Activity 13-02: Modeling Access Control Lists

Big Idea

Access Control Lists (ACL) are developed to identify which users have permission to access network resources, including the network itself. By the end of the activity, students should be able to understand how ACLs function in a real-world environment, and how to assign appropriate permissions to different user groups.

Materials

Materials vary based on your preference. They can include

- Paper and pencil/pen/marker or dry-erase boards
- Sticky notes or scraps of paper of different colors, scissors
- Small blocks, LEGO®, or game pieces

Vocabulary

Access Control List (ACL)
Users
Network resource
Groups
Permissions

Background

Consider all the different types of people who access a school network and its resources. There are teachers and students, of course, but administrators, counselors, support staff, and others. Many networks also allow guests to join and access network resources. People are considered **users** of the network and its resources.

A **network resource** may be the network itself or it can include a wide range of applications and web-based services. It includes some physical devices that connect to the network, like storage drives, whiteboards, security cameras, and more. All of these applications and devices generate and use data, but not everyone who accesses a network should be able to access every network resource and all the data it manages. For example, your teachers have permission to access grade records but you should only have permission to access yours. Your school may

have bookkeepers and office staff that process payments and so have permission to access financial records, but those resources obviously need to be kept secure from others.

An Access Control List (ACL) can identify everyone who logs into the network and give them different **permissions** to the resources and information they need, but *only* those resources and information. ACL can use different methods to determine the permissions that are given to users. One common method is to organize users by **groups.** When a user is identified as a member of a particular group, they have the same permissions that everyone in that group does.

You may be familiar with granting permissions if you use Microsoft OneDrive or Google Drive to share documents with others. When you share them, you have options like allowing others to View only, Comment on a document, or have complete rights as an Editor. You can also limit others from accessing your documents.

This video (12:20) from TechSpectrum Pro, Access Control Lists and Layer 2 Security Features, provides an overview of these important security measures. Identify the importance of ACLs in real-life as mentioned in the video. A simplified version of security features you might be familiar with are parental controls in home networks that parents can set to block some content and keep their children safe.

Activity Directions

1. Use the table below to generate a list of different types of users that may access your school district's network. Think about all of the places on and off campus where people might access the network, including people who work in the cafeteria, transportation, and administrative offices, along with different types of students and teachers. A couple of examples have been provided to get you started.
2. In the second column, make a list of different types of network resources. You can confer with your Tech Team coordinator or someone from the ID Department to identify resources you may not know about. For example, there may be some software that is purchased only for some students, like specialized computer-assisted design (CAD) software or specialized math or graphic software. There may be hardware-based resources, such as storage drives, printers, document cameras, and others that all access the network.
3. The third column provides a simplified list of permissions.
4. Using your list, create groups that should have the same type of permissions for different resources. You can do this with paper and pencil or you may want to print and cut out your lists so you can make them easier to move around. You can also use sticky notes or even small blocks, LEGO®, or game pieces, that represent different users and

resources that you can manipulate easily. Different colors can represent different groups or different permissions. Figure out what works for you.

Users	Network Resources	Permissions
Classroom Teachers Teachers Aides School Counselors Cafeteria Staff All Students CTE Students Parents Visitors/Community Members	School Network Guest Network Printers in the Library The Library's Card Catalog Interactive Whiteboard 3D Printer	**Read or View:** permission to view the content of a file or folder/directory. **Write:** Permission to create, modify, or delete files or folders/directories. **Execute:** Permission to run a file or access all of a folder/directory. **Full Control:** All permissions including the ability to change the ACL for other groups.

Extension Activities

Assigning Permissions to Groups
Introduce roles with the groups (ex. network administrator, user group representative, other) to encourage understanding of different perspectives in network security. Possibly include a scenario with conflicts, such as overlapping permissions or exceptional cases, to encourage critical thinking.

Modeling ACLs
Use different colors of sticky notes to represent different user groups or permission levels.