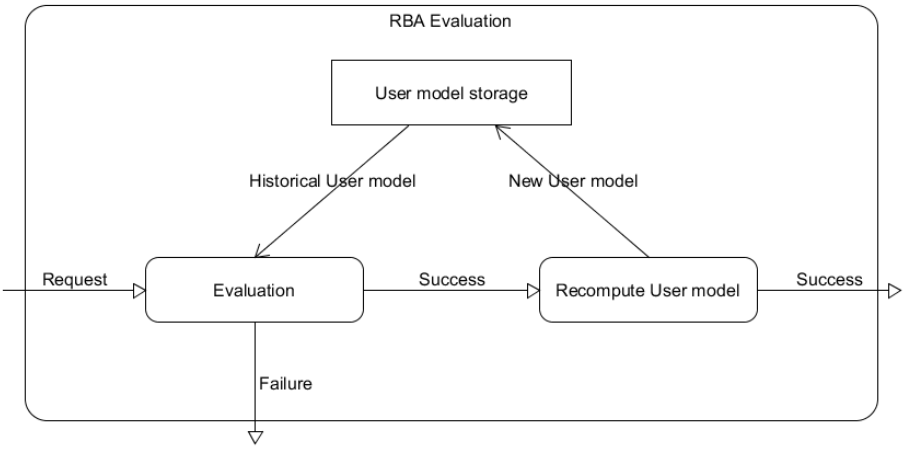

Figure 2: RBA evaluation of user context-aware conditions

Login Failures and Login Interval

Although we consider them to be general risk conditions, the login failures and login interval risk conditions are somewhat special in that they depend on several user-specific parameters: login failures on the number of subsequent login failures (incorrect credentials use) and login interval on the interval since the last successful login.

The login failures condition enables a more fine-grained approach to **account locking** by softening the hard limit of unsuccessful attempts allowed. The hard limit can be increased while the condition may enforce the use of stronger authentication methods after a lower number of attempts.

User context-aware Risk Conditions

The user context-aware (UCA) risk conditions represent a very powerful mechanism. They fully leverage **user-dependency** to model user behavior and then perform a risk-level assessment on the model. The underlying algorithms employ several machine-learning techniques and principles according to the structure of the data used for the evaluation.

Each UCA risk condition by itself gives the relative confidence (risks) connected with the evaluated data. The evaluation output needs to be able to express this fact. Hence, the output of the UCA risk condition evaluation can be drawn from the values in the continuous interval to the defined risk level.

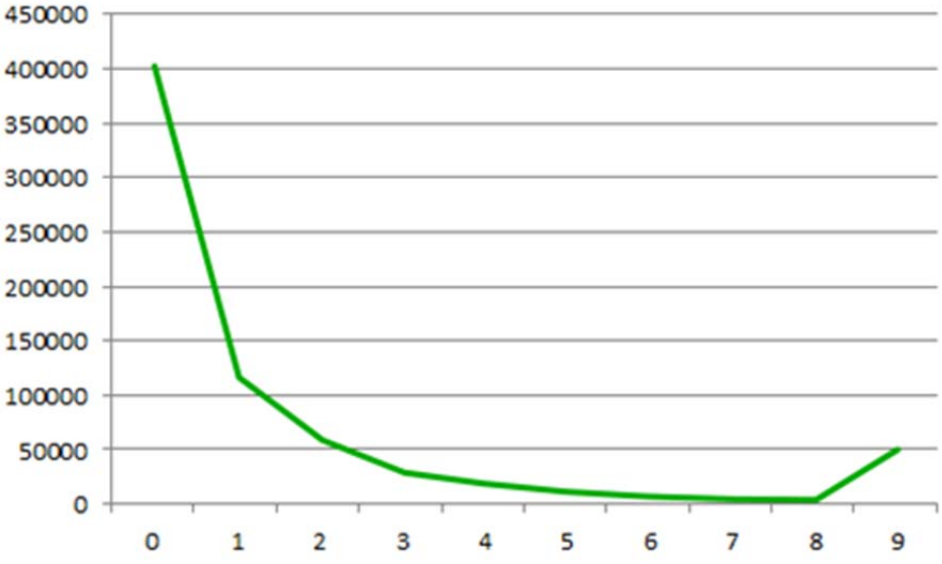

Figure 3:
The distribution of the risks (x-axis; minimal 0; maximal 9) for the access time data. Y-axis shows the number of requests evaluated for the corresponding risk level.

