Exploration of Access Contorl Systems: A Structured Evaluation Metric

1st Jessy Liao
Computer Science
Colorado School of Mines
Golden, US
jessyliao@mymail.mines.edu

***Abstract*—There are countless security solutions when it comes to access control. Although most solutions share some core features, each of them provide unique ones as well. With so many different solutions and each providing their own unique features it is difficult to determine which solutions would best fit a user's or company's needs. The evaluation metric developed in this paper gives us the proper tool to evaluate and compare each of these solutions to determine what strengths and weaknesses a solution possesses. The approach to this evaluation gives insight to not only the specialties of each solutions, but also what overall trends occur for all solutions that were reviewed. Overall this tool can be expanded and utilized by companies for them to better pinpoint which security solution would best fit their needs.**

I. Introduction

The goal of computer security is to protect resources/information from theft and unauthorized usage. Many companies utilize a identity and access management (IAM) solution to ensure all security needs are met. As businesses transition to the digital age, the importance of keeping information secure becomes a higher priority. At the core of identity and access management is a computer security principle, access control.

Access control is the use of policy to identify users, and regulate what resources they are allowed to access/manipulate. There are four main access control polices that are commonly used:

- Discretionary access control: controls access based on the identify of the requester, and access rules which state what the requester is allowed to do
- Mandatory access control: controls access using security labels and security clearances
- Role-based access control: controls access based on roles that are assigned
- Attribute-based access control controls access based on the attributes of the user, the resources, and the environment of the system

Many of the solutions available utilizes a combination of these policies, this gives more control over what resources are given out and thus making the system more secure. These polices are not absolute and can be modified to prioritize the needs of the user. Since there are many ways to implement access control into an IAM system, it is difficult to determine which solution is the most suitable for a users needs. The rest of the paper will provide an evaluation metric to rank these different solutions, based on different categories, in order to answer this question.

II. Evaluation Metric

The table in figure 1 presents an evaluation metric that will aid in ranking the different IAM solutions. The table contains 3 main categories, in each category there are subcategories listed within them. These subcategories are treated as features, an IAM solution will be labeled with having, not having, or partially-having a subcategory or feature.

Feature Categories		
Identification	**Access Management**	**Security**
Advance Authentication	Ghost Users	Monitoring
Single Sign On	Hybrid Environment	Atuo-Reporting
	Ease of Use	Multi-Policy
	Database Backup	Granularity
	Trickle Down Privileges	Encrypted Communication
	Multi-Database	
	Principle of Least Privileges	

Fig. 1. List of all categories and their features

The rest of this section will delve into the explanation of the three main categories as well as a description of each of the subcategories/features. Along with the description, an explanation on the motivation of adding this feature into the evaluation metric will be provided.

A. Identification

This category encompasses features relating to how the IAM solution identifies a user, and the process in which they use to authenticate them. Due to the similarity of a different paper

on evaluating authentication schemes, this category was left rather short. There are two subcategories in this section.

I-1 *Advance Authentication*:
This subcategory means whether the IAM solution contains an advance authentication method or not. "Advance" means whether is uses an authentication scheme more complex than just a simple text password. A few examples of authentication schemes that would meet the requirements of this feature is multi-factor authentication, bio-metric authentication, third-party authentication, etc. This is easily one of the most important features of an IAM solution, as it is the first layer of protection, and if it is compromised, anyone could falsely be authenticated and access the system.

I-2. *Single Sign On*:
The IAM solution has single sign on capabilities. This feature was added to the metric table because most companies have large networks with multiple systems. Having single sign on capabilities would allow users to access these systems without repeatedly entering their information. This is more important for large-scale enterprises.

B. Authentication Management

This category represents features that provide the users with functionalities that make the overall system easier to use. For example, features that automatically handle situations would be under this category. Some of the features within this category may seem similar to the security category, however, the difference is that the features in this category, if not available, can be implemented by the user. The features in the security category, if not available, cannot be implemented and thus the overall system is less secure. The exception to this is features that are strictly for quality of life. Therefore, having them not implementable doesn't cause a security risk.

