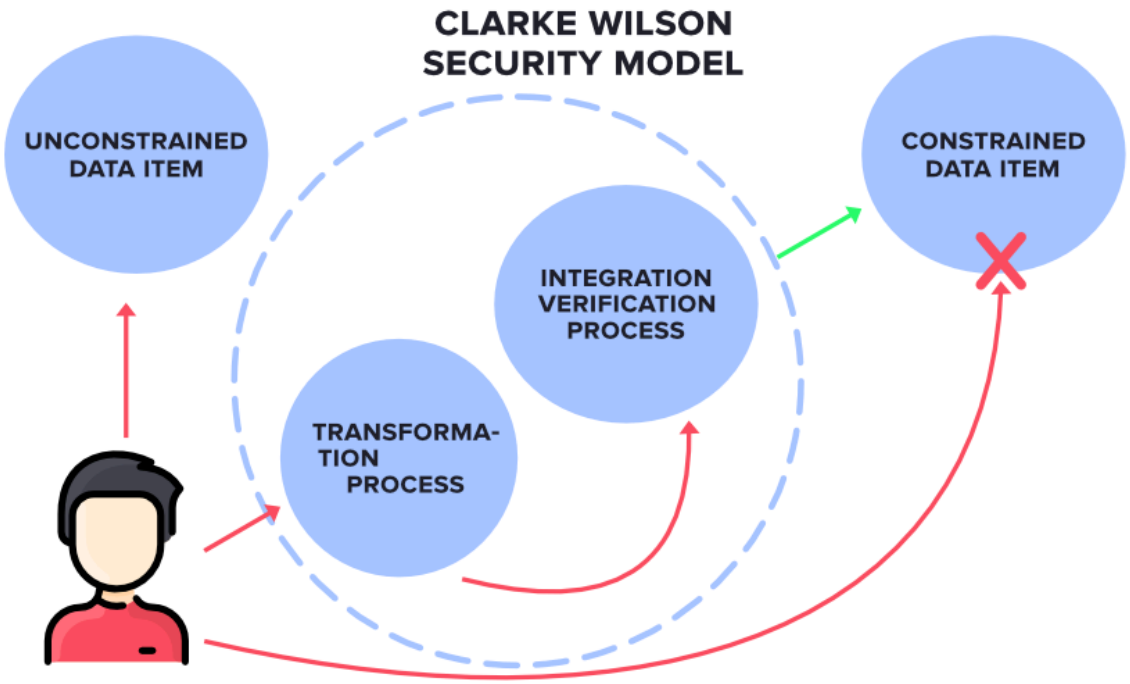
Different Security Models

The field of security has a wide range of intricate aspects that necessitate a variety of security model types to meet different needs. We detail a number of noteworthy categories within the security model spectrum below.

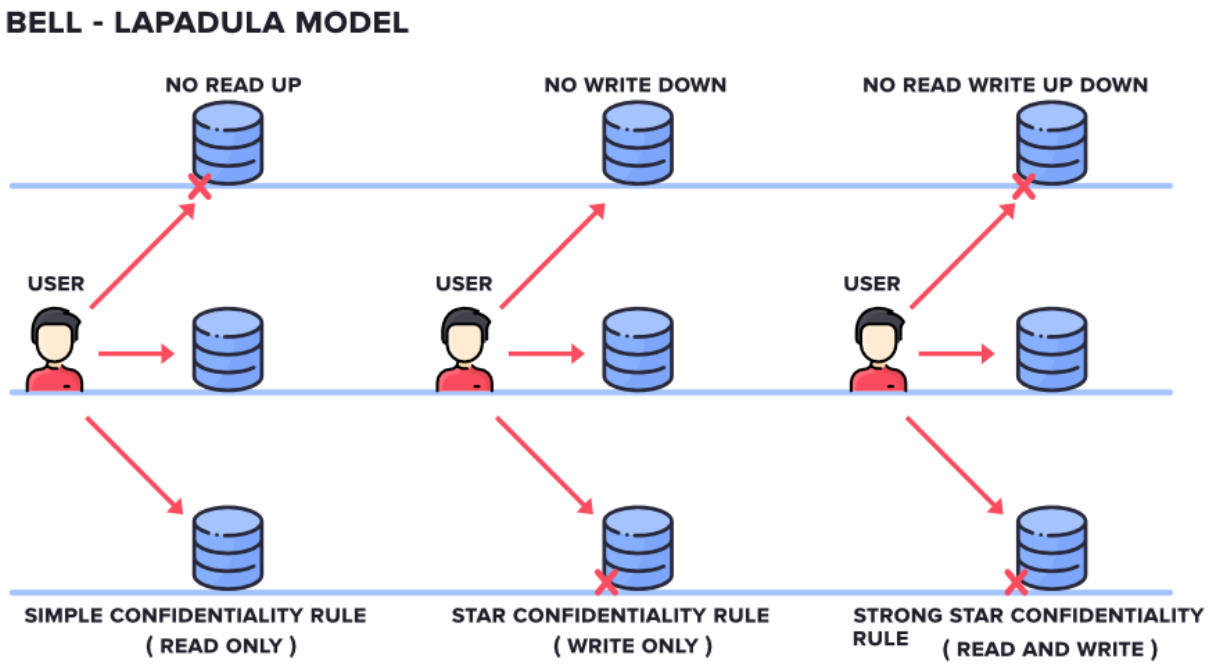
1. Clark-Wilson Model: The Clark-Wilson Model, falling under types of security models, delineates between constrained data items (CDIs) and unconstrained data items (UDIs), alongside two transaction types: Integrity Verification Procedures (IVPs) ensuring the validity of Transaction Procedures (TPs) resulting from CDIs, with only authorized TPs permitted to manipulate CDIs, thus establishing a framework for safeguarding information integrity against hostile data-altering attempts, formalizing integrity policies to maintain data validity across system states, and specifying certification and enforcement procedures as well as the roles and capabilities of system principals.



