Jan Rehwaldt
University of Tartu, Secure Programming Techniques, April 2012

Exercise 3:

1. *Describe 2 security set-ups that cannot be expressed with traditional Unix permission model*
2. *Describe 2 security set-ups that cannot be expressed with Unix ACL-enabled permission model*
3. *Describe 2 security set-ups that cannot be expressed with Windows 7 security model*

1a) This and all subdirectories as well as files have read-only access. In order to express this scenario the permissions have to be copied to all subfolders (e.g. by the OS), they are not automatically inherited.

1b) Everyone may not access the file (- - -). Owner may read and write, but not execute (r w -). User A can read, write and execute (r w e). User B can read and execute, but not write (r - x). There is no way to express more than the three parties owner, selectable group of user and everyone else.

2a) Group G may access the file fully (r w e). User A belongs to group G. User A may not access the file (- - -). As no negative permissions may be expressed this won't work.

2b) User A may write into a file, but not delete it. This won't work as only read-write-execute privileges are distinguished.

3a) User A is allowed to append content to a file, but not to overwrite it. This won't work as there is no distinction between those two made.

3b) Restrict modify permission for file owner is not possible, as the owner may overtake the modify-right. As the creator of a file is the initial owner this may be a problem.

Scenarios, which are not representable in higher levels (e.g. 3) are generally also not representable in lower levels (e.g. 1 or 2).