# Transcript: IT Podcast - Ep 106 - C836 Lesson 3 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU IT audio series, flexible, portable, profound.

Hey, this is Arthur with WGU. I'm one of the course instructors for a C836 fundamentals of information security and this is lesson 3. Just as a reminder, this series is to enhance the reading material, not to replace it. Let's get to it. It's highly recommended that you don't schedule your first assessment until all material is covered. Take the pre-test, review lessons 1-12, paying close attention to Chapters 1-6. Complete lessons 1-12 flashcards, paying close attention as to Chapters 1-6, complete lessons 1-12 quizzes and learn and test mode and again, paying close attention to Chapters 1-6. Authorization, after a user is identified and then authenticated, the next step is authorization. Authorization is what the user can access, modify, and delete.

Principle of least privilege is the lowest level of authorization allowed for a user to perform duties. Violation of the principle of least privilege is a user having more than necessary access to perform the duties assigned. This user can allow bad actors to cause damage to the production data. I want to expand upon this. The violation of the principle of least privilege can also be called creeping privileges. Usually it happens when a individual or a user has been at an organization for a set period of time and has transitioned into several different roles without an actual audit of the authorization taking place, and this can cause to that creeping privileges.

There are four basic tasks that we want to carry out and access control: allowing access, denying access, limiting access, and revoking access. Allowing is just giving a particular party access to the given resource. Denying is simply the opposite of allowing access. Limiting access basically limits the access up to a certain point, maybe sandbox limitations are put in place just for that particular resource, user application entity or whatever the object is accessing. Revoking is taking way access once a user is terminated or a program is terminated, and it might not necessarily always be termination. It could be again that job change role, whereas we had Jim who's in accounting and now he's over in IT, so we might have to revoke his accounting privileges and make sure we change them into his IT privileges.

Access control list, often referred to as ACLs, are very common choice for implementing access control. ACLs are usually to control access at a file system on which our operating systems run on and control the flow of traffic into the networks from which our systems are attached. When we look at ACLs, we usually have three sets of permissions that come with them. Its read, allowing us to read the contents of the file.

Write, allowing us to write to the file or directory, and execute to run the contents of the file being that a script or some sort of software application. Network ACLs, when we look at a variety of activities that take place on our network, both public and private, we again see ACLs regulating the activity. In the case of network ACLs, we particularly see that they are controlled by identifier's that we use Bing, IP addresses and Media Access Control, MAC addresses and ports. Permissions on these types of ACLs are binary in nature. They either deal with allowing or denying, there's no in-between. It's either a one or a zero, on or off. Capability based securities provide us with an alternative solution to the binary one or zero that we were just talking about with network ACLs, where ACLs define the permissions based on the given resource and identity. There is a set of permissions, all generally hailed from a file, some capabilities are orientated around the use of that token for our access. For example, let's say access to that datacenter. Now, we might have visa access, which is just a temporary one day pass.

But we're still going into the same datacenter whereas a visitor we might only have so many hours that we can go in, whereas if we worked in a datacenter, we might have access from let's say 8:00-5:00 if we're first shift. Then if we're in management, we might have access around the clock to come in after hours if there is an issue.

The confused deputy problem is a common type of attack that uses system ACLs. The crux of the confused deputy problem is seen when the software has a greater level of permissions to access a resource then the user controlling the software. We can often trick the user that is using it to misuse the software that has greater authority and potentially carry out an attack. Often two types of confused deputy problems that we see are cross-site request forgery, I apologize, cross-site scripting is a another tack totally, and click jacking.

Cross-site request forgery is an attack that misuses the authority of the browser on the user's computer. If the attacker knows or can guess a website that a user might already be authenticated to perhaps such as Amazon, they can attempt to carry out a cross-site scripting attack. This is done by embedding a link into the web page or HTML based email, generally a link or an image in which the user is directed to without their knowledge, then the application begins to run some command line behind the scene. Whereas click jacking is where you have a user who's going to a particular site and the bad actor has already taken control of a certain portion of the site. Now the user going to that portion that the bad actor now controls, the bad actor can layer a invisible frame or an invisible window on top of a legitimate link. Once the user clicks on it, can actually run scripting code in the background to carry out the attack that gets the user.