A-1 *Ghost Users*:
Does the IAM solution automatically remove ghost users? A ghost user is a user in the system that no longer needs access to their resources anymore. An example of when this case would occur is when an employee leaves a company and no longer needs access to any resources. This feature was added not just for the fact that it would be a convenient, but also because not removing ghosts users leaves a system vulnerable to attacks.

A-2 *Hybrid Environment*:
All users on the system are able to work from any environment. If the IAM solution requires the users to provide an IP address to white-list a location, then it would get ranked as partially-having this feature. Otherwise, if a user could work from any environment then it has this feature. With the popularity of remote work (partially forced by the pandemic), this is an important feature that IAM solutions should be providing now.

A-3 *Ease of Use*:
The IAM solution provides some sort of interface such that if an admin needed to add or remove privileges for users, it would be intuitive to do so, and easily done. The entire backbone of IAM solutions is providing privileges to authenticated users, therefore it would make sense that adding privileges be as convenient as possible.

A-4 *Database Backup*:
The IAM solution performs automatic backups on the databases. This feature is important for quality of life reasons and security reasons. Constant backups are good to have in-case mistakes were made. Security-wise, if a privilege was entered that breached the security of the system, with database backups, it could roll-back to a stable and secure version.

A-5 *Trickle Down Privileges*:
Trickle down privileges is the ability for users that were given privileges to pass down equal or less privileges to other users. For example, if a user was a project manager and wanted to give access to files to his team, he could create privileges for that and assign them to his team instead of submitting a ticket for IT to do it.

A-6 *Multi-Database*:
Multi-database means whether the IAM solution automatically stores all data in multiple databases. This feature is in the access management category because if this feature was not available, an admin could simply create multiple databases and do it that way themselves. However, this would be an extremely convenient feature if handled by the IAM solution.

A-7 *Principle of Least Privileges*:
The principle of least privileges is the concept of giving the least amount of privileges to a user so that they may perform some task. For example, if a user was tasked with updating the about page of a website, they should only get access to the pertaining html/php file that would update the about page. This feature may sound like it should be in the security category, but since a user could theoretically create privileges that follow this philosophy, this feature is more seen as a convenience than a security feature.

C. Security

The security category contains features that would improve the security of the overall system. If the features in this category are not available in the IAM solution than the overall security of that solution is lowered. As discussed in the previous section, if the feature is not available there is no way for a user to implement these features through other means.

S-1 *Multi-Policy*:
The IAM access control solution resembles features of multiple policies that was discussed in the introduction. This is important because the more advance the policy is, the more nuance and control you have over privileges.

Thus, giving the potential to having a more scrutinized system.

S-2 *Monitoring*:
The solution provides automatic monitoring. In other words, it does some sort of logging of all user activities, and what resources they attempt to access. Knowing who attempted to access certain resources is crucial for making sure users are accessing files they are allowed to access, and tracking down attackers if you know a resource has been compromised.

S-3 *Granularity*:
Granularity feature pertains to how specific can users make privileges when assigning them. Are privileges based on users and what resources they can access, or can users create complex rules where they could assign multiple users into these rules. Another example of this would be are privileges given to access a computer, or can it be more nuanced, where privileges are given to individual files/directories within a system.

S-4 *Auto-Reporting*:
Auto-reporting is a feature where if an entity attempts to access a resource that is supposed to be top-secret, the system will alert the admin that someone is trying to access that resource. This is important because if a user has resources that no one should know about, then chances are if someone is trying to access these resources, it is because of malicious intent.

S-5 *Encrypted Communication*:
All communications within a system or network are encrypted. This is especially important for the IAM solutions that also provide the A-2 features since they would be accessing information through a public network. For IAM solutions that is strictly on-site this feature is given to them since it can be considered as encrypted, since users have to be on-site to access any resource.

III. Existing Solutions & Evaluations

In this section we will utilize the evaluation metric that was created to evaluate a list of IAM solutions. Figure 2 at the end of this section displays all solutions and their respective features they were ranked with having.

To preface, the ranking of these solutions were done without actual access to the solution. Therefore, ranking a solution on a feature was done by scouring public information about the solution and looking through available documentation. The main method that was used was finding public documentation on setting up certain features in the solutions. This worked the best since it can be assumed that if there was no setup documentation for a specific feature, then that feature must not exist. For features that don't need setting up, the best way to determine if the solution provides that feature was to just look on their website.

