A Survey of Active Directory Security and Privacy Threats and Implementation Administration

Matthew Zaldaña

California State University, Long Beach

Mr. Oscar Samayoa

CECS 303 – Networks and Network Security – Sec 3

Abstract

There are many risks that pose a threat to security and privacy in the Information Technology (IT) world, whether that is, as per usual, to an organization as a whole or to an individual user. A compromised account is only the first step to taking control of an organization and can be done in a variety of ways. However, a great majority of organizations use Microsoft's built-in service for user authentication in their Windows Operating Systems, namely, Active Directory. This central repository of information allows the System Administrator(s) to control and manage all the user information and company assets via a method that is flexible to scale and fairly easy to use. However, given the rise of many different types of attacks on organizations, especially during the pandemic of COVID-19, it is imperative to delve into the inner workings of Active Directory and build a more robust implementation of the most used IT Administrative Service. In this paper, we will focus on the works that other researchers have done. We will first compare some of the important risks that pose a threat to the Active Directory service as well as some of the solutions that can be implemented to each of these. Then, we will look at some of the current, alternative solutions to secure and control Domain Administrator accounts. Finally, we will explore a different solution that can be used with Active Directory, its inner workings and implementation.

Keywords: Information Technology (IT), Active Directory, Kerberos protocol, Domain Controller, IPSec protocol, Domain Admin, Azure Active Directory, Active Directory Log Analysis, Anomaly Detection, Advanced Persistent Threat, ransomware, Windows server, Multi-factor authentication, Event logs, Machine Learning, LDAP, SAML.

A Survey of Active Directory Security and Privacy Threats and Implementation Administration

Before we begin, we will briefly cover what the Active Directory, or AD, service is. Active Directory is a service that combines all user information and organization assets into one central database of information. Personally, I thought about a GitHub repository, which contains all the project folders and files pertinent to a single solution. While there may be several different projects in the same solution, there can only be one solution. For Active Directory, this includes created user information, credentials and the protocols used to authenticate them, IT assets such computers, peripherals, servers, etc., as well as important shared folders or files across a network. Each user and group within the service is given an amount of administration or privilege over a certain amount of information. This allows users to only have the required permissions to the resources they need. AD lives on the Microsoft Operating System, Windows Server, which started in the year 2000 and has evolved to the current version of 2022. On a more personal note, given its popularity and use, I have only seen and met organizations (including the current organization in which I currently stand) use Windows Server 2012 or 2016. This is another problem that we will briefly discuss as well. Given AD's flexibility for management, it is no surprise that it is the most used Administrative controller in organizations around the world. Given that all information is in a central location, information can easily be found and retrieved when needed. There are several other benefits to using AD, however, Binduf et al summarizes it best:

"SIMPLIFIES NETWORK RESOURCE MANAGEMENT AND SECURITY POLICY MANAGEMENT IN A HIERARCHICAL ORGANIZATION OF ACTIVE DIRECTORY; THE ABILITY TO MEET THE INCREASED AND GROWING NEEDS OF THE ORGANIZATION. THEREFORE, AFTER THE ACTIVE DIRECTORY INSTALLED IT

ALLOWS MODIFYING THE PROPERTIES AND ADDING OBJECTS. ALLOW MANAGING THE ORGANIZATION FROM ONE POINT. IT ENHANCED SECURITY BY PROVIDING A SECURE LOGIN MORE THAN ANOTHER DIRECTORY SERVICE. IT'S USED IPSEC PROTOCOL IN WINDOWS SERVER 2000/2003 AND KERBEROS PROTOCOL USED IN WINDOWS SERVER 2012" (BINDUF ET AL, 2).

Issues and Challenges

Yet, there are several issues and challenges that AD faces to authenticate users. Older versions of Windows sever have vulnerabilities that could cause an organization to become dysfunctional and allow hackers to gain access to AD. Some of the more prevalent are issues with over-permissioned service accounts which allow a user with the account to work directly with the OS itself. Given that this is a very special account, adding more privileges to it could cause a serious security danger if not well-maintained or protected. Another account that has a lot of power and privilege functionally is that of Domain Admins. These administrators contain all the administrative rights of all domains inside of AD and the AD controller itself. This type of account manages everything. However, with the correct configuration in setting account permissions, this account can be kept safe, yet, if compromised, risks to expose the entire AD service to an attacker. On a personal note, in my current organization, our Domain Administrator supervisors have set Group Policy rules in place so that only specific users are Domain Admins and created rules so that specific users can have other privileges. Limitations are key. For example, I am a current Domain Admin, however, I have limited rights regarding read and write operations to the AD controller when managing assets. Full control is given to the IT administrators such as my supervisor. This allows certain users, such as IT field technicians like me, to still have added privileges compared to other network users, yet not too much in case of a

breach in security. Another issue with AD is that local administrator accounts might have the same credentials for certain assets, such as workstations or network equipment. Thus, if an attacker gains access to any one of the workstations, the attacker gains access to all of them. For security reasons, I will comment further as to how we do this but will want to fix this issue in a different way, possibly in one of the solutions that will be provided. Lastly, risks are high when Domain Controllers are running an "old version of OS", because older versions of Windows Server have more vulnerabilities and security dangers. Of course, with each newer version, security improvements increase OS security and performance, giving an easy, feasible solution to those who have not yet implemented this service (Binduf et al, 3-5).

