

Security foundations

Privileges Permission & Authority



Authority

The effects that an entity can accomplish, either independantly OR INDIRECTLY.



Permission

The effects that an entity can accomplish
INDEPENDANTLY.



Principle Of Least Privilege (POLP)

Saltzer and Schroeder 1975

“Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.”

Privilege ?

Commonly used term.
Not unambiguous in its meaning!



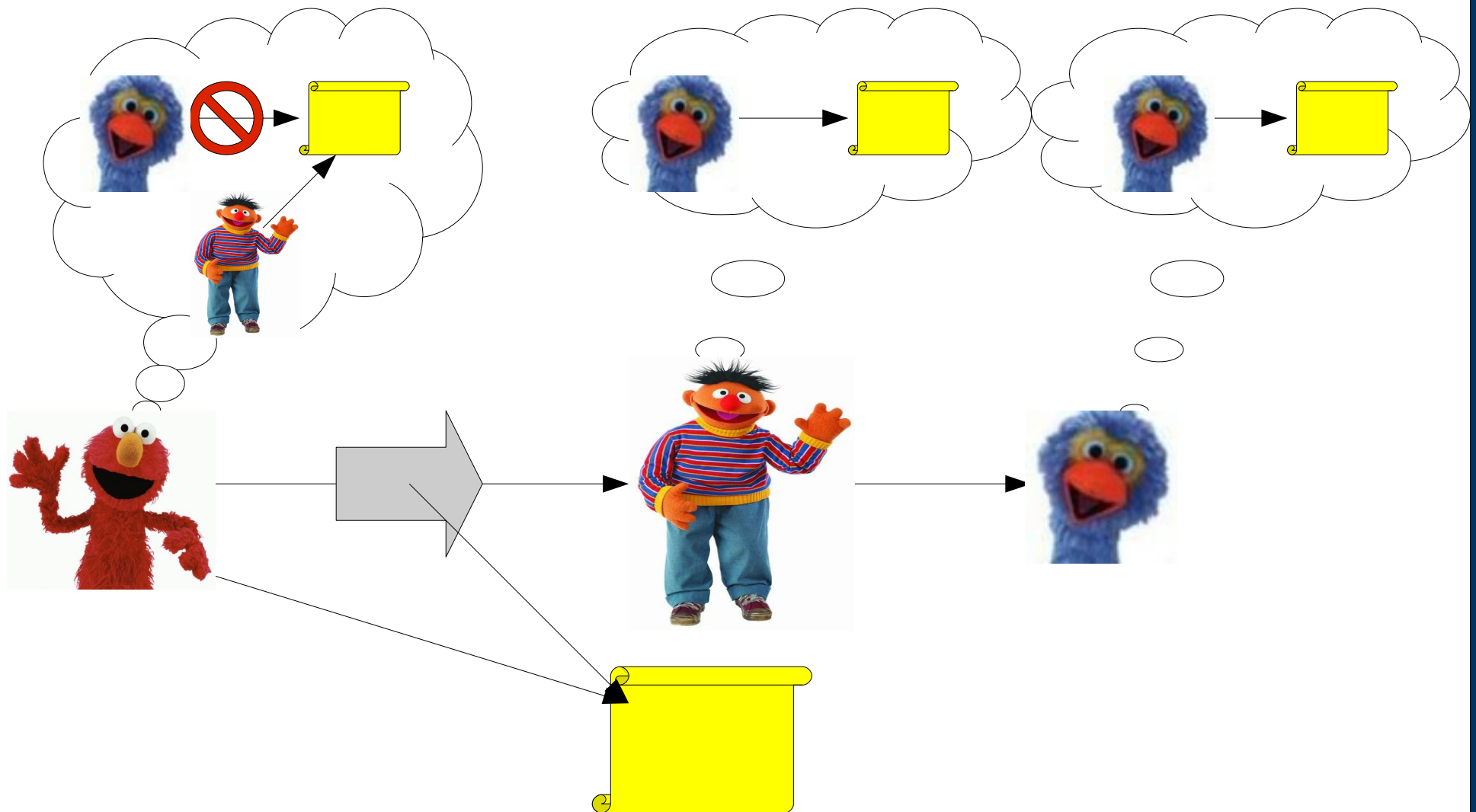
Privilege ?

