Computer Security (COM-301)

Mandatory Access Control

Live exercise solving

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Mixing models

To protect both the integrity and the confidentiality of the assets in your system, you decide to establish policies following both BIBA and BLP security models setting the same integrity and confidentiality security levels. As a result:

(a) All subjects can read files on security levels that dominate them

(b) Subjects can read only within their own security level

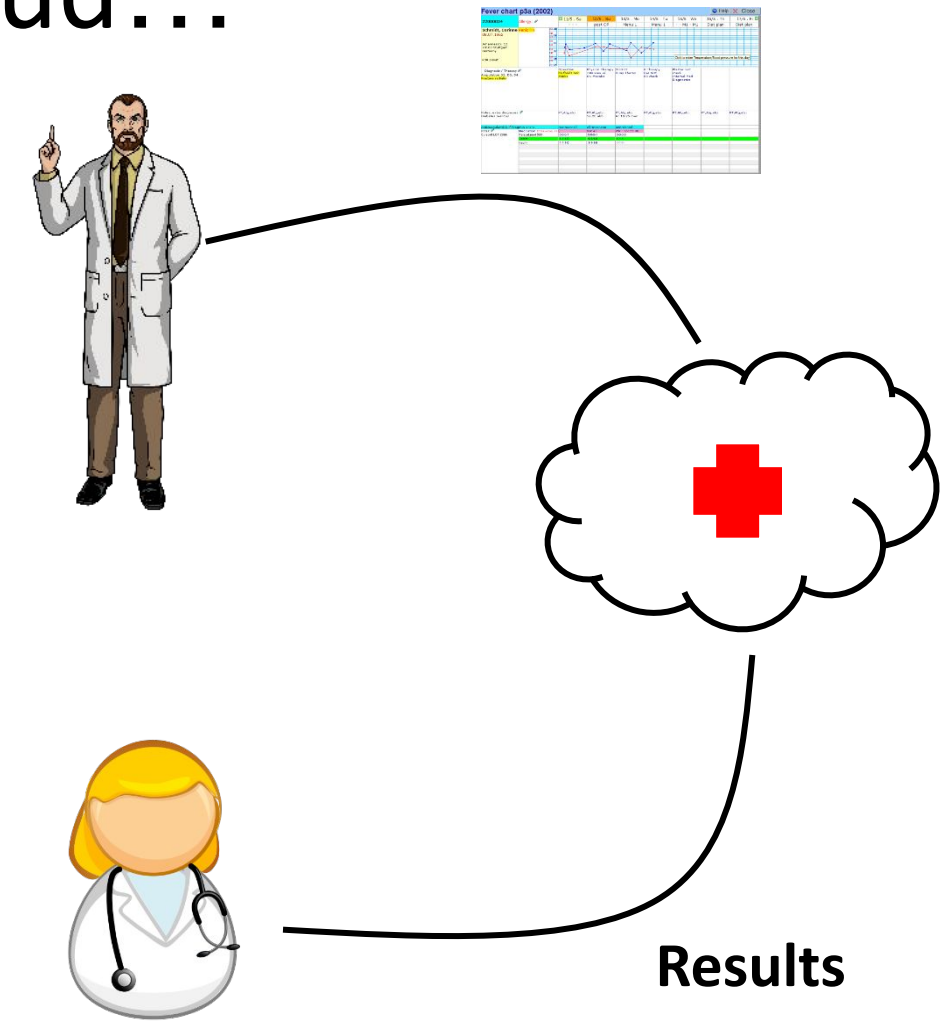
(c) Subjects can read and write only within their own security level

(d) No subject can read or edit any files

A hospital buys an internal cloud…

To process internal clinical data. They ask you, their Chief Security Officer to design the security and privacy policy.

Explain how the Bell LaPadula model can help you reason about this use case.



Covert communication

You decide to help a journalist on an investigation about your current employer EvilCorp. The journalist asks you to inform them about the times when EvilCorp Boss' is in the office. The journalist asks you to communicate via email, but as he knows that your email is monitored at work, they give you an address that will not raise suspicion. However, you cannot directly write the times, as that would raise alarms.

Propose a covert channel to let the journalist know about the Boss' schedule

Respecting Chinese Wall

Assume two Conflict of Interest classes COI1={C1, C2, C3} and COI2={C4, C5, C6}

Assume that you have a consultancy firm. Consultancy services may involve read, write or both accesses to the company dataset. Consider the following requirements:

- Providing consulting services to C1 requires read and write access to C1 records.
- Providing consulting services to C2 requires read access to C2 records.
- Providing consulting services to C3 requires read and write access to C3 records.
- Providing consulting services to C4 requires read and write access to C4 records.
- Providing consulting services to C5 requires read access to C5 records.
- Providing consulting services to C6 requires read access to C6 records.

What is the minimum number of consultants you would need to ensure that you provide consultancy services to the six companies as per the Chinese Wall model? Show the consultant to company assignments.