Logistics 80 Mark Exam
5 Mark In Class Test - Week 5
5 Mark Assignment - Week 8

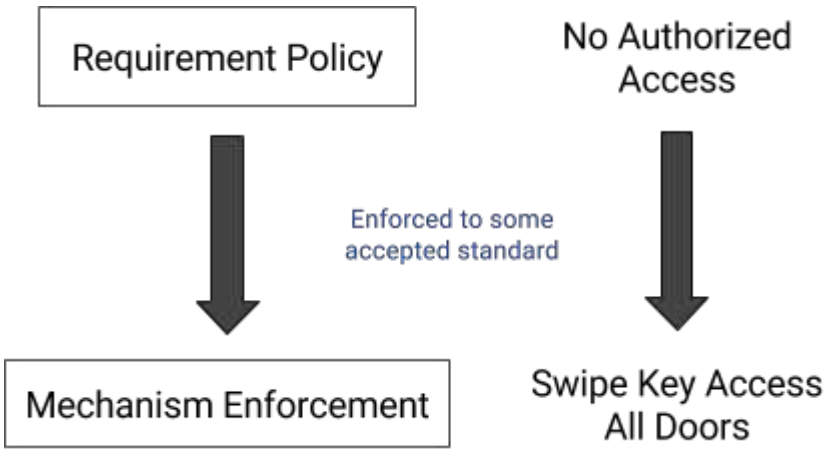
Last year the course was focused on end to end security with the existence of attackers on the network. This course will focus instead and the security of the system.

Attacker comes from outside (Over a network)
Attacker comes from within the system (Malicious Code)

So, this course is about the principles of system security.

But what is meant by system security?
What does it mean for a system to be considered secure ?

No Unauthorized access (Needs an enforcement mechanism)
No external operation on normal operation.
Has an authorized access policy.
No internal influence on normal operation. (no one on the inside poses a threat)



We add things that we can afford to make things / system more secure.
We do this to an acceptable level of defence against attack.

What is meant by security and where does the Policy come from ?

This means that we must define the threat **and** decide the security policy to which it adheres.

Consider the server

`cs1.ucc.ie`

Many people have access to this server and suppose one of them creates a shell script

```
/bin/sh
chmod a + rwx $home
/bin/ls
```

And this user has a "." (dot) in their PATH

```
PATH ".;/bin/usr/bin
```

Such that when the next user when looking for a file called the **`ls`** command , the shell script called ls runs and modifies the content

is the server cs1.ucc.secure ?

Well it depends on what you call secure , this attack has not violated any of the rules of linux since the user who ran the script has access to their own files.

This attack was performed from someone inside the system on another but has broke no security.