Learning Process

DirX Access employs the received user-specific data that can be used in UCA RBA in the learning phase. These data update the **user model** that is subsequently used during the evaluation. The entire process is highly configurable due to performance reasons and the need to address the specific data dependencies. Examples of configuration options include the learning frequency during the user session and the data expiration time.

The data learned during one session are propagated into the user model at the end of the session and are then employed within the evaluation of the subsequent session.

Risk Evaluation Process

For each UCA risk condition, the evaluation phase takes the relevant data from the user model and operates on them according to its internal algorithm.

The system allows for configuring arbitrary UCA risk conditions. On the other hand, determining the relevance of a particular condition type with a particular configuration can be a complex task that can be eased somewhat by understanding the requirements and constraints on UCA RBA.

The main intuitive requirement is this: Assign the minimal risk level to any legitimate interaction between a legitimate user and the protected system. The simple solution to this requirement is to assign the minimal risk level to any interaction. As a result, the second requirement is this: Assign the maximal risk level to any interaction between the illicit user and the system. The problem is that we do not know the true distribution of the legitimate and illicit requests. To determine it, we use the very machine-learning mechanism at the core of the evaluation process. This process, however, transforms the initial requirements into this: Assign the risk level in proportion to how close the evaluated data are to the data expected for the legitimate user. UCA RBA handles the security aspect – the resilience against illicit requests – internally. Conversely, administrators can monitor the correct resolution of legitimate user requests and should leverage this information to determine the condition configuration. Figure 3 shows the risks determined for legitimate user requests by evaluating access times (in a real deployment). We can see that the evaluation gets closer to granting the minimal risk level most of the time. The tail of the graph shows the peak for the maximal risk level, which is due to learning a new and previously unobserved user behavior. Considering usability, the distribution seen in Figure 3 is approximately the one to look for when designing an efficient condition.

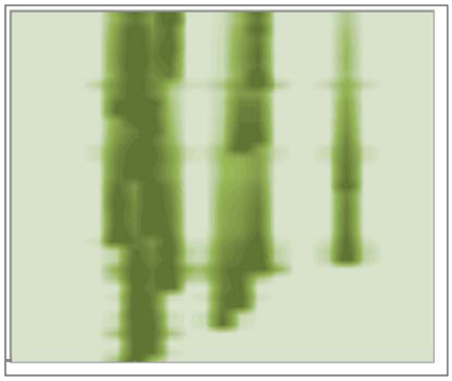

Figure 4:
The potential risk levels: the darker the color, the smaller the risk,
X-axis = authentication time,
Y-axis = number of interactions of the legitimate user with the system.

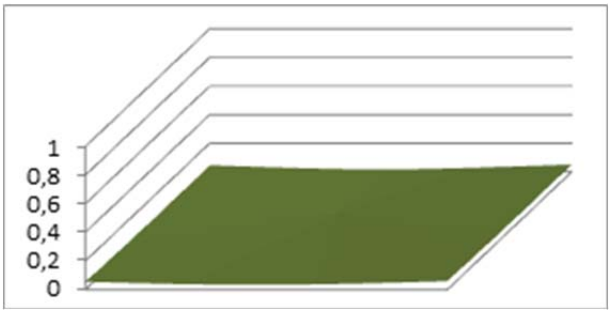

Figure 5:
After the first interaction: RBA is tolerant.

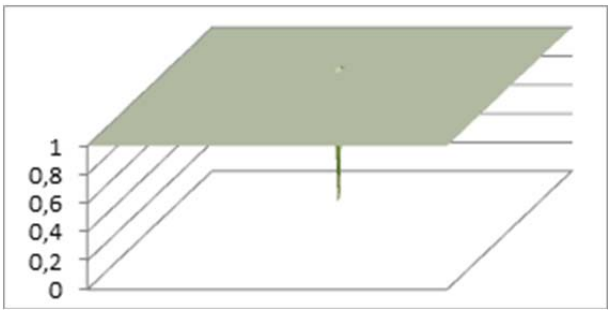

Figure 6:
Several following interactions occur at almost the same place: RBA assumes that the position does not change and is very precise.

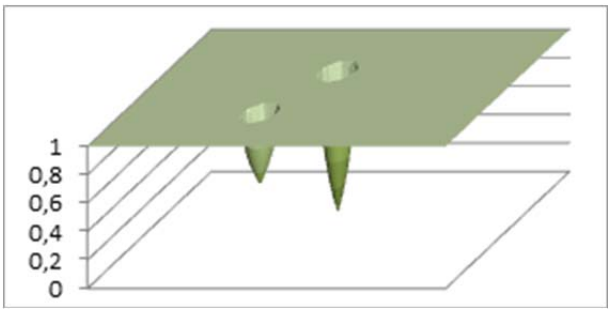

Figure 7:
An access from another place is recorded: RBA starts to be more tolerant but preserves the expected areas and their proportions.

