BEST PRACTICES FOR IMPLEMENTING ACCESS CONTROL SYSTEMS

By Isaac McGuire

East Carolina University
ICTN 4040

Best Practices for Implementing Access Control Systems

As a network administrator or information security specialist, you might find yourself wondering if your network is safe. You are constantly asking yourself, "What can I do to ensure that the data on my network is protected?" One of the ways to protect your network is what I would like to talk about and that method is through access control systems. In this paper, I am going to cover what access control is. I am also going to talk about the two different types of access control, physical and logical, and some of the methods of both. Next, and the main point, I would like to talk about the security best practices for implementing access control systems. Access control systems are powerful security tools that can help you protect the data on your network.

Access control can be summed up as identifying a person doing a specific job, authenticating them based on identification, and then only giving that person access to the minimum of what they need to complete their job. When it comes to access control systems, there are two different types that need to be implemented in a business. The two types are physical and logical. Physical access control is any type of physical barrier that prevents data from being accessed. This can be anything from a keeping a computer secure by having a door locked in order to access it, using an access log that shows what people had access to a device, and using a camera surveillance system to see what people are accessing devices, or any other physical system that keeps data safe. Security from a door can either be very basic or complex; ranging from just a standard lock to physical tokens. Physical tokens are usually ID badges for the company. These ID badges will sometimes be swiped so the person can have access or sometimes they contain radio frequency identification tag (RFID) that is scanned for access. Access logs are usually on paper and they require the person to sign in with all their credentials like name and telephone number. If done correctly, access logs can complement video surveillance. Video surveillance on a closed-circuit television can be used by a business to see who is gaining physical access to devices or certain rooms of a particular building (Gentry, 2012). These types of physical access control systems are used on daily basis within an organization. They are useful because the identification and authentication process is easy and fast. In more advanced physical access control systems, a cryptographic encryption may be implemented so an attacker cannot eavesdrop on the data that the access control systems take in (Hajny, Dzurenda, & Malina). Physical access control can only do so much and it will never be perfect, but that is where logical access control comes into play (Gentry, 2012).

A current growing need for security when it comes to users' files has spurred various methods in keeping logical data safe (Rahimiasl & Azmi, 2011). Logical access control systems can implement different methods to secure data. Some of the methods include, but are not limited to, using access control lists (ACLs), group policies, passwords, and account restrictions. Access control lists (ACLs) are permissions that are assigned to certain files and they will either restrict or grant permission to a user depending on if they meet the requirements of the ACLs. The permissions assigned to certain files range from access denied to read-only to full control of the files. The entries that are contained within an ACL are called access control entries (ACEs). ACEs are configured with four pieces of information: a security identifier (SID), an access mask, a flag for operations that limit what can be done on the object, and another set of flags that point to inherited permissions. ACLs can provide in-depth access control but can sometimes spell trouble for an organization that is always changing and requires a person to manage many objects. Group policies are specific to a Windows environment but are useful because a network of computers can be managed through a centralized resource called Active Directory. These policies eliminate the need to go to every single computer on a network to configure access control. Passwords are the most common method of access control and are sometimes referred to as logical tokens. They are useful in any network environment but they need to be strong enough to where an attacker cannot easily figure it out. A password gets stronger as it gets longer and when more non-alphabetic characters are used. The last logical access control method to discuss is account restrictions. Two of the most common account restrictions are time of day restrictions, which only allow someone to access a device at certain times, and account expiration, which gets rid of unused accounts so an attacker cannot use them. Logical access control systems are not perfect either, but when best security practices are implemented they have a higher chance to protect data on a network (Gentry, 2012).

When it comes to best security practices when implementing physical access control systems, also referred to as PACs, there are a lot of things that need to be considered. When implementing a physical access control system that processes radio frequency identification tags (RFID) and near-field communication (NFC) there should be a general architecture that is laid out for the network. It should consist of a user database, a central server, access terminals, RFID and NFC readers, and the ID badges or a smartphone. The ID badges or smartphones relay information about the person that is trying to gain access through a door to an access terminal. The access terminal should be directly connected to the readers. The access terminal will keep a list of identifiers that will allow it to determine if the person should have access or not. Once this is set up, the access terminal should be directly connected the central server. The central server is the centralized point of where all the rules are based. An administrator can apply certain permissions to the central server for who can access through the door. Last, the central server should have a connection to a user database. The user database stores all the information about every employee in the company. It will help determine who can enter through the door (Hajny, Dzurenda, & Malina). This system only works if you have good access control key management. All access control systems should have secret keys. The access cards that are given out to be used with the readers should have strong encryption such as 3DES or AES. When the cards are read, the readers should follow an authentication protocol. The secure channel between the readers and the access terminal should employ a good protocol like TLS because it is well analyzed. The channel should provide mutual authentication between the access terminal and the backend, AKA the central server, as well to give access for the person (Rohr, Nohl, & Plötz).

