Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

ACL systems

Mahmoud Barakat

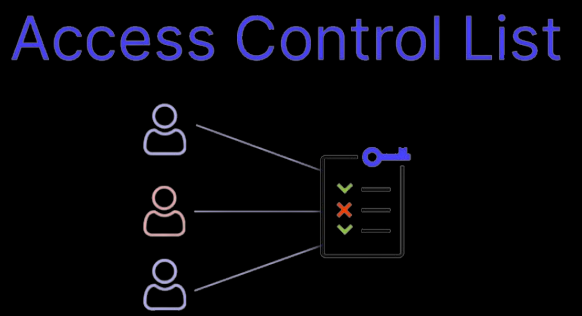
Big Data Management und Analytics in datenzentrischen Wissenschaften
Prof. Patrick Fuhrmann

Agenda

- What is ACL?
- Types of ACLs
- How ACL works?
- Access Check Algorithm
- ACL on Network
- Why ACL?
- RBAC vs ACL
- Demo
- Access control vulnerabilities and privilege escalation – Hack for Money!
- Questions?

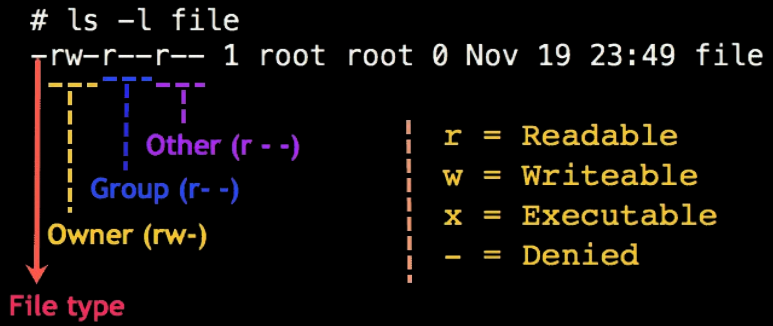
What is access control list?

- An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
- Each entry in a typical ACL specifies a subject and an operation.
  - Ex: Read, Write Permission



Types of ACLs

- Filesystem ACLs



- Networking ACLs

Source	Destination	Protocol	Size	CPS
117.18.237.139,https	192.168.1.2,60120	tcp	23K	7319
117.18.237.139,https	192.168.1.2,60001	tcp	21K	6980
117.18.237.139,https	192.168.1.2,59999	tcp	19K	2060
117.18.237.139,https	192.168.1.2,60117	tcp	15K	4726
117.18.237.139,https	192.168.1.2,60394	tcp	13K	7087
r-199-59-150-39.t,https	192.168.1.2,50477	tcp	9K	1693
117.18.237.139,https	192.168.1.2,60119	tcp	5437	1513
192.168.1.2,59999	117.18.237.139,https	tcp	3636	532
192.168.1.2,60394	117.18.237.139,https	tcp	3171	938
192.168.1.2,60120	117.18.237.139,https	tcp	2931	722
192.168.1.2,60001	117.18.237.139,https	tcp	2872	706
192.168.1.2,60117	117.18.237.139,https	tcp	2248	758
192.168.1.2,48146	173.255.230.5,http	tcp	2145	1722
192.168.1.2,60119	117.18.237.139,https	tcp	2132	652
192.168.1.2,50477	r-199-59-150-39.t,https	tcp	1918	43
173.255.230.5,http	192.168.1.2,48146	tcp	871	
117.18.237.139	192.168.1.2	tcp	512	272
192.168.1.2,59312	snt-re2-7b.sjc.dro,http	tcp	352	
192.168.1.2,46777	jabber.odesk,xmpp-clien	tcp	312	23
jabber.odesk,xmpp-clien	192.168.1.2,46777	tcp	312	20
snt-re2-7b.sjc.dro,http	192.168.1.2,59312	tcp	283	
192.168.1.2	r-199-59-150-39.twttr.c	tcp	128	

How ACL works?

- A filesystem ACL is a table that informs the operating system of the access privileges a user has to a system object.

