Information Flow Modeling

Security

Otago Polytechnic
Dunedin, New Zealand

What is wrong with this?

1. A user supplies a password.
2. A password checking method hashes the password.
3. The method requests the stored hashed password from a database.
4. The method compares the two and returns true if the hashed passwords match.

The problem

- The password database is a high security value information source.
- The password checking method is a lower security value function.
- Information flowed from a higher security area to a lower security area.
- There is a possibility that information could have been leaked.

Instead, the password checking method should have queried the database to see if it held a hashed password that matched the one prepared from user input.

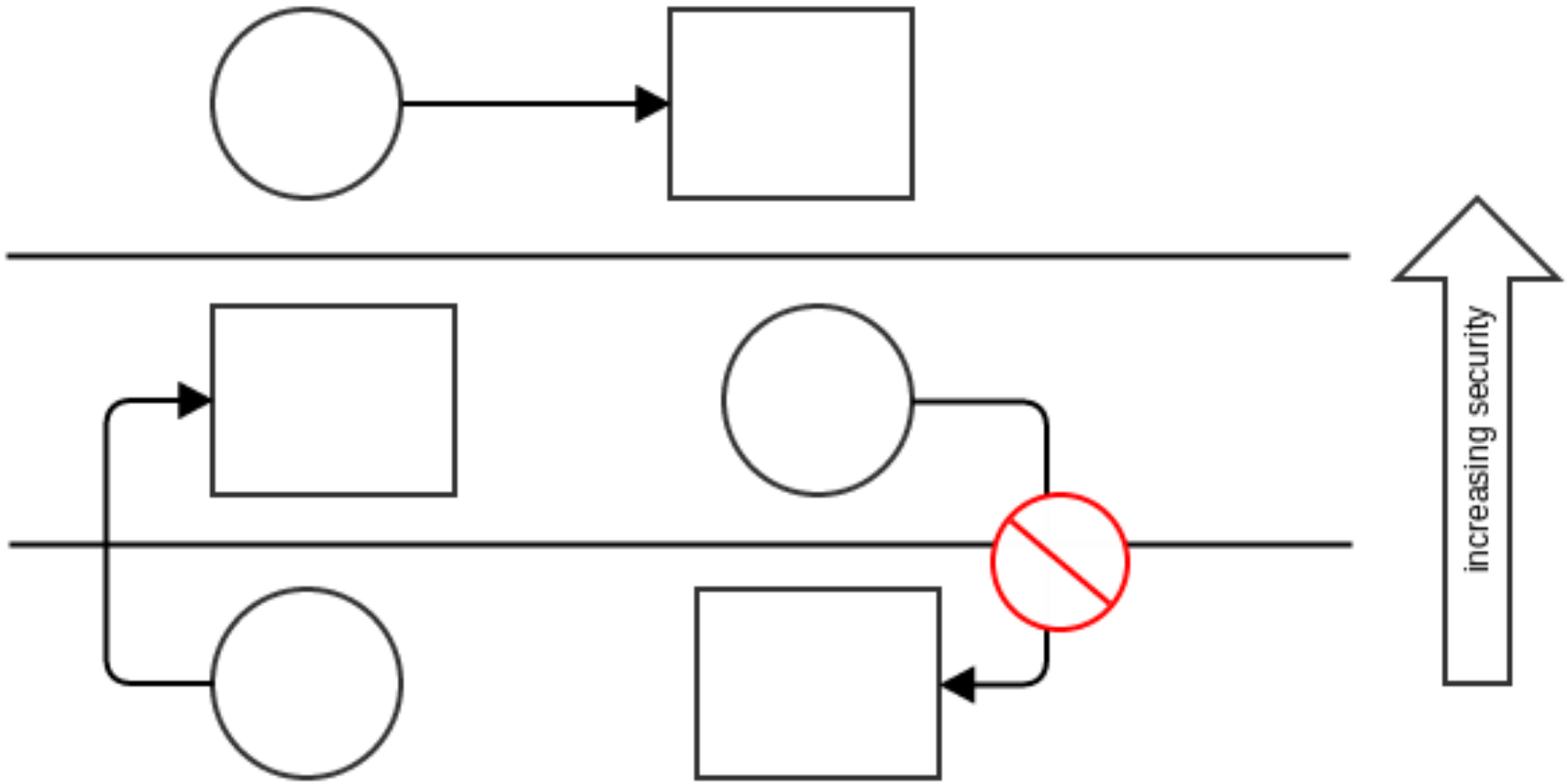
Information Leakage

The difficulty with information leakage at this level is that it's not the result of coding errors. It's the result of *system design* errors. We need to find design principles to guard against this.