For each of the solutions that are going to be evaluated, first the solution itself will be described in short. Afterwards, the policy that most matches the solution is described. Lastly, the actual evaluation of the solution on the three different categories is performed.

A. OnGuard

The first solution that was evaluated is OnGuard which was created by a company called LENEL. OnGuard is an access control and management software solution. They provide a series of packages that can be installed in unison. For this evaluation, the main solutions that were focused on was the OnGuard Version 7.5 + the OnGuard Cloud Edition.

After reviewing the OnGuard solution, the policies that most resembles it is a mix between a role based policy and a discretionary policy. Their solution allows for a list of rules to to be written (which they call policies). Each policy can be customized to give specific privileges. Within each policy, privileges can be specified further to targeting certain users. Therefore, there is enough granularity in privileges for it to resemble a discretionary policy.

For the identification category, they provide multiple advance authentication schemes. One of these schemes is multi-factor authentication. They also provide bio-metric scanners. The bio-metric authentication may pertain to physical security (eg. building security), it is unclear whether they apply to computer systems, however they have the technology and therefore they're ranked with having this feature. The OnGuard solution does provide single sign on capabilities.

For the access management category the OnGuard solutions does not have the ghost user removal feature. They do provide the hybrid environment feature, however this feature only comes if the OnGuard Cloud Edition is purchased. In terms of ease of use, OnGuard provides an easy to use interface that is fairly intuitive, and thus is ranked with having this feature. For database backup, there was no information about it possessing this feature, and for trickle down privilege, it does not have this feature. It also does not provide principle of least privileges feature.

Lastly, in the security category, OnGuard does keep a log of all users activities and thus is given the monitoring feature. Since the solution also allows for custom policies to be written it is given the granularity feature. For authentication, it notifies if an entity tries too many attempts to access the system and thus is given the auto-reporting feature. It also is advertised as having the capability to segment databases and thus has the multi-database feature. It also advertised with having encrypted communication. This makes sense as one of their main product is cloud based, and thus an encrypted communication channel is integral.

B. UnityIS

Another solution that was evaluated is the UnityIS access control system created by Imron. UnityIS is a cloud based solution providing an easy to use interface to handle all access control needs. Due to their solution being cloud based, their system can be easily integrated and provides access from any location, as well as being fully scalable. They also provide physical security for buildings, meaning access control for

building access. For their physical security, they use third party hardware provided by Mercury.

The policies that align the most with UnityIS's solution is mainly discretionary policy. Their web browser interface allows for editing privileges of specific users or entities. Since they have a partnership with Mercury, their system also resembles a mandatory access control policy as well, as they have the ability to assign different users with different clearances. These different clearances section off which areas of a building a user can enter.

In terms of the identification category, UnityIS provides multiple advance authentication techniques. The main one being multi-factor authentication. Also, with their partnership with Mercury, they have hardware that handles bio-metric authentication which is provided in their Series 3 product. Since UnityIS utilizes a cloud base solution as well as solutions provided by a third party, they implemented single sign on capabilities. This makes sense since there are different components to their entire system and having single sign on capabilities is convenient for the user to access all these different components.

In the authentication and management category, they have a majority of these feature. Like the OnGuard system, they do not provide an automatic way to remove ghost users. Thanks to their cloud-based solution they do have the hybrid environment as a user can be anywhere and still have access to the cloud. They also provide a clean user interface that is available in a browser, tablets, and mobile devices. In their documentation they also stated that they provide frequent database backups and retain database backups for 90 days. However, they did not state anything about separating their databases or segmenting them and thus are not given the multi-database feature. They also do not automatically handle trickle down privileges nor the principle of least privileges features.

For the security category, they hit every security feature in this category. For monitoring, they have a log manager which keeps logs of all users activities. They also have macro rules that can be designed to trigger certain instances, therefore functioning as an auto-reporting system. This macro capability also gives them the granularity feature. They also use TLS 1.2 and 2048 bit SSL Key for browser-client communication and thus checks off the encrypted communication feature.

