THE PRINCIPLE OF THE LEAST PRIVILEGE

AWS SECURITY

SECURITY …

- … is an attribute of something and is meaningless by itself
- … depends on the established trust model
- … most of the times opposes convenience

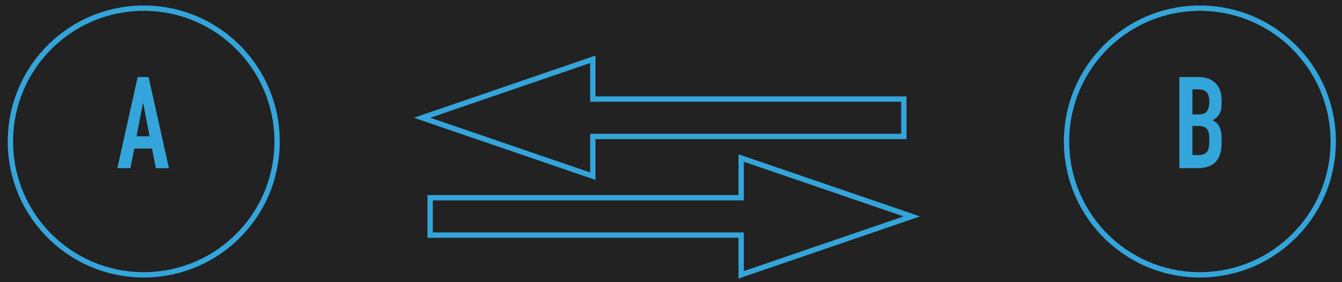
AWS SECURITY | THE PRINCIPLE OF THE LEAST PRIVILEGE

> EVERY PROGRAM AND EVERY USER OF THE SYSTEM SHOULD OPERATE USING THE LEAST SET OF PRIVILEGES NECESSARY TO COMPLETE THE JOB.

J. H. Saltzer

The Protection of Information in Computer Systems (1975)

IT IS ALL ABOUT RELATIONSHIPS . . .



. . . AND CONTROLS YOU PUT IN PLACE TO MANAGE THE COMMUNICATIONS

COMMUNICATION IS A TWO-WAY STREET

- … so you need to ensure that you control both directions from a viewpoint of the domain you are securing
- Controlling the ingress (inbound) communication is usually easy and straight-forward
- Controlling the egress (outbound) communication is harder and not always possible

WHITELIST VS BLACKLIST?

- Blacklisting seems to be easier but it is retrospective and there are almost always a way to bypass it
- Whitelisting is deterministic and ensures that you are getting the expected results
- Whitelisting is harder to implement
- Fallback to blacklisting only if whitelisting is unfeasible