Access Control / Berechtigungen

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Gliederung

- Access Control allgemein
- Logische Access Control Modelle
- Access Control Implementationen
- Virtuelle Maschinen & Containerisierung

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Access Control allgemein

- Steuerung vom Zugriff auf Ressourcen
- Physische und Logische Access Control
- Abgrenzung von Authentisierung, Authentifizierung und Autorisierung

Beispiele von physischer Access Control

Flughafengate

- Person durch Ausweis authentisieren
- Ticket durch Abgleichen mit Flugplätzen authentifizieren
- Person dazu autorisieren, das Flugzeug zu betreten

Beispiele von physischer Access Control

Schlösser

- Person durch Schlüssel authentisieren
- Schlüssel durch Abgleich authentifizieren
- Person dazu autorisieren, die Tür zu öffnen

Logische Access Control

- Access Control von Softwaresystemen
- Granularität: kleinste schützbare Einheit
- Operationen: lesen, schreiben, ausführen usw.
- Zugang: welche Methode benutzt wird

Beispiele von logischer Access Control

Anmeldebildschirm

- Granularität: grob, Zugriff auf den ganzen Benutzer
- Operationen: lesen, schreiben und löschen
- Zugang: Nutzerkennung ggfs. mit Passwort oder PIN

Beispiele von logischer Access Control

Dateifreigabe

- Granularität: fein, ein Ordner oder eine Datei
- Operationen: lesen, schreiben oder löschen
- Zugang: Rechte durch Besitzer von Datei/Ordner erlangen

Logische Access Control Modelle

Mandatory Access Control

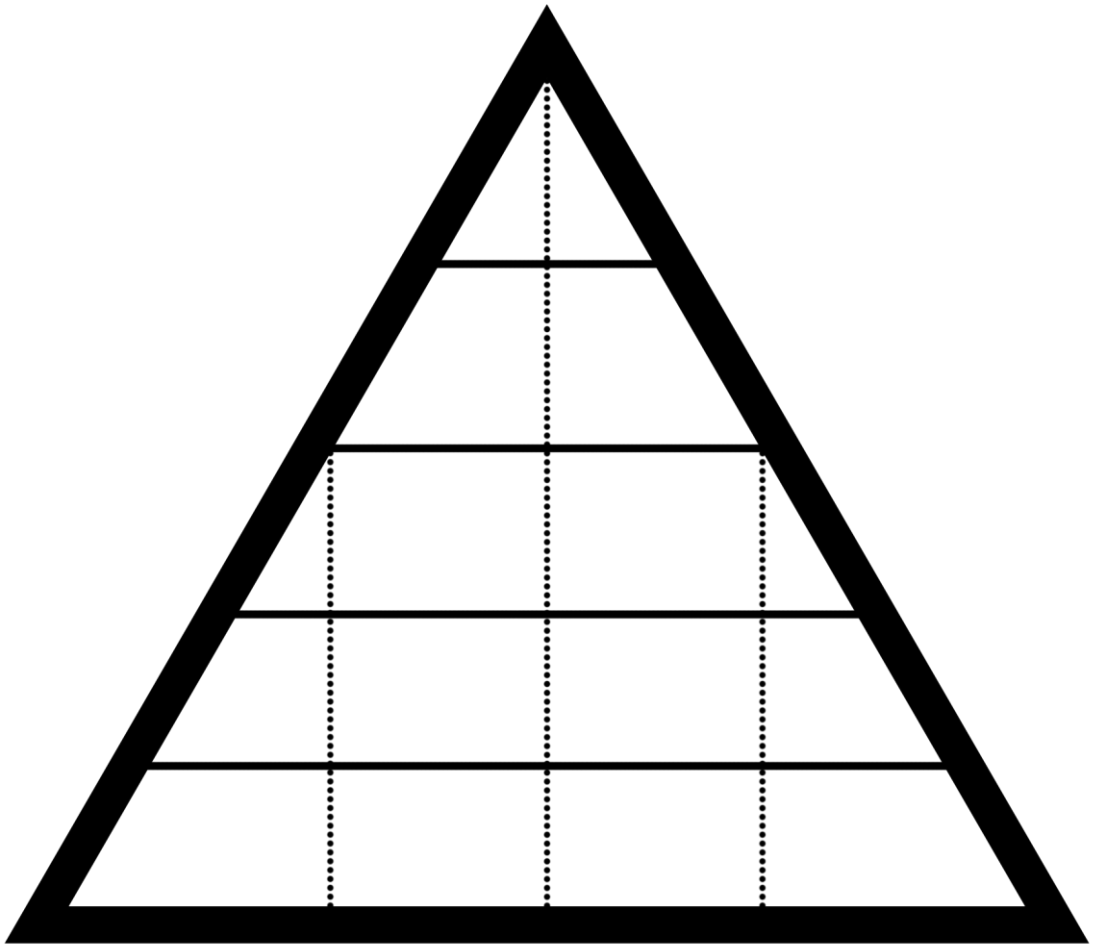
- Zugriffsrechte werden zentral von einem Administrator gesteuert
- Sowohl Nutzer als auch Dateien haben Labels
- Labels sind hierarchisch angeordnet
- Wird häufig in Regierungsorganisationen eingesetzt

