

Handout 4 (Access Control)

Access control is essentially about deciding whether to grant access to a resource or deny it. Sounds easy, no? Well it turns out that things are not as simple as they seem at first glance. Let us first look, as a case-study, at how access control is organised in Unix-like systems (Windows systems have similar access controls, although the details might be quite different). Then we have a look at how secrecy and integrity can be ensured in a system, and finally have a look at shared access control in multi-agent systems.

Unix-Style Access Control

Following the Unix-philosophy that everything is considered as a file, even memory, ports and so on, access control in Unix is organised around 11 Bits that specify how a file can be accessed. These Bits are sometimes called the *permission attributes* of a file. There are typically three modes for access: **r**ead, **w**rite and **e**xecute. Moreover there are three user groups to which the modes apply: the owner of the file, the group the file is associated with and everybody else. This relatively fine granularity seems to cover many useful scenarios of access control. A typical example of some files with permission attributes is as follows:

```
1 $ ls -ld . * */*
2 drwxr-xr-x ping staff 32768 Apr 2 2010 .
3 -rw----r-- ping students 31359 Jul 24 2011 manual.txt
4 -r--rw--w- bob students 4359 Jul 24 2011 report.txt
5 -rwsr--r-x bob students 141359 Jun 1 2013 microedit
6 dr--r-xr-x bob staff 32768 Jul 23 2011 src
7 -rw-r--r-- bob staff 81359 Feb 28 2012 src/code.c
8 -r--rw---- emma students 959 Jan 23 2012 src/code.h
```

The leading **d** in Lines 2 and 6 indicate that the file is a directory, whereby in the Unix-tradition the **.** points to the directory itself. The **..** points at the directory “above”, or parent directory. The second to fourth letter specify how the owner of the file can access the file. For example Line 3 states that **ping** can read and write **manual.txt**, but cannot execute it. The next three letters specify how the group members of the file can access the file. In Line 4, for example, all students can read and write the file **report.txt**. Finally the last three letters specify how everybody else can access a file. This should all be relatively familiar and straightforward. No?

There are already some special rules for directories and links. If the execute attribute of a directory is *not* set, then one cannot change into the directory and one cannot access any file inside it. If the write attribute is *not* set, then one can change existing files (provide they are changeable), but one cannot create new files. If the read attribute is *not* set, one cannot search inside the directory (**ls -la** does not work) but one can access an existing file, provided one knows its name. Links to files never depend on the permission of the link, but the file they are pointing to. Otherwise one could easily change access rights to files.

While the above might sound already moderately complicated, the real complications with Unix-style file permissions involve the `setuid` and `setgid` attributes. For example the file `microedit` in Line 5 has the `setuid` attribute set (indicated by the `s` in place of the usual `x`). The purpose of `setuid` and `setgid` is to solve the following puzzle: The program `passwd` allows users to change their passwords. Therefore `passwd` needs to have write access to the file `/etc/passwd`. But this file cannot be writable for every user, otherwise anyone can set anyone else's password. So changing securely passwords cannot be achieved with the simple Unix access rights discussed so far. While this situation might look like an anomaly, it is in fact an often occurring problem. For example looking at current active processes with `/bin/ps` requires access to internal data structures of the operating system, which only root should be allowed to. In fact any of the following actions cannot be configured for single users, but need privileged root access

- changing system databases (users, groups, routing tables and so on)
- opening a network port below 1024
- interacting with peripheral hardware, such as printers, harddisk etc
- overwriting operating system facilities, like process scheduling and memory management

This will typically involve quite a lot of programs on a Unix system. I counted 90 programs with the `setuid` attribute set on my bog-standard Mac OSX system (including the program `/usr/bin/login` for example). The problem is that if there is a security problem with only one of them, be it a buffer overflow for example, then malicious users can gain root access (and for outside attackers it is much easier to take over a system). Unfortunately it is rather easy to cause a security problem since the handling of elevating and dropping access rights in such programs rests entirely with the programmer.

