

Engineering Secure Software Systems Winter 2020/21

Exercise Sheet 12

issued: February 2, 2021

due: February 11, 2021

Exercise 12.1, uniqueness of unwindings (10 Points)

Show that P-unwindings are not unique, but that minimal P-unwindings are, that is:

1. give an example for a system M and a policy \succrightarrow such that there are (at least) two different P-unwindings for M and \succrightarrow ,
2. show that if M is P-secure with respect to a policy \succrightarrow , then there is a P-unwinding for M and \succrightarrow that is contained (via set inclusion) in all P-unwindings for M and \succrightarrow .

Exercise 12.2, IP-Security examples (10 Points)

Which of the following systems are IP-secure? Assume that as usual, the state names indicate the observations made by L , that lowercase letters denote actions performed by agents with the corresponding higher-case letter name, and the policy $H \succrightarrow D \succrightarrow L$. Additionally, assume that H and D make the same observation in each state of the system.