Logische Access Control Modelle

Role Based Access Control

- Nutzer werden vom Admin in Rollen eingeteilt
- Jede Rolle hat bestimmte Rechte
- Vertikale Sicht im Gegensatz zur horizontalen Sicht von MAC
- RBAC und MAC werden teilweise gleichzeitig eingesetzt

Logische Access Control Modelle



Logische Access Control Modelle

Discretionary Access Control

- Zugriff auf Ressourcen basiert auf Identität
- Jedes Subjekt (zB Nutzer oder Programm) hat eine Identität
- Jede Identität hat eine eigene Menge von Rechten
- Rechte werden von anderen Subjekten erteilt und entzogen

Logische Access Control Modelle

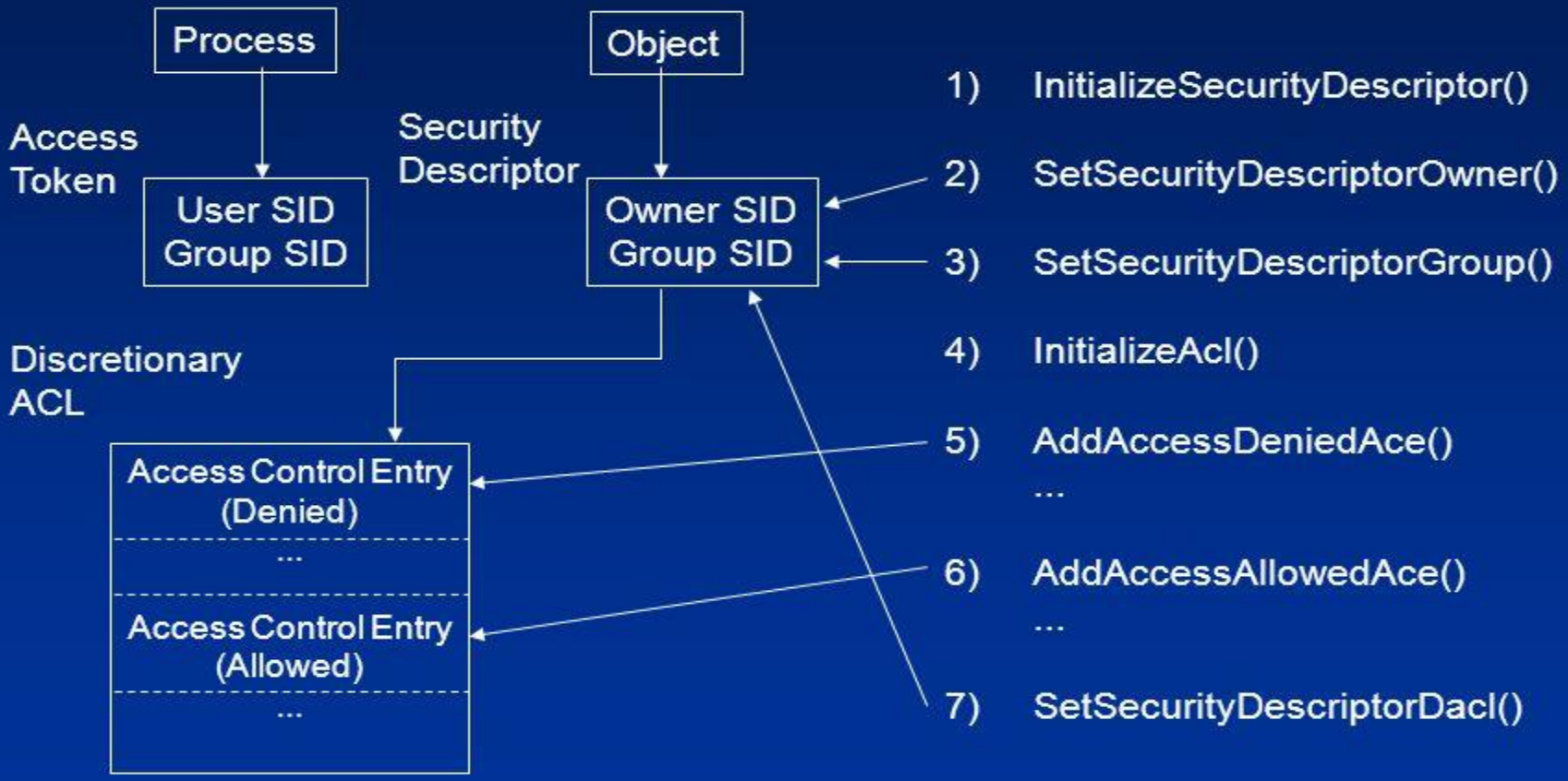
Access Control List

- Liste aus Nutzern bzw. Gruppen und Dateien
- Wird von den meisten bekannten Betriebssystemen implementiert
- Access Control Entries bestimmen Rechte
- Meistens zusammen mit DAC benutzt

Access Control Implementation: Windows

- Zwei Elemente: „Access Tokens“ und „Security Descriptors“
- Der Access Token hat alle relevanten Informationen über den Nutzer
- Wichtig für Access Control sind die SID
- Die Security Descriptors beinhalten SID über Objekte

Constructing a Security Descriptor



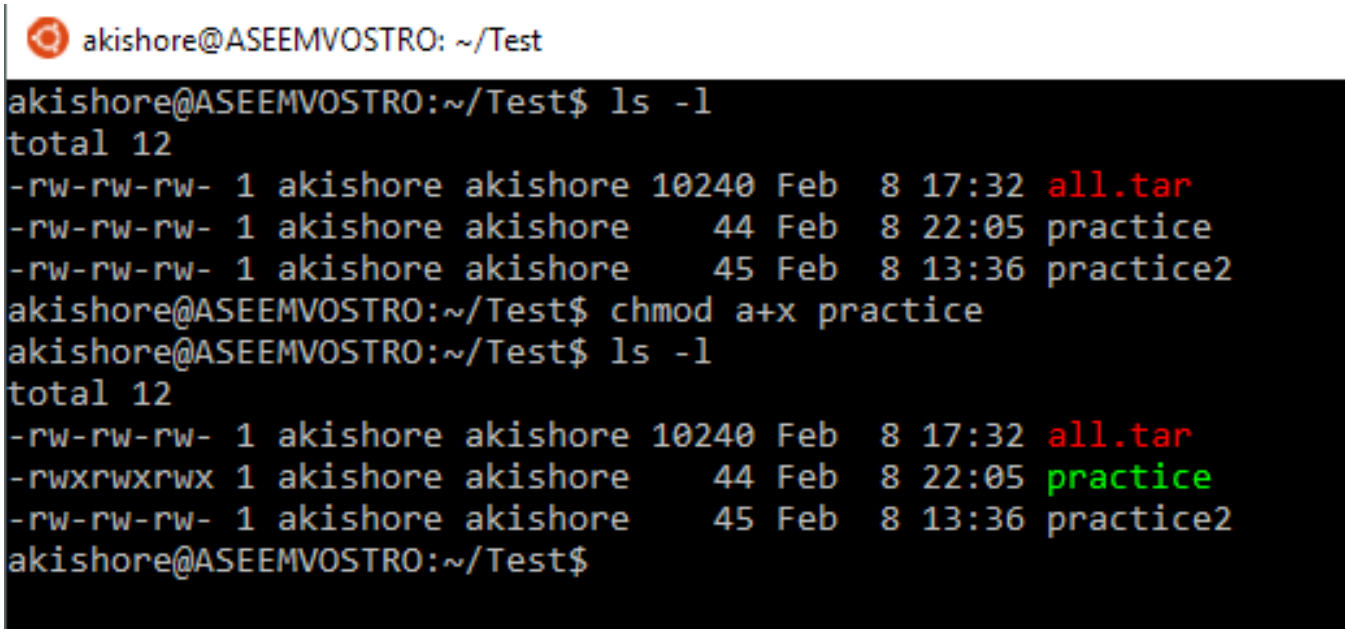
Quelle: https://slideplayer.com/slide/7028404/