Alternate Solutions

In this section, we will provide insight and knowledge into how Anomaly Detection and Machine Learning can aid in attacks such as APT and AD Event Logs, giving System Admins a method to reduce the risk or impact of an attack on AD.

Anomaly and APT Detections using Machine Learning.

This Taiwanese paper was very theoretical and statistical in nature; however, it surpassed all my expectations as to the results that machine learning could give in current context. The researchers gave us some context on APTs, which is Advanced Persistent Threats on a system, in this case, AD, which allows hackers to continue to exploit vulnerabilities in the system unbeknownst to the user. Unfortunately, it takes "averagely at least 346 days for more than 81% victims to aware that they have been hacked" (Hsieh et al, 1). The researchers collected a large amount of AD log data from a large Taiwanese organization and pre-processed the information. This allowed the researchers to create an example behavioral model for the data to be tested on the AD controller. Then they mapped this to a Markov chain model and presented the results.

Based on their model and the experiments that they ran, they analyzed the data logs from AD and created a Markov model and found that “best performance of about 66.6% recall and 99.0% precision rates” were achieved (Hsieh et al, 6). This allows AD Domain controllers to set up the experiment in their own sandbox so that they can test this out and see that anomalies are caught in the AD Data logs of the Domain Controller and stop malicious actors provided they leave tracks.

Another form this kind of attack can be found was through a different experiment performed by different researchers. These scientists proposed a method to use outlier detection with machine learning to look at the AD Events logs related to user processes (Matsuda et al 2). These attacks and the experiment rely on the assumption that the user who is compromised is the Domain Admin, which is the highest privileged form in AD. This greatly benefits organizations all over and enhances the possibility that this method of risk mitigation may be taken. Since activities by the Domain Admin are recorded, their method investigated the recorded logs to find APTs. First, they pre-process data for the behavioral model to learn from. The result of the experiment was greatly beneficial. They delved into specific event logs that are recorded into the log monitor for the AD Domain Admin controller log file. This would include files such as “Add users”, “reset user passwords”, “check Event viewer”, etc. (Matsuda et al, 5). Given these interactions, The precision of the ML classifier exceeded that of 81% for Events such as attempted user change of password with 95% accuracy. This method of finding APTs within the Event Viewer controller “yields a high recall and precision rate even if a legitimate Domain Administrator account is leveraged, or a file name of an attack tool is changed” (Matsuda et al 6). Given its versatility and the tools it uses, it would be easily feasible to implement this into existing AD controllers.

A New Hope… Approach

Given its vastness, I found a paper that offers a promising solution to AD authentication and would like to share its new and promising way of authenticating users using multi-factor authentication methods. While a user's credentials are the most valuable piece of information that can be stored inside any controller, current popular methods for logging in only suit, at most, the first three-factor authentication paths. Two factor-authentication suits the something you have, and obviously, the user will have something they know, however, something you are is not typically implemented into large organizations. We do, however, see it even more increasingly available in small devices, such as our phones, which can take fingerprints and face ID recognition to comply with something you are. However, the researchers propose a five-factor authentication method, which would fulfill the where you are and when you are methods of authentication. This information would be stored in a Kerberos package(?) and the user would send their responses to the Kerberos Authentication service. Even before logging in, the user would already see displayed on their screen some of this information which would be publicly available (eyes) but not to the controller.

Conclusion

I appreciate the fact that this knowledge exists out there and that I can understand and learn this in a way that ties everything I have learned thus far in my degree. Some of these ideas are worth implementing into my current organization, however, the information may not be freely given to me as to whether it is already or can be done. Active Directory is a very popular authentication service and the protocols and management tools it provides allow easy access and flexibility when interacting with its data. While the tools exist to strengthen it, I remember Professor Samayoa's words: "No system is ever truly secure."

References

Binduf, A., Alamoudi, O., Balahmar H., Alshamrani, S., Al-Omar, H., Naya N. (2018). Active Directory and Related Aspects of Security. *IEEE*.

Hsieh C., Lai, C., Mao, C., Kao, T., Lee, K. (2018). AD^2: Anomaly Detection of Active Directory Log Data for Insider Threat Monitoring. *IEEE.*

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., Buchanan, W. (2022). Ransomeware: Analysing the Impact on Windows Active Directory Domain Services. *MDPI*. https://doi.org/10.3390/s22030953

Kadlec J., Jaros D., Kuchta, R. (2010). Implementation of an Advanced Authentication Method Within Microsoft Active Directory Network Services. IEEE.

Matsuda, W., Fujimoto M., Mitsunaga T. (2018). Detecting APT attacks against Active Directory using Machine Leaning. *IEEE.*

Rajput M., Yadav D. (2020). SAML Based Authentication. *IEEE.*