

COMPUTER SECURITY

Access-Control List (ACL)

Lecture 6

4th stage – (2020-2021)

Dr. Moceheb Lazam Shuwandy

OUTLINE

- **What is an Access Control List?**
 - Reasons to use an ACL
- **How ACL Works?**
- **Types of Access Control Lists**
 - Standard ACL
 - Extended ACL
- **Linux ACL vs. Windows ACL**
- **ACL Best Practices**
- **RBAC vs ACL**
- **Role-Based Access Control with Imperva**

WHAT IS AN ACCESS CONTROL LIST?

- An access control list (ACL) contains rules that grant or deny access to certain digital environments.
- There are two types of ACLs:
 - Filesystem ACLs—filter access to files and/or directories. Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.
 - Networking ACLs—filter access to the network. Networking ACLs tell routers and switches which type of traffic can access the network, and which activity is allowed.
- Originally, ACLs were the only way to achieve firewall protection. Today, there are many types of firewalls and alternatives to ACLs.
 - However, organizations continue to use ACLs in conjunction with technologies like virtual private networks (VPNs) that specify which traffic should be encrypted and transferred through a VPN tunnel.

WHAT IS AN ACCESS CONTROL LIST? CON. (REASONS TO USE AN ACL)

- **Traffic flow control**
- **Restricted network traffic for better network performance**
- **A level of security for network access specifying which areas of the server/network/service can be accessed by a user and which cannot**
- **Granular monitoring of the traffic exiting and entering the system**

HOW ACL WORKS

- A filesystem ACL is a table that informs a computer operating system of the access privileges a user has to a system object, including a single file or a file directory.
 - Each object has a security property that connects it to its access control list. The list has an entry for every user with access rights to the system.

- Typical privileges include the right to read a single file (or all the files) in a directory, to execute the file, or to write to the file or files.
 - Operating systems that use an ACL include, for example, Microsoft Windows NT/2000, Novell's Netware, Digital's OpenVMS, and UNIX-based systems.

- When a user requests an object in an ACL-based security model, the operating system studies the ACL for a relevant entry and sees whether the requested operation is permissible.

HOW ACL WORKS ...CON.

- Networking ACLs are installed in routers or switches, where they act as traffic filters.
 - Each networking ACL contains predefined rules that control which packets or routing updates are allowed or denied access to a network.

- Routers and switches with ACLs work like packet filters that transfer or deny packets based on filtering criteria.
 - As a Layer 3 device, a packet-filtering router uses rules to see if traffic should be permitted or denied access.
 - It decides this based on source and destination IP addresses, destination port and source port, and the official procedure of the packet.

TYPES OF ACCESS CONTROL LISTS

- Access control lists can be approached in relation to two main categories:
 - Standard ACL
 - An access-list that is developed solely using the source IP address. These access control lists allow or block the entire protocol suite.
 - They don't differentiate between IP traffic such as UDP, TCP, and HTTPS.
 - They use numbers 1-99 or 1300-1999 so the router can recognize the address as the source IP address.
 - Extended ACL
 - An access-list that is widely used as it can differentiate IP traffic.
 - It uses both source and destination IP addresses and port numbers to make sense of IP traffic.
 - Can also specify which IP traffic should be allowed or denied. They use the numbers 100-199 and 2000-2699.

LINUX ACL VS. WINDOWS ACL

- Linux provides the flexibility to make kernel modifications, which cannot be done with Windows. However, because you can make kernel modifications to Linux, may need specialized expertise to maintain the production environment.
- Windows offers the advantage of a stable platform, but it is not as flexible as Linux. In relation to application integration, Windows is easier than Linux.
- A user can set access control mechanisms in a Windows box without adding software.
- In terms of patching, Microsoft is the only source to issue Windows patches. With Linux, you can choose to wait until a commercial Linux provider releases a patch or you can go with an open-source entity for patches.

ACL BEST PRACTICES

- When configuring ACLs, you should adhere to a few best practices to ensure that security is tight and suspicious traffic is blocked:

1. ACLs everywhere

- ACLs are enforced on each interface, in nearly all security or routing gear.
This is fitting as you can't have the same rules for outward-facing interfaces and interfaces that form your campus network.
However, interfaces are similar and you don't want some protected by ACLs and some exposed.
- The practice of an ACL on all interfaces is essential for inbound ACLs, specifically the rules that decide which address can transfer data into your network.
Those are the rules that make a considerable difference.

ACL BEST PRACTICES CON.

2. ACL in order

- In almost all cases, the engine enforcing the ACL begins at the top and moves down the list.

This has implications for working out what an ACL will do with a specific data stream.

- One reason organizations adopt ACLs is that they have a lower computational overhead than stateful firewalls and that they work at high speeds.

This is essential when you try to implement security for fast network interfaces.

However, the longer a packet remains in the system, while it is examined against the rules in the ACL, the slower the performance.

- The trick is to put the rules that you expect will be triggered at the top of the ACL.

Work from the general to specific, while ensuring the rules are logically grouped.

Should know that each packet will be acted on by the initial rule that it triggers, Could end up passing a packet via one rule when you intend to block it via another.

Consider how you want the chain of events to happen, in particular when adding new rules.

ACL BEST PRACTICES CON.