- Networking ACLs are installed in routers, where they act as traffic filters.

Access Check Algorithm

If
the user ID of the process is the owner

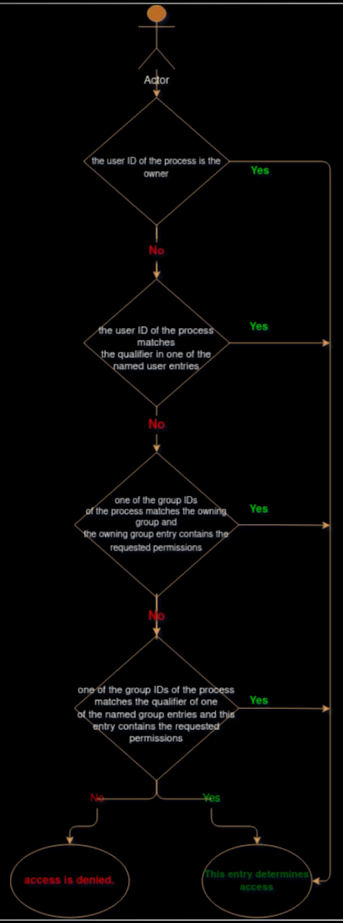
else if
the user ID of the process matches the qualifier in one of the named user

else if
one of the group IDs of the process matches the owning group and the owning group entry contains the requested permissions

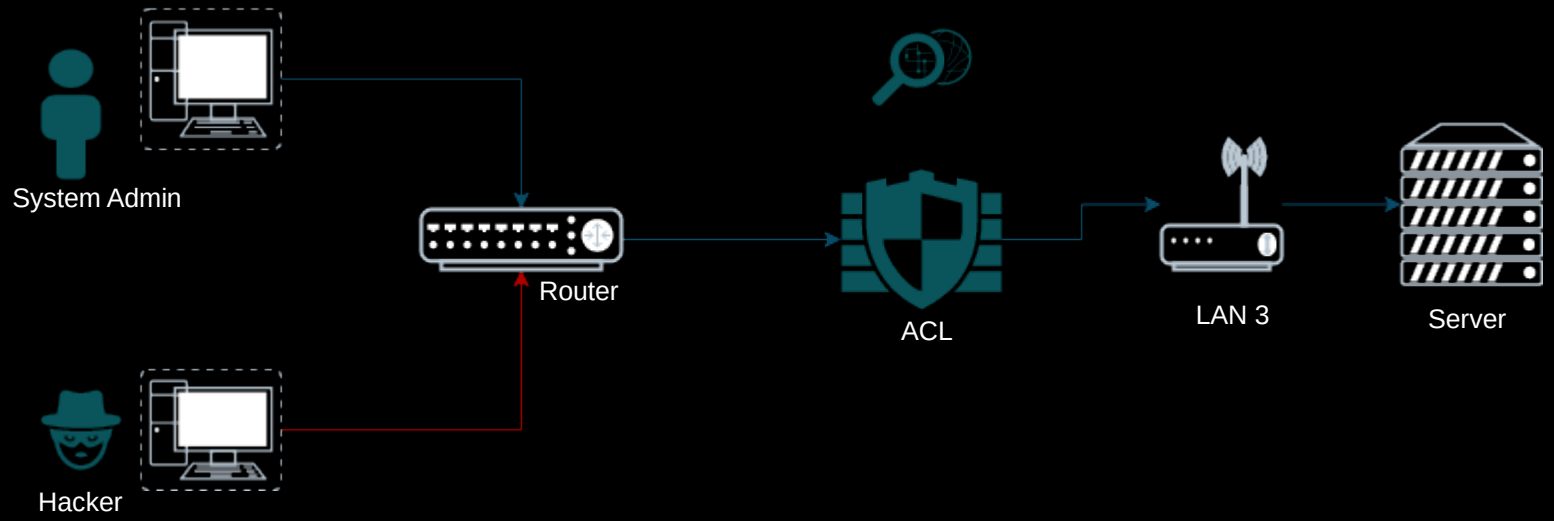
else if
one of the group IDs of the process matches the qualifier of one of the named group entries and this entry contains the requested permissions

else if
one of the group IDs matches the owning group or any of the named group, but neither the owning group nor any of the matching named group contains the requested permissions

else
the other entry determines access.