Access control models. There are five different access control models that we're going to discuss: discretionary, mandatory, rule-base, role-based, atrophy.

Discretionary access control deck is the access control model based on being determined by the owner of the resource in question. It's very common in Microsoft where you own the file and you're allowing other users on the computer or network to actually have allowed them access to the file. Mandatory access control is a model based on whether or not the owner of the resource does not get to decide who it is.

Unlike DAG, but it's actually control is set up by a group or individual authorizing authority on the resources that may or may not own it. You see this a lot more common in larger environments, especially military. I really think the Department of Defense right here, when I think of mandatory access control.

Rule-based access control is similar to that of the ACLs that we were talking about dealing with firewalls and routers. It's that very basic binary on, off, allow or deny. Rule-based access control is similar to that of a Mac, but it's set based upon the user's role within the organization. For an example, if you have a clerical staff at the front of a doctor's office, they would have certain permissions assigned to their role dealing with billing and patient information. Whereas the provider in that bag may only be able to see the access their patient records dealing with their medical treatment. Attribute base access control is based on the attributes, whereas this one is more along the lines of the context at which somebody is trying to access the resource. You must be this tall to ride this based off of your height. It could be. You may have to be geo-located from somewhere in the US with a particular IP address. It might be the type of time that it might be the time at data in which you're trying to access this resource in which you can't be deny.

Attribute-based is based off of Khan techs.

Sometimes when one access control level isn't enough, you have to layer them on top of each other. We're going to specifically look at three different types of multilevel access control, which is the bell Lupita model forgive me for my pronunciation there. The piper model and the Brewer Nash model.

The bill model is a combination of Discretionary Access Control and Mandatory Access Control that primarily deals with confidentiality. The best way to sum this model up is there is no read up and know right now. In short, this means that we are handling classified information. We can not read any higher than our security clearance, and we cannot write, classify that down to a lower clearance level.

The piper model is the exact opposite of the bill model and the piper model focuses on integrity of the data. The way I remember it is Bill confidentiality, piper I integrity. To summarize this particular model, it says no, read down, no right up.

This might seem counter-intuitive when we are considering protecting information. But remember that we had changed the focus from confidentiality to integrity. In this case, we want to make sure that the enforce integrity by ensuring that our resource can only be written to by those of a high level of access. That those with a high level of access do not access a resource from a lower classification.

The brood Nash model, also known as the Chinese Wall model, is the access control model that is designed to prevent conflicts of interests. Again, this is another data integrity model. Objects are resources such as files or information pertaining to the single organization. Company groups, how objects pertaining to a particular organization, and conflict classes or groups of objects that contain competing parties.

For example, if you have a law firm that take and this law firm has several attorneys there, and you had the attorneys that take on to clients that are opposing ends of a court case. In order to protect the non-compete clause, you have to make sure that both of these cases are completely separate from one another and that eat neither attorney can actually gain an advantage by looking at the other clients data files and logs. Physical access controls, often around controlling the movement in and out facilities. One of the most common physical access controls deal with that of tailgating or piggybacking, depending upon the resource that you use. Tailgating is when we see somebody that is following very closely behind another person who's just authenticated with a badge.

That other person might not have any identification or anything on them. Or we step outside for a quick second, we see somebody struggling with a box and they're just asking us to hold the door while they come in. But again, you don't see any authorization to actually allow that person in. Once we actually allow that person in without having that clearance and that authorization, they have just performed a tailgating or a piggybacking scenario to gain unauthorized access into the facility.

I want to bring this to a close. Thank you. Again, I appreciate you stopping by and listening to this audio series on C8 36, Fundamentals of information security. With this, I would challenge you to contact your course instructors if you're having any issues within the course and apply these concepts to your daily lives. They will flow a lot easier. Thank you very much, and have a nice day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.