CS-301 Fall 2020 Mini-Exam 1

September 27, 2021

1 Security Principles

The World Economic Forum (WEF) has hired two different security consultants to revise its security mechanisms for controlling access to its conference venue in Davos because it is afraid that climate change activists might attempt to enter the venue without invitation. Consultant 1 suggests the following security measures to control access to the venue: "All invited participants will receive a badge before the start of the conference and only people carrying a badge will be allowed in. Guards securing the entries to the venue will check that every person entering the venue has a personalised badge. Furthermore, a list of invited participants is distributed to the guards and the guards will check the name of every person entering the venue in addition to the validity of badges." Consultant 2 suggests an alternative strategy: "Because climate activists are often young, no one below the age of 18 will be allowed into the venue and guards securing the entries to the venue will enforce this policy. Furthermore, there will be random checks by additional security guards patrolling the venue to ensure that activists who managed to sneak past the entry guards will be detected." Pick 2 out of the 8 main security principles and compare the two strategies in terms of their compliance with these principles, i.e., discuss whether each strategy satisfies your chosen principles. What strategy would you recommend the WEF to implement? Justify your choice.

2 Threat Modelling

Based on a recommendation from a friend, you have recently installed a new app on your phone that allows you to pre-order drinks at Satellite to avoid long queues on busy nights. The app is connected to your CAMIPRO account so that, once you have ordered the drinks through the app, your order is directly paid for from your account. Access to the app is password-restricted and each user can choose their own password when they first register.

3 Security Policies

Alice uses the Quickgram social network for sharing her photos with friends and family. Alice posts pictures about her studies at EPFL, her trips in Switzerland, and parties. The posts on Quickgram by default are visible to all Quickgram users. In the network's settings, Alice can narrow down the set of users who can see which posts. Consider two threat models: (a) a Quickgram user that is not Alice's friend who can access photos of Quickgram users, (b) Alice's parents that can also access photos of Quickgram users. (1) Come up with one hypothetical threat to Alice's privacy within each threat model. (2) Propose appropriate security policies for access to Alice's pictures that would prevent these threats that can be implemented using Quickgram settings as mentioned above. List all the principals and assets in the policies.

4 Unix permissions Alice

Alice owns a business and has decided to develop a program to keep track of the shop inventory and manage her employees. However she's not an expert in Unix permissions and has asked you to give her a hand in configuring the access control. Give a good configuration of the access control, using the Unix format, ensuring the following system requirements (e.g. *-rwxrw-r– user1 group2 'file3'*):

Users:

1. Alice is the owner of the business
2. Bob, Charlie and Dave are employees

Files:

1. Employees schedules are written in *f1.txt*.
2. Inventory is written in *f2.csv*
3. *f3* is a program to update the inventory (run everytime an item is bought by a client)
4. *f4* is a directory containing files for each employee's CV

Requirements:

1. Employees should be able to read their schedules but not modify them, only Alice should be able to.
2. Only Alice should have permission to access or modify the inventory file.
3. Both employees and Alice should be able to run the 'f3' program. This program requires read and write access to 'f2.csv' to work correctly.
4. Only Alice can delete or rename CV files from the 'f4' directory, but both

employees and Alice can add CVs to the directory.

5 Unix permissions Charlie

Charlie owns a business and has decided to develop a program to keep track of the shop inventory and manage his employees. However he's not an expert in Unix permissions and has asked you to give him a hand in configuring the access control. Give a good configuration of the access control, using the Unix format, ensuring the following system requirements (e.g. *-rwxrw-r– user1 group2 'file3'*):

Users:
1. Charlie is the owner of the business
2. Alice, Bob and Dave are employees

Files:
1. Inventory is written in *f1.csv*.
2. *f2* is a directory containing files for each employee's CV.
3. Employees schedules are written in *f3.txt*.
4. *f4* is a program to update the inventory (run everytime an item is bought by a client)

Requirements:

1. Employees should be able to read their schedules but not modify them, only Charlie should be able to.
2. Only Charlie should have permission to access or modify the inventory file.
3. Both employees and Charlie should be able to run the *f4* program. This program requires read and write access to *f1.csv* to work correctly.
4. Only Charlie can delete or rename CV files from the *f2* directory but both employees and Charlie can add CVs to the directory

6 Unix permissions Bob

Bob owns a business and has decided to develop a program to keep track of the shop inventory and manage his employees. However he's not an expert in Unix permissions and has asked you to give him a hand in configuring the access control. Give a good configuration of the access control, using the Unix format, ensuring the following system requirements (e.g. *-rwxrw-r– user1 group2 'file3'*):

Users:

1. Bob is the owner of the business
2. Alice, Charlie and Dave are employees

Files:
1. *f1* is a directory containing files for each employee's CV.
2. Inventory is written in *f2.csv*.
3. *f3* is a program to update the inventory (run everytime an item is bought by a client)
4. Employees schedules are written in *f4.txt*.

Requirements:

1. Employees should be able to read their schedules but not modify them, only Bob should be able to.
2. Only Bob should have permission to access or modify the inventory file.
3. Both employees and Bob should be able to run the *f3* program. This program requires read and write access to *f2.csv* to work correctly.
4. Only Bob can delete or rename CV files from the *f1* directory but both employees and Charlie can add CVs to the directory

7 ACL and Capabilities

Because of COVID-19, EPFL has decided to restrict access to the study rooms on campus: each student needs to book on the EPFL app a seat for the day in a study room to be able to get into the given room.
Propose a high-level mechanism for access control of the study rooms. List subjects, objects, and rights. Does your mechanism use the capability or access-control list model? Discuss the advantages and disadvantages of your proposal.