Once a good physical access control system is implemented, a logical access control should be implemented. When implementing a logical access control system, there are ten best practices that need to be followed to start with. The ten best practices are: create an access baseline, automate user provisioning, find the business case, tie access controls to the network environment, segregate access using roles, apply the doctrine of least access, channel big brother, terminate orphaned accounts with extreme prejudice, proactively monitor for unusual activity, and control remote access. To create an access baseline means to have the IT department start out by determining the current access levels and controls that are in place for the company. This will help provide the company with the necessary information on who needs access to what to do their job and do it proficiently. Once the baseline is established, the user provisioning needs to be set up as automatic. If user provisioning is done by manual ways, then detecting unusual behavior can become difficult. Manually user provisioning the network can result in missing a lot of issues. It is recommended to use a user provision software because when the process becomes automated, the company can determine what each worker needs to complete their job.

Also, the software can adjust to role changes easier. After implementing an automated user provisioning software, the company should look to find the business case. This allows the company to get the most for its investment. With more automated services, the company does not need as many IT workers. Next, the company that is implementing a new logical access control system should tie access controls to their network environment. Access controls are going to be based on the network environment, so they should meet only the requirements that the company needs. There does not have to be as strong a security for a small mom and pop shop as there should be at a large company. Once the access controls have been tied to the network environment, the company should segregate access using roles. All this means is that there should be a separation of duties, for example someone working in the programming department should not have access to corporate financial data. Next, the company should apply the doctrine of least access. This means that the worker should have the least amount of access to data that they need to complete their job. After that, the company should channel big brother, which means that they should audit everything to keep a watchful eye over every employee. Once the company has established an audit system, they should make sure to terminate orphaned accounts with extreme prejudice. This just means that the company should make sure to get rid of any accounts of former employees because they are a security risk if they are malicious. Proactively monitor for unusual activity is the next step when implementing a logical access control system. They should monitor access patterns to watch for unusual activities, such as a spike in a user's access to a file with sensitive information. Finally, the company should also control remote access plus applications and databases. As a company expands it must create rules for workers that are displaced and have remote access privileges. These ten best practices are a step in the right direction of implementing a good logical access control system, but no system is going to be perfect (Schwartz, 2007).

No access control system is going to be perfect, but if the right procedures are put in place when implementing both a physical and logical access control systems then there is a higher chance of data being safe. A physical access control system should be implemented in a way that only allows the correct people through the physical barrier like a door with a RFID scanner. A logical access control systems needs to have certain rules implemented that only allow workers access to data that is required to do their job. They should not have access to data that is not necessary to complete a typical work day. Companies are still vulnerable to attacks even with access control systems but most of the time these attacks come from within. If security best practices are implemented, then the access control systems should cut back on successful attacks against your company.

References

[1]Gentry, S. (2012, November 28). *Access Control: Models and Methods*. Retrieved from Infosec Institute: http://resources.infosecinstitute.com/access-control-models-and-methods/#gref

[2]Hajny, J., Dzurenda, P., & Malina, L. (n.d.). *Secure Physical Access Control with Strong Cryptographic Protection.* Brno, Czech Republic: Department of Telecommunications, Brno University of Technology.

[3]Rahimiasl, F., & Azmi, R. (2011). SeKMAC: A Secure Model for Key Management and Access Control in Cryprographic File System. *6th International Conference on Internet Technology and Secured Transactions*, 732-737.

[4]Rohr, A., Nohl, K., & Plötz, H. (n.d.). *Establishing Security Best Practices in Access Control.* Berlin, Germany: Security Research Labs.

[5]Schwartz, M. (2007, March 3). *Access Control: 10 Best Practices*. Retrieved from Enterprise Systems Journal: https://esj.com/articles/2007/03/27/access-control-10-best-practices.aspx