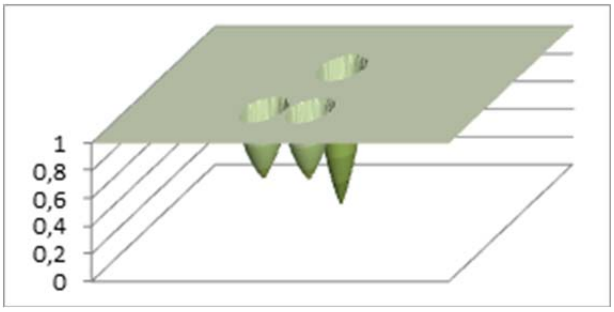

Figure 8:
An access from yet another place is recorded: RBA becomes even more tolerant to cover larger areas around the past occurrences.

DirX Access provides an RBA **test mode** for realizing this methodology. If a UCA risk condition is switched to test mode, the entire learning and evaluation process proceeds normally except that the result has no effect on the compound evaluation result. Instead, the results are monitored and can be further analyzed to achieve the optimal UCA RBA configuration.

Risk Evaluation Algorithm

The risk evaluation algorithm depends on the type of supplied data.

Ordinal Evaluation

Ordinal evaluation is based on the proximity of evaluated values to the ones recorded in the user model. In this way, DirX Access can process the **access time**, **IP address**, and **geolocation** data.

The geolocation data are transported to the system using the HTTP Geolocation header defined in a standard draft[1]. The Authentication Application enables using devices that can provide the geolocation data through the JavaScript Geolocation API.

Figure 4 shows the potential risk level assigned to the authentication request at a particular time of day. The changes are caused by the interaction of a legitimate user with the system over time – their behavior is re-evaluated on each new authentication request.

Figures 5 to 8 show the changes to the modelled geolocation over the time of the interaction with RBA. The vertical axis represents the normalized risk level while the horizontal axes represent the geolocation. In this case, the visible square depicts the area of a town, where the data have been collected for a single user. The resulting graph shows the potential risk level assigned to a request from the particular position (for all possible positions).

Device ID

When the device ID risk condition is configured, DirX Access attempts to deploy a long-term cookie on the client side. This cookie is subsequently used to identify the device (more precisely, the client application) and this information is used in a specific evaluation process.

String Evaluation

String evaluation is the simplest process. It is based on the strict match of current request values and user model values. However, to extend its expressiveness, regular expressions can be used in the evaluation process. This way, DirX Access evaluates the **HTTP request headers** and custom string data supplied to the system via a **customization** interface.

Complexity

RBA was designed with a major emphasis on its usability in the enterprise environment. This focus naturally resulted in complexity optimization. We did not identify any substantial increase in time or spatial requirements for the general risk conditions.

Depending on the actual configuration, the UCA risk conditions may cause an increase in time consumption during the request processing. However, this increase is for reasonably-configured conditions in the same order as the time of the condition-less request processing. Taking into account that the decisions are sent over a network, which is much more time-costly, the UCA-related time consumption can be considered insignificant for the decision consumer. The UCA risk conditions also impose space demands to store the user-related data. These demands are highly configurable, enabling the customer to set, for example, the upper limits of the space consumption.

Future Outlook

Continuous research and development of the risk-based authentication mechanism provides a long-term cutting-edge solution. The evolution of contemporary technologies makes the area of risk-based authentication look very promising. In particular, mobile devices are enabling the use of a growing number of sensors that produce interesting user data. Together with the ever-more-frequent employment of mobile devices in the enterprise environment, this trend offers a unique opportunity to improve the security of the information systems.

The development of machine-learning mechanisms is opening up other great possibilities. Even the currently transmitted data contained within every request contain much more information than is currently usually used. The focus is on evolving from a risk evaluation mechanism to a mechanism that provides an independent authentication method.

[1] Geographic extensions for HTTP transactions. https://tools.ietf.org/html/draft-daviel-http-geo-header-05

About Atos & Bull

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

For more information, **visit atos.net**

Bull, the Atos technologies for the digital transformation

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.

Bull is the European leader in HPC and its products include bullx, the energy-efficient supercomputer; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; Trustway, the hardware security module and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information, **visit bull.com**

DirX_Access_RBA-White-Paper-en1

Trusted partner for your **Digital Journey**

Atos