Access Control Implementation: Linux

- Simpleres System als bei Windows
- Jedes Objekt hat jeweils für Besitzer, Gruppen und alle anderen Berechtigungen, die in 3 bit codiert sind
- Das resultiert in einer dreistelligen Oktalzahl
- Mit chmod kann man Berechtigungen verändern

Access Control Implementation: Linux

Numeric Value	Permission
0	---
1	--x
2	-w-
3	-wx
4	r--
5	r-x
6	rw-
7	rwx



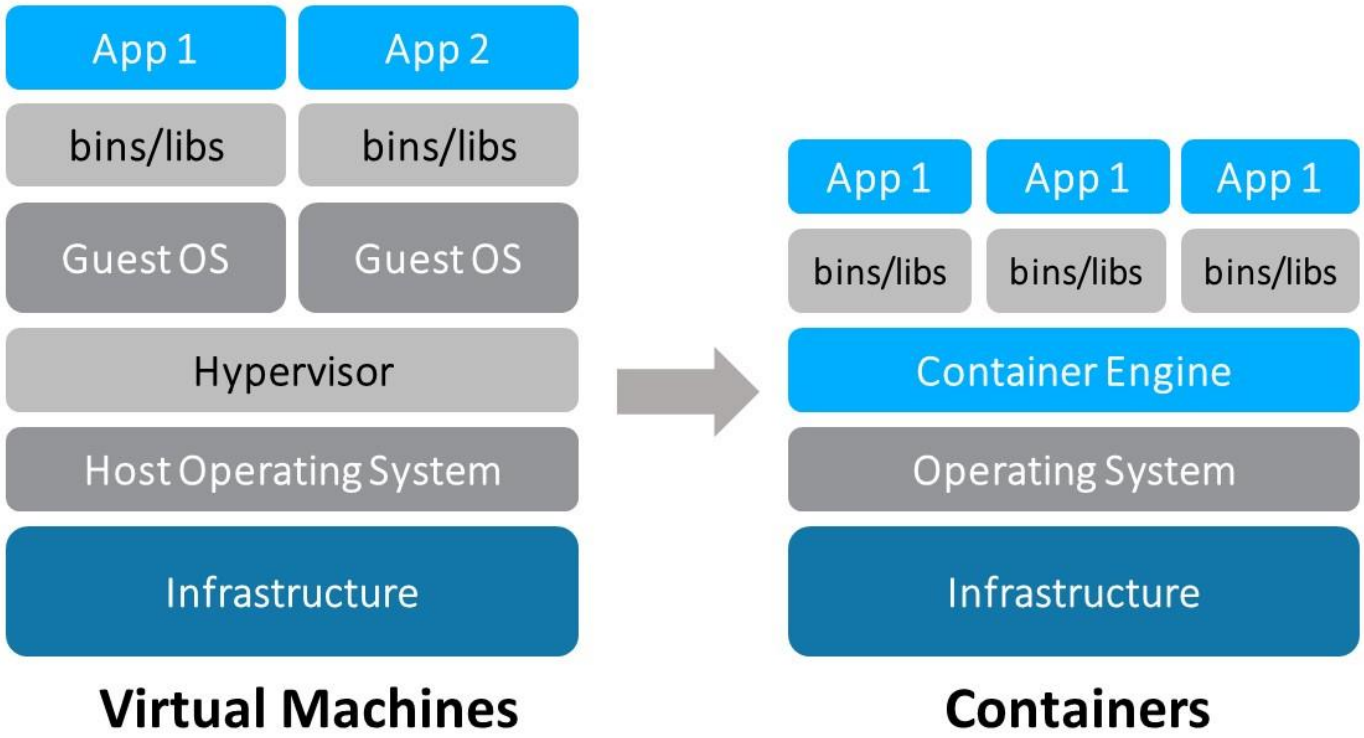
Quelle links: https://trainwithctg.com/wp-content/uploads/2018/04/Octal-Table.png