2. Chinese Wall Model: The Chinese Wall Model, also known as the Brewer and Nash model, within the realm of types of security models, emphasizes conflict of interest avoidance by restricting access to confidential information belonging to separate stakeholders, with access control policies dynamically adjusting based on user behavior to prevent access to conflicting data, promoting data segregation and dynamic access controls in response to user interactions with critical information, although it is not as commonly adopted as other models of security.

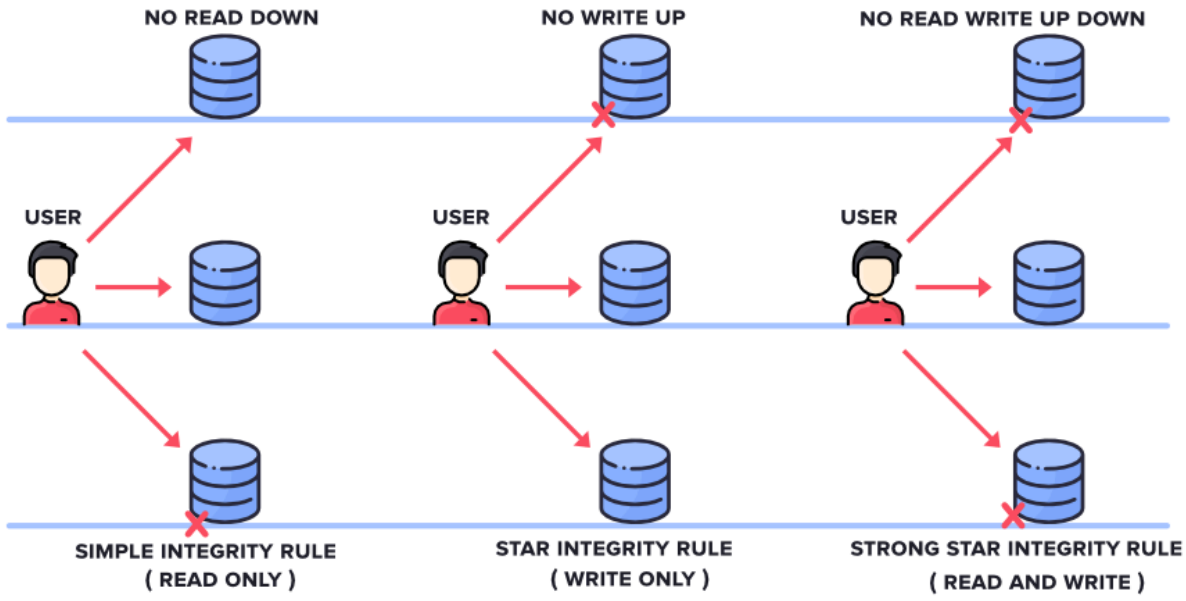
3. Bell-LaPadula Model (BLP): Bell-LaPadula is a traditional Mandatory Access Control (MAC) security model that emphasizes confidentiality. It is defined by three main properties:

the *-property (star-property), which focuses on preventing “write-down” access; the DS-property, which addresses discretionary security; and the SS-property, which addresses simple security or the prohibition of “read-down” access. A system that complies with BLP must meet all of these properties. The only true implementation of the model can be found in Honeywell Multics, though it has not been widely adopted. This highlights the model’s strict control over information flow, where subjects are unable to downgrade information or change security levels once instantiated, creating a framework for secure information handling within classified environments.



4. Biba Model: The Biba Model, a complementary Mandatory Access Control (MAC) framework emphasizing data integrity, delineates integrity levels and access principles analogous to BLP but in reverse, featuring the Simple Integrity Property where subjects are barred from writing to objects at lower levels, the *-Property prohibiting subjects from reading objects at higher levels, and the Discretionary Integrity Property preventing objects from being elevated in integrity level, thereby providing a comprehensive structure for safeguarding data integrity within secure environments.

BIBA MODEL


NO READ DOWN
NO WRITE UP
NO READ WRITE UP DOWN
USER
USER
USER
SIMPLE INTEGRITY RULE
(READ ONLY)
STAR INTEGRITY RULE
(WRITE ONLY)
STRONG STAR INTEGRITY RULE
(READ AND WRITE)