Access Control

Petr Ročkai

User Database on UNIX

- UNIX API: `#include <pwd.h>`
- implemented by `libc`
- uses the system-configured user database
  - `/etc/passwd` by default
  - but can also be network-based (LDAP)
- `getpwent`, `getpwnam`, …

ACLs on UNIX

- POSIX 1003.1e: the `acl_*` family
  - never made it out of draft (withdrawn in ’97)
- ACL is represented by (opaque) `acl_t`
- the data structure is quite complex
  - `acl_entry_t`, `acl_permset_t`, `acl_perm_t`

UNIX: ACLs and Files

- ACL is associated with an i-node
  - just like normal permissions
- by path: `acl_set_file` and `acl_get_file`
- by descriptor: `acl_set_fd`, `acl_get_fd`

UNIX and Capabilities

- also part of POSIX.1e
- manipulated using `cap_*` family of functions
  - `cap_set_proc`, `cap_set_file`, …
- individual capabilities are system-specific
  - `CAP_CHOWN`, `CAP_SYS_BOOT`, …
  - `/usr/include/linux/capability.h`

Exercise: ACLs on Windows

- write a C or C++ program to set ACLs on Windows
- create a test directory (using the program)
  - allow read access for everyone
  - make it so that such read access is inherited
  - check it works in the file properties dialog

Exercise: ACLs on Windows

- create 2 new files in the directory
- check that they inherited the right ACE
- deny access to the file content to yourself
- add one ACE to first file (keeping the others)
- replace the entire ACL on the second file with one ACE

Exercise: Resources

- refer to MSDN
- some of the functions you may want to use
  - `GetNamedSecurityInfo`
  - `SetNamedSecurityInfo`
  - `SetEntriesInAcl`
- other useful articles
  - Modifying the ACLs of an Object in C++
  - Access Control Lists

Homework: Invocation

- write a C (or C++) program that modifies ACLs on UNIX
- `./addacl directory '*.txt' user1 user2`
  - `directory` is a name of a directory (a path)
  - the `*.txt` is a pattern (a glob)
  - `user1` … `userN` are user names

Homework: Semantics

- find all matching files in the given directory (1pt)
- grant read access to all the users given as arguments (2pt)
- ensure pre-existing ACLs are undamaged (1pt)
- comment the code and write a short report (1pt)