Network

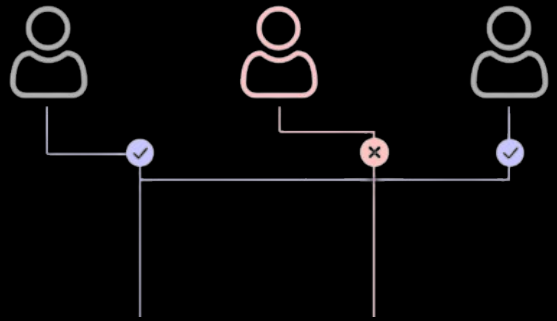


Reasons to use an ACL

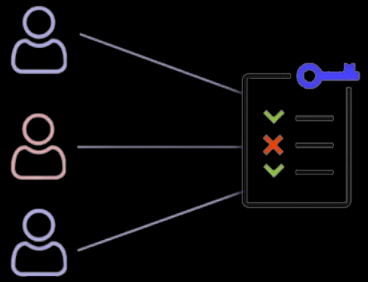
- Traffic flow control.
- Restricted network traffic for better network performance.
- A level of security for network access specifying which areas of the server/network/service can be accessed by a user and which cannot.
- monitoring of the traffic exiting and entering the system.

RBAC vs ACL

RBAC



Access Control List



Demo Time

- VIDEO OR LIVE

Hack for money!

Thursday, June 27, 2019 at 11:44 PM

Our reply

Hi Mahmoud Barakat,

After reviewing this issue, we have decided to award you a bounty of $1000. Below is an explanation of the bounty amount. Facebook fulfills its bounty awards through Bugcrowd.

This vulnerability reported an issue where the link used for donation on iOS devices were not logging out users and could thus be used in session fixation attacks.

Thank you for reporting this to us

Thank you again for your report. We look forward to receiving more reports from you in the future!

20 #824802 **URN Request bypass ACL Checks** Share:

TIMELINE

jeriko_one submitted a report to **Internet Bug Bounty**. Mar 19th (2 years ago)

Summary:

Attacker can bypass ACL checks gaining access to restricted HTTP servers such as those running on localhost. Attacker could also gain access to CacheManager if VIA
header is turned off. Only lines with : will be readable though, and the response must be less than 4096 bytes or it'll trigger the Heap Overflow I reported earlier.

This is due to URN request being transformed into HTTP request, and not going through the ACL checks that incoming HTTP request go through.

<= Squid-4.8 Vulnerable
Fixed in Squid-4.9
Squid Announce: http://www.squid-cache.org/Advisories/SQUID-2019_8.txt
Assigned CVE-2019-12523

19 #824203 **Cache Manager ACL Bypass** Share:

TIMELINE

jeriko_one submitted a report to **Internet Bug Bounty**. Mar 19th (2 years ago)

Summary:

ACL Manager can be bypassed giving non authorized users to squid-internal-mgr.
Possible to bypass other url_regex, but only focused on manager.

<= Squid-4.7 vulnerable
Silently Fixed in Squid-4.8
Announce page was allocated, but never made http://www.squid-cache.org/Advisories/SQUID-2019_4.txt As another issue similar to this wasn't fixed

Patch: http://www.squid-cache.org/Versions/v4/changesets/squid-4-e1e861eb9a04137fe81decd1c9370b13c6f18a18.patch

Assigned: CVE-2019-12524

Reported March 19, 2020 12:53am +0100

jeriko_one

Participants

State Resolved ()

Reported to Internet Bug Bounty

Disclosed August 27, 2021 1:28am +0200

Severity Critical (9.3)

Weakness *None*

Bounty $12,000

CVE ID *None*

Disclosed August 27, 2021 1:32am +0200

Severity Critical (9.1)