C. SecureAuth

The next solution that was evaluated is called SecureAuth. SecureAuth is actually the company name and they provide a list of access management solutions such as authentication services, protecting web applications, and protecting other third party resources such as amazon cloud instances and 365 office applications. When evaluating this solution, it was assumed that a company implementing these services would get all of the available products, and thus if any one of their products meets a feature requirement, it is given that feature.

The policies that most resemble the solution provided by SecureAuth are mainly a discretionary access control policy. Since most of their products rely on authentication for individual users, privileges and access to resources are given out in a similar manner. However, since they have the capability to protect third party application resources, such as 365 office documents, this can also be seen as a role based access control policy.

The SecureAuth solution excels in the identification category. Its part of their company name, identification and authentication. Two of their most popular products are the passwordless authentication and their advance two-factor authentication solution. They use machine learning and adaptive authentication to view the behaviour of users and to continuously authenticate whether the user is who they are. Since they also protect a lot of third party resources, they have single sign on capabilities which allow users to access any application with a single authentication.

In the access management category, they do not have any products/solutions that automatically handle ghost users. In terms of a hybrid environment, since they have advance authentication scheme and utilize third party applications that are cloud services, they have the ability for users to access resources from anywhere. The products also come with a easy to use interface which gives them the ease to use feature. For database backup, they are ranked with partially having this feature since amazon cloud services provide data backups and a company could use this as their main solution. SecureAuth does not have trickle down privileges or principle of least privileges features. They also do not have the multi-database feature.

In the security category they definitely have the encrypted communication category as a majority of the products deal with a secure authentication connection to access resources. They do not have any features that deal with monitoring or auto-reporting however. Due to their specialized solution, they don't have any features for granular privileges. Their solution mainly focuses on correctly authenticating a user and then giving them access to an application or resource.

D. AccessIt!

The last evaluated solution is called AccessIt!. This solution has four tiers that are available. The first two tiers do not have a lot of access control capabilities so the focus will be on their highest tier which is AccessIt! Universal.NET Enterprise Edition. The AccessIt! solution combines a comprehensive access control management system that encompasses on site, physical building, security and computer and network system security. They provide a in browser interface to control the entire system as well as normal terminal functionality.

AccessIt! is a mix of discretionary, mandatory , and role-based access control policy. Their system allows for users to be given specific access to certain resources. Along with that, they have the ability to construct specific privilege macros that can be assigned to multiple users, thus functioning like a role-based access control policy.

For the identification category, they meet the advance authentication feature by having bio-metric scanners as well as

card readers available. They do not have any single sign on features available.

In the access management category, they do have a feature in place that somewhat handles ghost users. For their card scanners, cards that are not used frequently actually expire and are no longer usable. The information on their card scanners mostly talked about physical security (building security) versus computer system security. Therefore, this solution is ranked with partially having the ghost user feature. This is also because the users information and clearance could still be in the system, and if an attacker got in, they could still pose as this ghost user. For the hybrid environment feature, they do not have anything advertising cloud based solutions, therefore they are not given this feature. Their solution focuses more on individual sites. For ease of use, they provide a web browser interface where they can create new macros and give privileges, this is an add-on that could be used in addition to having a terminal handle everything. AccessIt! also provides, what they call, data import/export and data replication, which is essentially database backup and recovery. Their solution does not provide trickle down privileges features, and it does not have any automatic privilege creation that follows principle of least privileges. For multi-database, they are categorized with partially having this feature since they actually segment information for different sites. For example a company with three different locations can have the solution data separated into three different segments. Within each site, there is no information on whether they segment the databases storing the resources.

For the security category, they hit all features except for the encrypted communication. The encrypted communication feature is marked with partially having the feature. This is because their solution is focused on onsite access, which would partially remove the need for encrypted communication. Their software system allows for fine macros to be created and thus they fulfill the granularity feature. These macros can be customized to handle both monitoring and auto-reporting where certain resources or behaviour will trigger a response or alert.

The table displayed in figure 2 shows all solutions and their respective ranked features. As shown in the table, the general trend of unavailable features lies in the access management category. With a few unavailable features existing in the security category. Overall, most of the solutions that were reviewed had a majority of these features.