The fundamental idea behind the `setuid` attribute is that a file will be able to run not with the callers access rights, but with the rights of the owner of the file. So `/usr/bin/login` will always be running with root access rights, no matter who invokes this program. The problem is that this entails a rather complicated semantics of what the identity of a process (that runs the program) is. One would hope there is only one such ID, but in fact Unix distinguishes three(!):

- *real identity*
This is the ID of the user who creates the process; can only be changed to something else by root.
- *effective identity*
This is the ID that is used to grant or deny access to a resource; can be changed to either the real identity or saved identity by users, can be changed to anything by root.

- *saved identity*

If the `setuid` bit set in a file then the process is started with the real identity of the user who started the program, and the identity of the owner of the program as effective and saved identity. If the `setuid` bit is not set, then the saved identity will be the real identity.

As an example consider again the `passwd` program. When started by, say the user `foo`, it has at the beginning the identities:

- *real identity: foo*
effective identity: foo
saved identity: root

It is then allowed to change the effective identity to the saved identity to have

- *real identity: foo*
effective identity: root
saved identity: root

It can now read and write the file `/etc/passwd`. After finishing the job it is supposed to drop the effective identity back to `foo`. This is the responsibility of the programmers who wrote `passwd`. Notice that the effective identity is not automatically elevated to `root`, but the program itself must make this change. After it has done the work, the effective identity should go back to the real identity.

Despite this complicated semantics, Unix-style access control is of no use in a number of situations. For example it cannot be used to exclude some subset of people, but otherwise have files readable by everybody else (say you want to restrict access to a file such that your office mates cannot access a file). You could try setting the group of the file to this subset and then restrict access accordingly. But this does not help, because users can drop membership in groups. If one needs such fine-grained control over who can access a file, one needs more powerful *mandatory access controls* as described next.

Secrecy and Integrity

Often you need to keep information secret within a system or organisation, or secret from the “outside world”. An example would be to keep insiders from leaking information to competitors. An instance of such an access control system is the secrecy levels used in the military. There you distinguish usually four secrecy levels:

- top secret
- secret
- confidential

- unclassified

The idea is that the secrets classified as top-secret are most closely guarded and only accessible to people who have a special clearance. The unclassified category is the lowest level not needing any clearance. While the idea behind these security levels is quite straightforward, there are some interesting phenomena that you need to think about when realising such a system. First this kind of access control needs to be *mandatory* as opposed to *discretionary*. With discretionary access control, the users can decide how to restrict or grant access to resources. With mandatory access control, the access to resources is enforced “system-wide” and cannot be controlled by the user. There would be no point to let users set the secrecy level, because if they want to leak information they would set it to the lowest. Even if there is no malicious intent, it could happen that somebody by accident sets the secrecy level too low for a document. Note also that the secrecy levels are in tension with the Unix-style access controls. There root is allowed to do everything, but in a system enforcing secrecy, you might not like to give root such powers.

There are also some interesting rules for reading and writing a resource that need to be enforced:

- **Read Rule:** a principal P can read a resource O provided P 's security level is at least as high as O 's
- **Write Rule:** a principal P can write a resource O provided O 's security level is at least as high as P 's

The first rule implies that a principal with secret clearance can read secret documents or lower, but not documents classified top-secret. The second rule for writing needs to be the other way around: someone with secret clearance can write secret or top-secret documents—no information is leaked in these cases. In contrast the principal cannot write confidential documents, because then information can be leaked to lower levels. These rules about enforcing secrecy with multi-level clearances are often called *Bell/LaPadula* model, named after two people who studied such systems.

A problem with this kind of access control system is when two people want to talk to each other but are assigned different security clearances, say secret and confidential. In these situations, the people with the higher clearance have to lower their security level and are not allowed to take any document from the higher level with them to the lower level (otherwise information could be leaked). In actual systems, this might mean that people need to log out and log into the system again—this time with credentials for the lower level.

While secrecy is one property you often want to enforce, integrity is another. This property ensures that nobody without adequate clearance can change, or tamper with, systems. An example for this property is a *fire-wall*, which isolates a local system from threads from the Internet, for example. The rule for such a system is that somebody from inside the fire-wall can write resources outside the firewall, but you cannot write a resource inside the fire-wall from outside.