Quelle rechts: https://s10629.pcdn.co/wp-content/pictures/2017/02/chmod-usage-linux.png

Virtuelle Maschinen & Containerisierung

- Zwei Ansätze dafür, Anwendungen in fremden Umgebungen ausführen zu können
- Virtuelle Maschinen benutzen Hypervisor
- Stellen separate Systeme dar
- Container nutzen gemeinsame Daten

Virtuelle Maschinen & Containerisierung



Quelle: http://cdn.rancher.com/wp-content/uploads/2017/02/16175231/VMs-and-Containers.jpg

Virtuelle Maschinen & Containerisierung

- Isolation von Prozessen steht für mehr Sicherheit
- Aber: Die Isolation kann durchbrochen werden
- Vor allem bei Containern kann das schwerwiegende Folgen haben
- Deswegen wird davon abgeraten, Container nur als neue VM Lösung zu sehen

Vielen Dank für die Aufmerksamkeit!

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Quellen

- https://www.searchdatacenter.de/definition/Virtuelle-Maschine-Virtual-Machine-VM
- https://wiki.archlinux.org/index.php/File_permissions_and_attributes
- https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Technical
- https://docs.microsoft.com/de-de/windows/desktop/SecAuthZ/security-identifiers
- https://docs.microsoft.com/de-de/windows/desktop/SecAuthZ/access-tokens

Quellen

- https://docs.microsoft.com/en-us/windows/desktop/secauthz/dacls-and-aces
- https://docs.microsoft.com/en-us/windows/desktop/secauthz/access-control
- https://docs.microsoft.com/de-de/windows/desktop/SecAuthZ/security-descriptors
- https://www.tenouk.com/ModuleH2.html
- https://compas.cs.stonybrook.edu/~nhonarmand/courses/fa14/cse506.2/slides/ACLs-Vasu_and_Yaohui.pdf
- https://neuvector.com/container-security/containers-vs-virtual-machines-vms/

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Quellen

- https://www.datenschutzbeauftragter-info.de/authentisierung-authentifizierung-und-autorisierung/
- https://www.geeksforgeeks.org/access-control-listsacl-linux/
- https://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control
- https://entwickler.de/leseproben/containerisierung-der-it-579775782.html
- https://www.ca.com/de/blog-automation/was-ist-containerisierung-und-bedeutet-sie-das-ende-der-virtualisierung.html

Quellen

- https://wr.informatik.uni-hamburg.de/_media/teaching/wintersemester_2015_2016/nthr-1516-berreis-virtualization_and_containerization-ausarbeitung.pdf
- https://de.wikipedia.org/wiki/Access_Control_List
- https://de.wikipedia.org/wiki/Role_Based_Access_Control
- https://de.wikipedia.org/wiki/Mandatory_Access_Control
- https://de.wikipedia.org/wiki/Discretionary_Access_Control
- https://de.wikipedia.org/wiki/Zugriffskontrolle
- https://de.wikipedia.org/wiki/Hypervisor

Quellen

- https://slideplayer.com/slide/7028404/
- https://www.heise.de/newsticker/meldung/Hacker-brechen-aus-virtueller-Maschine-aus-3658416.html
- https://blog.docker.com/2016/03/containers-are-not-vms/
- https://trainwithctg.com/wp-content/uploads/2018/04/Octal-Table.png
- https://s10629.pcdn.co/wp-content/pictures/2017/02/chmod-usage-linux.png
- http://cdn.rancher.com/wp-content/uploads/2017/02/16175231/VMs-and-Containers.jpg