3. Document your work

- When you add ACL rules, document why you are adding them, what they are intended to do, and when you added them.
- You don't need to have one comment per rule. You can make one comment for a block of rules, an intricate explanation for a single rule, or a combination of both approaches.
- Developers should ensure that the current rules are documented, so nobody needs to guess why a rule is there.

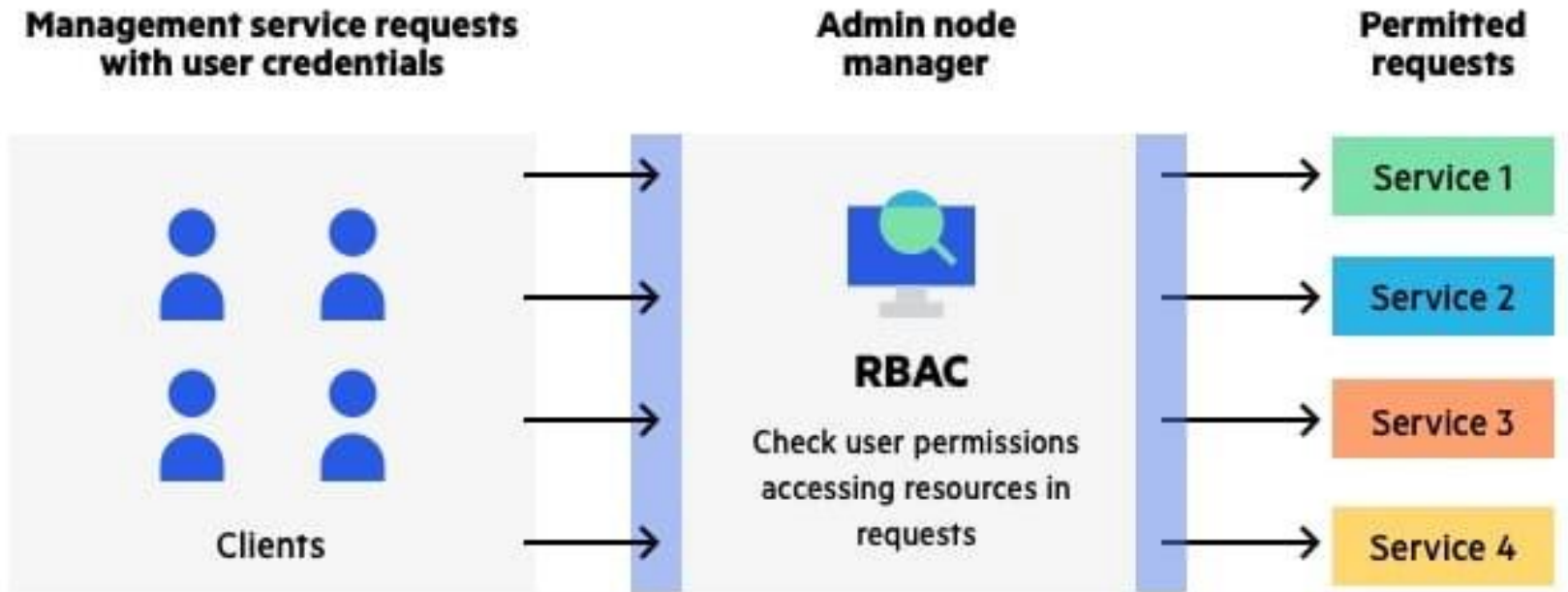
RBAC VS ACL

- Developers can use role-based access list (RBAC) systems to control security at a granular level.
- Rather than emphasizing the identity of the user and determining whether they should be permitted to see something in the application, RBAC governs security based on the role of the user within an organization.
- For example, rather than giving permission to John Smith, an architect in New York, RBAC would give permission to a role for U.S. architects. John Smith may be one of many users with that role.
- Thus, RBAC guarantees regulatory persons that only specific users have access to sensitive information, as it gives all approvals based on roles.

RBAC VS ACL CON.

- **RBAC is generally considered to be a preferred method for business applications.**
- **RBAC is more effective than ACL in relation to administrative overheads and security.**
- **ACL is best used for applying security at the individual user level.**
- **Can use RBAC to serve a company-wide security system, which an administrator monitors.**
- **An ACL can, for example, provide write access to a certain file, but it cannot define how a user can modify the file.**

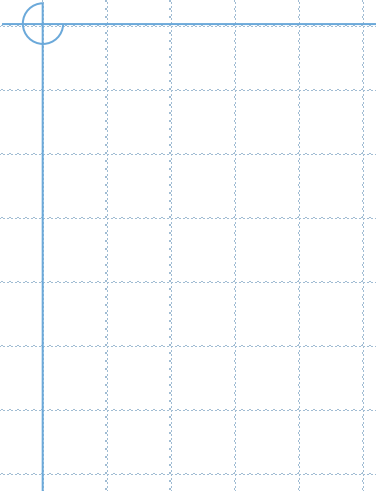
RBAC VS ACL CON.



Example of a role-based access control (RBAC) system

ROLE-BASED ACCESS CONTROL WITH IMPERVA

- Imperva allows for control of user privileges using flexible role-based access controls.
- Users are provided with view-only, edit, or restricted access to management functions and objects.
- Organizations can also hierarchically group and manage IT assets into categories for fine-grained access control, even in Managed Security Service Provider (MSSP) deployments and large-scale enterprise.



Q&A