- LBAC/MLS community:
 - Privilege == Permission
 - POLP == Principle Of Least **Permission**
- ZBAC/OCAP community:
 - Privilege == Authority
 - POLP == Principle Of Least **Authority**

Delegation

- Delegation of permissions can be limited and in many systems isn't possible.
 - Manipulation of discretionary access controls by subject.
 - Directly sharing authorization tokens.
 - Delegation of authority in the presence of a communication channel is ALWAYS possible.
 - Manipulation of discretionary access controls by subject.
 - Directly sharing authorization tokens.
 - Becoming a PROXY.
-
-

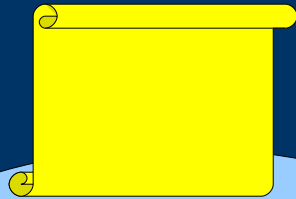
Cooperating Conspirators



Cooperating Conspiritors

- In the presence of a bi-directional communication channel between subjects, re-delegation is **IMPOSSIBLE** to prohibit.

Covert channels



Erny process

CPU
core

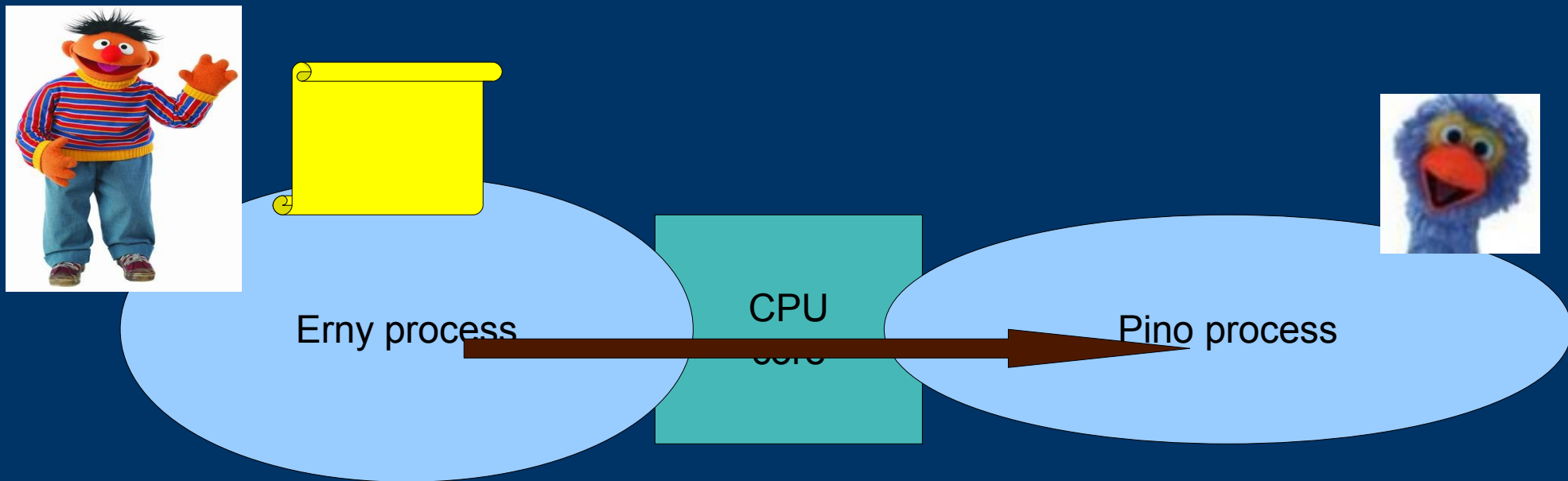


Pino process



Covert channels

- A shared resource can between cooperating conspirators be used as a covert communication channel.



Cooperating Conspiritors & covert channels.

- Practically every shared resource is usable as a covert channel.
 - This makes re-delegation practically impossible to prohibit in any environment with shared resources.
 - Sufficiently isolating resources to fully prevent covert channels, and thus prohibit re-delegation is extremely difficult and expensive.
-
-

Delegatie : LBAC/MLS

- Keep security levels sufficiently separated
- Avoid re-delegation of permissions.
- Re-delegation is the enemy of the Principle Of Least Privilege (Permission).



Delegatie: ZBAC/OCAP

- Don't prohibit what you can not prevent.
- Re-delegation of attenuated or decomposed authority is a tool in accomplishing security goals.
- Re-delegation is the best friend of the Principle Of Least Privilege (Authority).



Recap

- Privilege is a concept that has a violently different meaning for different groups of security professionals
 - Don't add to the confusion, avoid using the word 'privilege' when it matters.
 - LBAC en ZBAC proponents advocate opposite policies with respect to re-delegation of privileges
 - CIA: Cheap Integrity and Availability versus expensive Confidentiality.
-
-