Solution Comparisons				
	OnGuard	UnityIs	SecureAuth	AccessIt!
Identification				
Advance Authentication	✓	✓	✓	✓
Single Sign On	✗	✓	✓	✗
Access Management				
Ghost Users	✗	✗	✗	~
Hybrid Environment	✓	✓	✗	✗
Ease Of Use	✓	✓	✓	✓
Database Backup	✗	✓	~	✓
Trickle Down Privileges	✗	✗	✗	✗
Multi-Database	✓	✗	✗	~
Principle of Least Privileges	✗	✗	✗	✗
Security				
Multi-Policy	✓	✓	✓	✓
Monitoring	✓	✓	✗	✓
Auto-Reporting	✓	✓	✗	✓
Granularity	✓	✓	✗	✓
Encrypted Communication	✓	✓	✓	✗

Fig. 2. check-mark = has feature, cross = doesn't have feature, squiggly = partially have feature

IV. Weights for Evaluation

For those who are in the market for an IAM solution, this table can be used with weights in order to prioritize different features for different needs. There are three different methods in applying weights with each being more granular than the previous:

1. Default/Basic weight scheme
2. Category weight scheme
3. Feature weight scheme

The default weights treat all features equally. The category weights gives granularity in terms of the three main categories and the feature weights allow for individual weights to be applied on each feature. Below are the functions for each of the weighting schemes. The functions all calculate a percentage (or a grade), where 100% would be the best grade.

A. Default Weight Scheme

$$\text{Default Weight} = \frac{\Sigma\ AllFeatures}{14} \times 100$$

This equation treats all features and categories equally. Essentially, whichever solution has the most amount of feature would have the highest weight for this scheme.

B. Category Weight Scheme

$$\text{Category Weight} = \frac{W_A \Sigma A + W_I \Sigma I + W_S \Sigma S}{W_A * 7 + W_I * 2 + W_S * 4} \times 100$$

Where $W_A, W_I,$ and W_S are numerical weights applied to the three main category. It is recommended that a weight between 1 and 2 is used to not overly skew any category.

C. Feature Weight Scheme

Feature Weight $= \Sigma W_i f_i$
W = [.....] array of size 14

For each feature i, apply the weight i defined in the array. For no weight to be applied, the value in the array for that feature should be 1.

V. Results

From the table in figure 2, there are prominent patterns that exists in the features ranked. One pattern is the lack of trickle down privileges. One possible explanation to this is that since most of these solutions also provide a physical security aspect, they don't give users the ability to give out privileges to others. Most building security doesn't allow for users to give out key-cards to other people. This could translate over to their computer system security and thus the system doesn't have the trickle down privileges feature.

Another pattern that was prominent is the lack of the principle of least privileges feature. This pattern makes sense due to the fact that it is hard to automate a process in which the system gives out just the correct amount of privileges for a task. This kind of capability requires a company to generate rules that give the right amount of privileges for a given task. Since tasks are abstract, the company needs to make the correct customized rules.

Ghost users is another feature that almost all of the solutions did not have. This made sense since an access control system would not know which users don't need access anymore. This means that the admin is responsible for checking which users need to maintain their privileges and which need to be removed.

Overall, based on the trends of unavailable features, the biggest takeaway is that admin maintenance is a necessity to maintaining the security of a system. As stated before, the access management category contain features that if not provided, can be implemented by the users. The access management category had the most amount of unavailable features. This reinforces the idea of the importance of proper maintenance.

VI. Future Work

In terms of future work, there is a lot of growth for this paper. The process of evaluating each of these solutions was difficult due to not having access to the actual solutions. If I were to revisit this project again with access to the solutions, this would open up new possibilities of potential features. One of these potential features could be latency - how quickly does the system add new privileges and update.

Due to the modular nature of the evaluation table, it would be straight forward to add more features and continue evaluating solutions. On top of that this table can be used as a guideline, and others can review IAM solutions on their own with this table. With more time, this paper can be expanded with the expansion of more features and a larger IAM solution sample size.

VII. Conclusion

Overall, this paper laid a solid foundation for evaluating the countless number of IAM solutions that currently exists. Along with this table, a weighting formula can be applied to help users determine which access control solution best suit their needs. There is a lot of room for growth and collaboration to be implemented in this evaluation metric.