Otherwise an outside can just tamper with a system in order to break in. In contrast we can read resources from inside the fire-wall, for example web-pages. But we cannot read anything from outside the fire-wall. Lest we might introduce a virus into the system (behind the fire-wall). In effect in order to ensure integrity the read and write rules are reversed from the case of secrecy:

- **Read Rule:** a principal P can read a resource O provided P 's security level is lower or equal than O 's
- **Write Rule:** a principal P can write a resource O provided O 's security level is lower or equal than P 's

This kind of access control system is called *Biba* model, named after Kenneth Biba. Its purpose is to prevent data modification by unauthorised principals.

The somewhat paradoxical result of the different reading and writing rules in the *Bell/LaPadula* and *Biba* models is that we cannot have secrecy and integrity at the same time in a system, or they need to be enforced by different means.

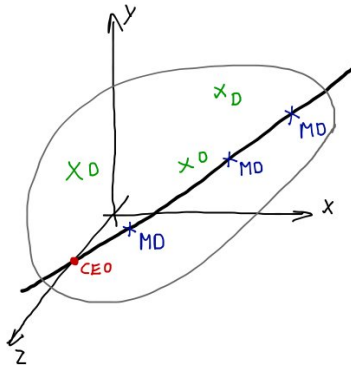
Multi-Agent Access Control

In military or banking, for example, very critical decisions need to be made using a *two-people rule*. This means such decisions need to be taken by two people together, so that no single person can defraud a bank or start a nuclear war (you will know what I mean if you have seen the classic movie "Dr Strangelove or: How I Learned to Stop Worrying and Love the Bomb"¹). Translating the two-people rule into a software system seems not as straightforward as one might think.

Let us assume we want to implement a system where CEOs can make decisions on their own, for example whether or not to sell assets, but two managing directors (MDs) need to come together to make the same decision. If "lowly" directors (Ds) want to take this decision, three need to come together. Remember cryptographic keys are just sequences of bits. A naive solution to the problem above is to split the necessary key into n parts according to the "level" where the decision is taken. For example one complete key for a CEO, halves of the key for the MDs and thirds for the Ds. The problem with this kind of sharing a key is that there might be many hundreds MDs and Ds in your organisations. Simple-minded halving or division by three of the key just does not work.

A much more clever solution was proposed by Blakley and Shamir in 1979. This solution is inspired by some simple geometric laws. Suppose a three-dimensional axis system. We can, clearly, specify a point on the z-axis, say, by specifying its coordinates. But we could equally specify this point by a line that intersects the z-axis in this point. How can a line be specified? Well, by giving two points in space. But as you might remember from school days, we can specify the point also by a plane intersecting the z-axis and a plane can be specified by three points in space. This could be pictured as follows:

¹http://en.wikipedia.org/wiki/Dr._Strangelove



The idea is to use the points as keys for each level of shared access. The CEO gets the point directly. The MDs get keys lying on a line and the Ds get keys lying on the plane. Clever, no? Scaling this idea to more dimensions allows for even more levels of access control and more interesting access rules, like one MD and 2 Ds can take a decision together.

Is such a shared access control used in practice? Well military command-chains are obviously organised like this. But in software systems often need to rely on data that might not be entirely accurate. So the CEO-level would correspond to the in-house data-source that you can trust completely. The MD-level would correspond to simple errors where you need three inputs and you decide on what to do next according to what at least two data-sources agree (the third source is then disregarded, because it is assumed it contains an error). If your data contains not just simple errors, you need levels corresponding to Ds.

Further Information

If you want to know more about the intricacies of the “simple” Unix access control system you might find the relatively readable paper about “Setuid Demystified” useful.

<http://www.cs.berkeley.edu/~daw/papers/setuid-usenix02.pdf>

About secrecy and integrity, and shared access control I recommend to read the chapters on “Nuclear Command and Control” and “Multi-Level Security” in Ross Anderson’s Security Engineering book (whose first edition is free).