EPFL

SPRING

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

(c)
BLP implies that subjects cannot read above their level, and cannot write below
BIBA implies that subjects cannot read below their level, and cannot write above

As a result subjects can only read and write in their own level.

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

A covert channel has to be undetectable (otherwise would be not covert).

The covert channel can be implemented:

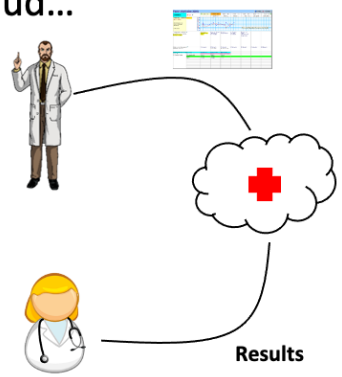
- In the content of the message, by including particular elements pre-agreed with the journalist.
- In the metadata of the message, by sending the message at a given time, with a particular size,…

Remember that the channel cannot be detected. This means that the message has to look as normal as possible. (Note that one can even prepare "normality" by changing other messages to make the new message understandable.)

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.



4

How you can think about this is:

Two subjects: analysts (Dr Krieger) and doctors (Dr. Alice)
Two objects: Research data, and results of the research analysis
Security levels (same for objects' classification and subjects' clearance, for simplicity): Research (high confidentiality) and Practitioner (low confidentiality).

Analysts have clearance "Research" and doctors have clearance "Practitioner"
Research data has classification "Research" and results have clearance "Practitioner"

When we reason like this, we notice that:
The doctors cannot have access to the research data (research data has a higher classification level than the doctors' clearance).
The analysts cannot write on results (results have a lower classification level than the analysts).

From this, it follows that when we reveal the results to the doctors we are performing an act of declassification. Therefore, we need to be extremely careful

that this information does not leak anything about the research data.
This includes intentional covert channels; but also inadverted information that may be inferred from the result. How to safely release information is a very active research field both in academia and industry.

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.

Case 1: assume read and write are equally important for establishing an information flow.

We have two sets of conflicts.

How can we assign employees?

Employee A -> C1, implies that A cannot work with C2, C3.
Employee A -> C1, C4, implies that A cannot work with C2, C3, C5, C6 -> need another employee
Employee B -> C2, implies that B cannot work with C1, C3.
Employee B -> C2, C5, implies that B cannot work with C1, C3, C4, C6 -> need another employee
Employee C -> C3, C6

Need 3 employees, minimum.

Case 2: only reading is not enough to establish an information flow. Information flow

from CX to CY only happens if an employee that can read CX, can write on CY.

In this case, an employee that works on C1 or C3 cannot work on C2; and an employee that works on C4 cannot work for C5 and C6.

Employee A -> C1, implies that A cannot work with C2,C3.
Employee A -> C1, C4, implies that A cannot work with C2, C3, C5, C6 -> need another employee
Employee B -> C3, implies that B cannot work with C1, C2.
Employee B -> C3, C5, implies that B cannot work with C1, C2, C4 but can work with C6. -> need another employee
Employee C -> C2

Need 3 employees, minimum.