University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Reference monitor

bristol.ac.uk

Access Control in OS

- Subjects (i.e. process) are associated with a security context
  - Linux: user identity, group identity and a set of privileges
- Objects (e.g. files) are associated with security information
  - Linux: owner, group and permission vector

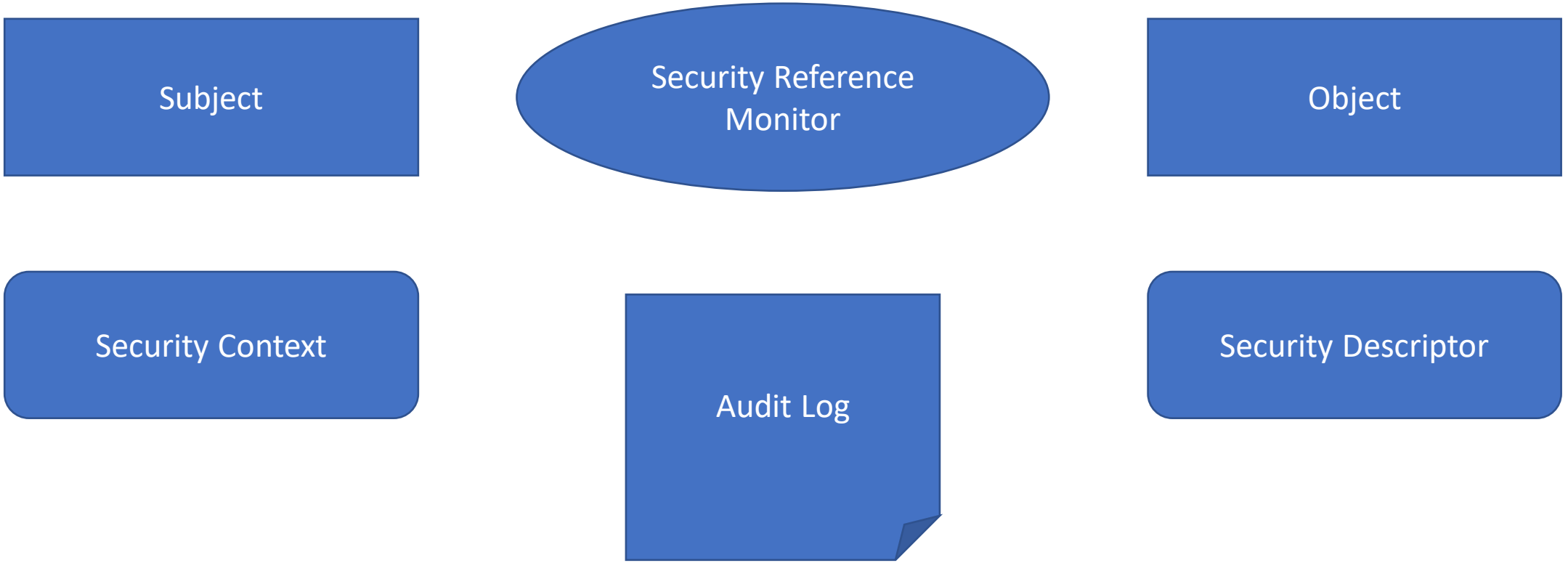
Access Control in OS

- Subjects (i.e. process) are associated with a security context
  - Linux: user identity, group identity and a set of privileges
- Objects (e.g. files) are associated with security information
  - Linux: owner, group and permission vector

On login:

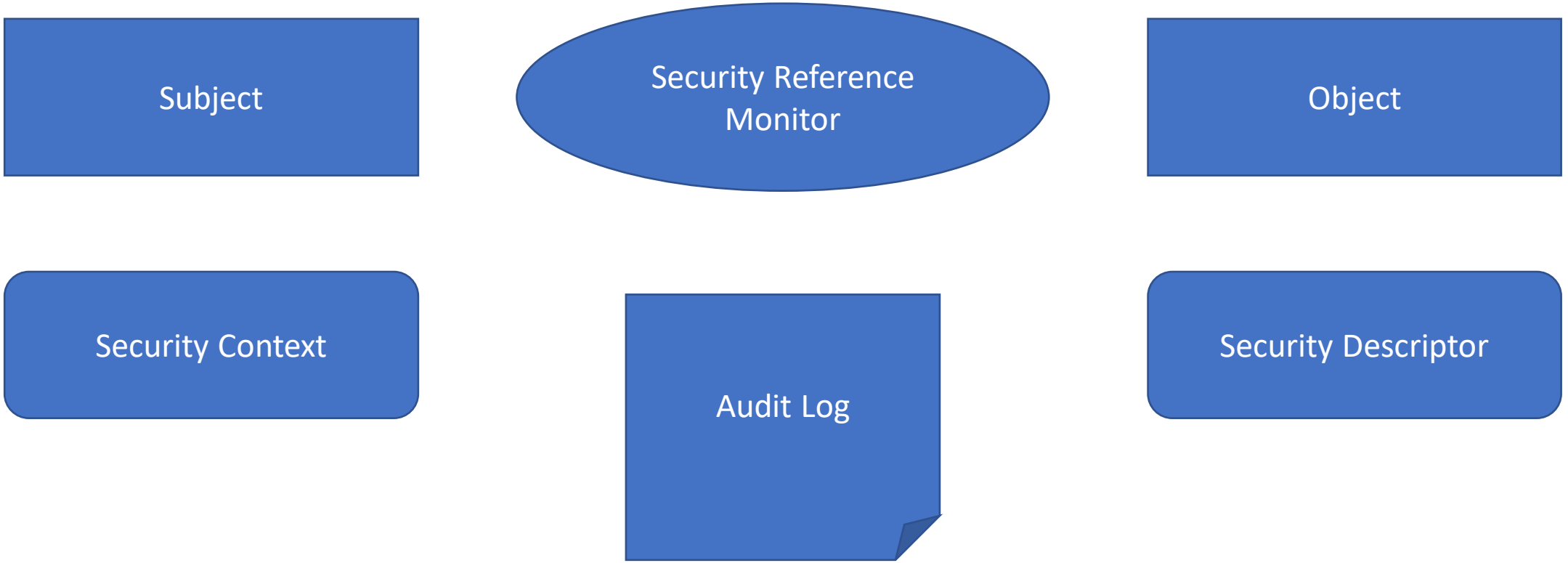
- Process created with the security context of the principal
- Descendent of this process inherit this security context

Reference Monitor



Reference Monitor

All interactions between subjects and objects must be mediated by the reference monitor



Reference Monitor

- Basic behavior on system call:
  - retrieve subject and object security information
- Apply policy based on security information
  - e.g. compared user/group id with read/write privileges
- Log decision
- Return decision

Reference Monitor

- Basic behavior on system call:
  - retrieve subject and object security information
- Apply policy based on security information
  - e.g. compared user/group id with read/write privileges
- Log decision
- Return decision

CAREFUL WITH RACE CONDITIONS

MAC

- Mandatory Access Control
- Access decision are not in the hand of objects owner, but system wide
- Simplest MAC is Multi-level security
  - Emerged from US military
  - Objects associated with security classificiation
    - Unclassified
    - Confidential
    - Secret
    - Top secret

MLS

- Bell-LaPadula model (confidentiality)
  - READ: may not read from an object with higher clearance than the subject
  - WRITE: may not write to an object with lower clearance than the subject
  - no-read-up, no-write-down
- Biba (integrity)
  - READ: may not read to an object with lower clearance than the subject
  - WRITE: may no write to an object with higher clearance than the subject
  - no-read-down, no-write-up

Security Criteria

- *The Trusted Computer System Evaluation Criteria* (aka *The Orange Book*)
- Define criteria to assess the security of a system (we summarize)
  - Grade D: minimal (nothing is done)
  - Grade C: discretionary protection
    - C1: provide users with mean to protect private data and to prevent accidental read or destruction of data (traditional UNIX or Windows would fit there)
    - C2: C1 + users must be accountable through logging of their actions (you can get UNIX or Windows system there by turning some options)
  - Grade B: mandatory protection
    - B1: C2 + informal statement of security and means to enforce mandatory access control on named subjects and objects. (Linux + AppArmor)
    - B2: B1 + formal security policy and MAC extend to all subjects and objects. (Linux + SELinux)
    - B3: B2 + smaller TCB and extensive testing, extended audit mechanism, tamperproofness and detailed recovery procedure.
  - Grade A: verified protection
    - A: B3 + formal verification.