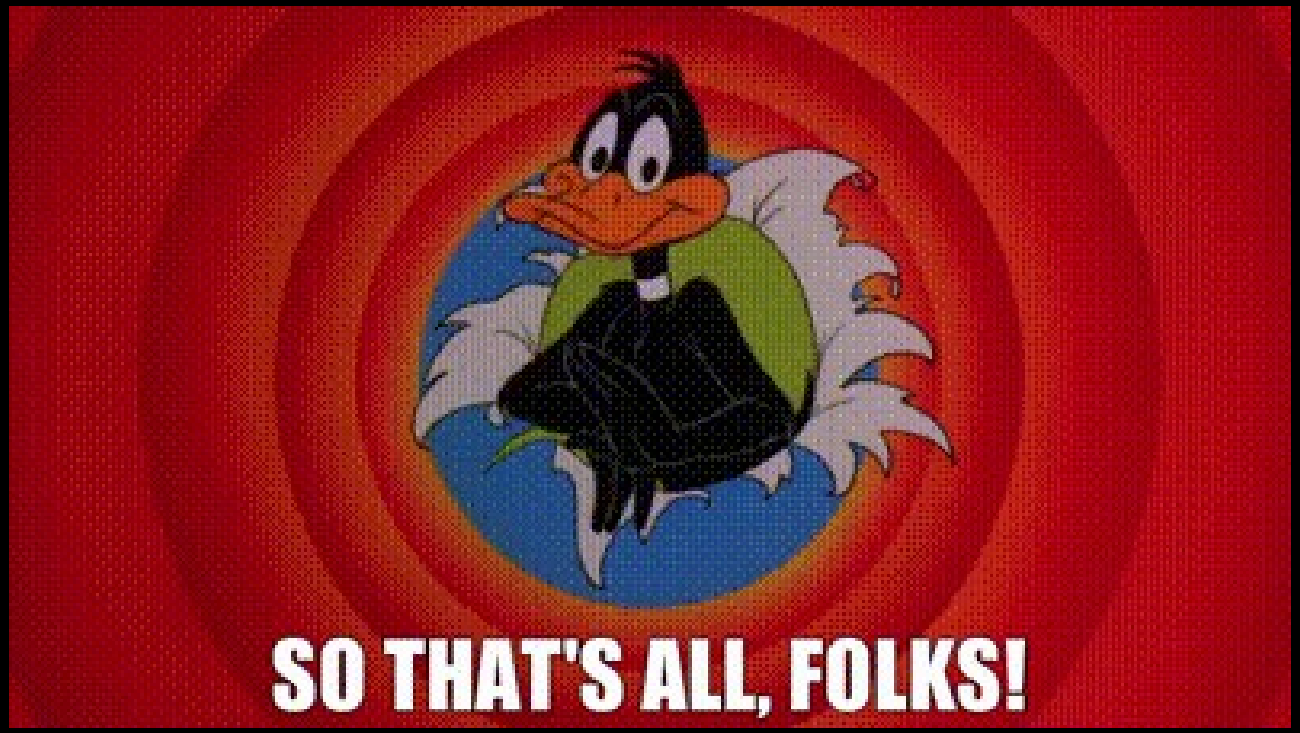
Weakness *None*

Bounty $12,000

CVE ID *None*

Any Questions?

SO THAT’S ALL, FOLKS!



Resources

- https://www.imperva.com/learn/data-security/access-control-list-acl/
- https://www.consul.io/docs/security/acl/acl-system
- https://en.wikipedia.org/wiki/Access-control_list
- https://portswigger.net/web-security/access-control
- https://www.comparitech.com/net-admin/create-configure-acl/
- https://itglobal.com/company/glossary/access-control-list/
- https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL
- https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8151_ra_2620_asg/content/ch10s04.html
- https://www.facebook.com/whitehat/thanks/
- https://www.draw.io
- https://www.youtube.com/watch?v=zXZgsVPRqnw
- https://www.usenix.org/legacy/publications/library/proceedings/usenix03/tech/freenix03/full_papers/gruenbacher/gruenbacher_html/main.html