Security Models summary

Latice	+one way information flow + confidentiality and integrity + security labels to all objects +this model is used by (Bell-lapadula, biba, chinese wall)
State machine models	- The policy define the points the secure state can change. - Check if current state is secure state. - check the state of the automated information system (AIS) - Go the one secure state to other secure state. - Based on Finate State machine
Non interference models	- is a research model - the inputs (high-level actions) don't determine what outputs (low-level actions) can see. - Restricted flows between inputs and outputs. - Activities are separated in security levels to reduce leaks. - Higher security level can not interfere in lowerlevel - Lower level cannot get any information from higher level.
Information flow models	- research model - labeled with security classes - it could flow upward or at the same level if allowed. - Bell Lapdula and Biba are infn flow models -based on state machine model
Bell-LaPadula model (BLP)	- Confidentiality model - DOES NOT address integrity or availability - Described in the orange book and TCSEC - Is a state machine & Infn flow model - employs Mandatory access control - The MAC is based on labeling both objects and (with classifications) and subjects (with their clearances) - The system (Reference Monitor) only allows access if the clearance is equal to or higher than the classification. - Uses latice and matrix. - simple security -> read down// no read -up -> subject of lower clearance cannot read an object of higher classification. - *(star) property -> write/append up // no writes down=-> hight level subject cannot send missages to lower-level object. - Discretionary security propery uses access matrix to enforce discretionary access control.
Biba model	- Integrity model -- Is a state machine & Infn flow model - complement to BLP - simple integrity -> subject read access to object only if subject level <= object level (no reads down) - the integrity * property ->subject have write access to object only if subject level => object level (no write -up) - no information from a subject can be passed on to an object in higher security level.

Clarkwilon	-Designed for commercial - Client <-> Interface <-> DB - Integrity by controlling changes - enforces seperation of duties. - Suitable for transaction systems - CORBA is based on Clark-Wilson, it creates relations between objects. - no changes by unauthorized subjects, no unauthorized changes by unauthorized subjects. - subject-program-object binding. - subject authentication and identification - only a set of programs can access objects - users can run only a set of programs - External consistency -> The system is doing what is expected to do. - Internal consistency -> The data being consistent and similar to real world. - CDI -> Constrained data item -> integrity protected. - UCDI -> Unconstrained data item -> data not controlled by Clark-Wilson. - IVP -> Integrity verification procedure -> Procedure scanning, data and confirming its integrity. - Transformation procedures -> Procedures allowed only to change a cconstrained data item.
Graham-Denning	- Secure creation of subjects and objects - collection of 8 primary rules 1. Create object 2. Create subject 3. Delete object 4. Delete subject 5. Read access right 6. Grant access right 7. Delete access right 8. Transfer access right
Brewer-Nash (chinese wall)	- Prevent conflict of interest. - Access control rules change user behavior. - cretes security domain