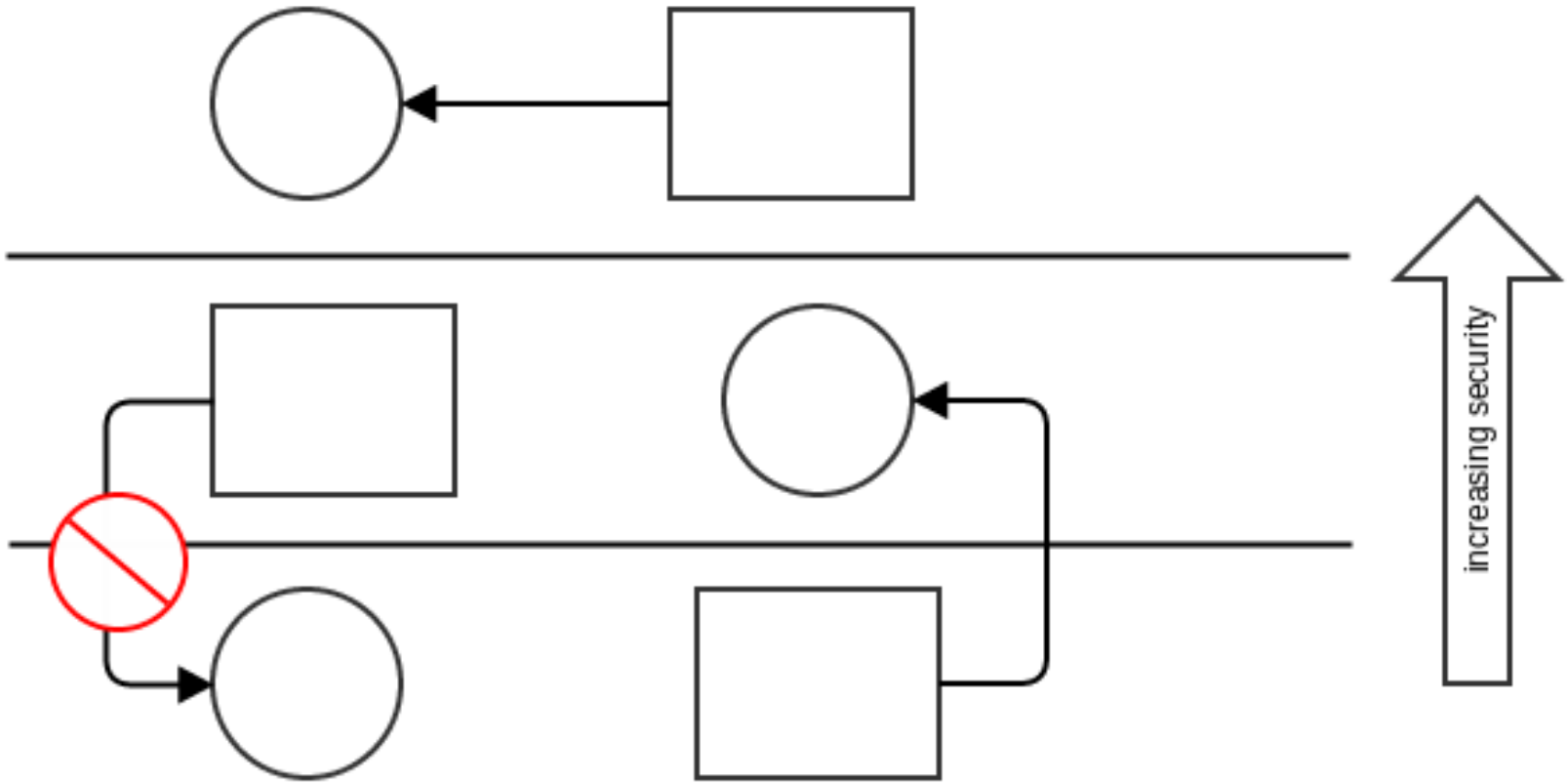
Bell-LaPadula Model

- Originally developed to formalise military security classifications.
- We divide our problem domain into a hierarchy of security levels.
- We have rules for how information can flow from one level to the next.

Write operations



Read operations



Exercises