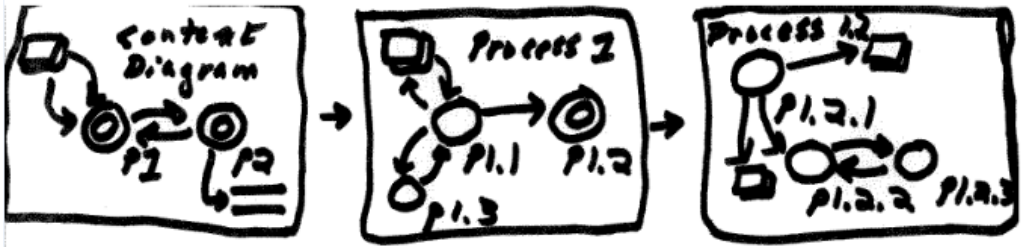
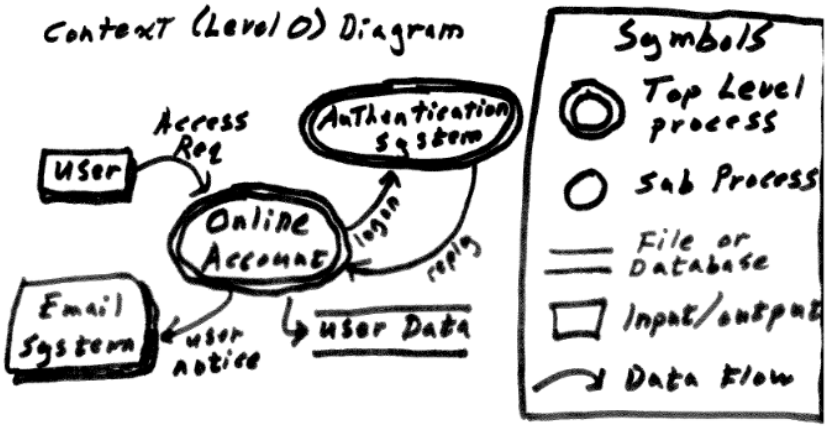
Data Flow Diagrams (DFDs) for Threat Modeling

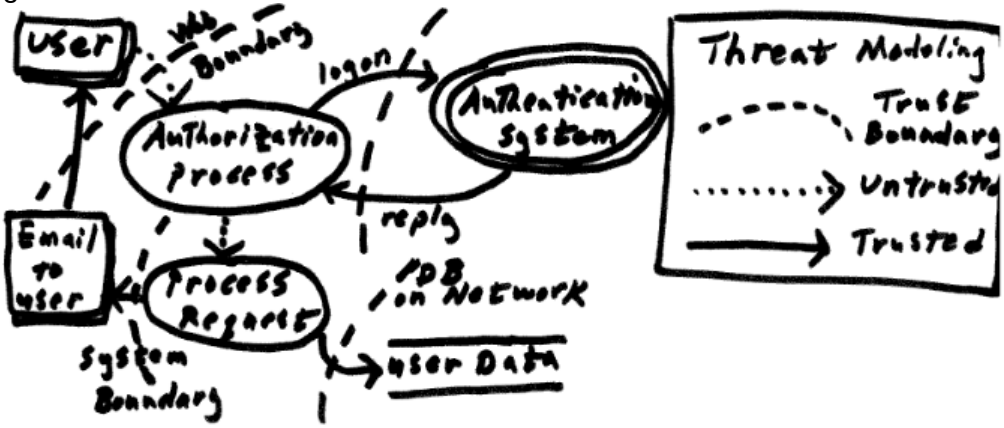
A Data Flow Diagram (DFD) visually depicts the movement of data between the components of a software system. The DFD diagrams show the interaction between the system and any external components. Unlike workflow diagrams, DFDs do not show decision points, data states, or the sequence of data manipulation.



The highest-level diagram (Context Diagram), shows the system being modeled at its most basic level with only other major systems interacting as inputs and outputs. Additional diagrams (Child Diagrams) show lower levels of detail in the system being modeled.



Components include the data sources/destinations (eg a user), processes to act on, and where data is stored (eg databases or files). Usually 2-3 diagram levels are needed to show where outside input is processed. Each process is often given a number for reference.



Threat modeling for security uses DFDs to identify aspects of a software system's design that might be open to attack. Communication between system components (Trust Boundaries) are where attacks are possible. Also, security modeling focuses on the data or transaction requests from a source that may be not be trusted. Untrusted communication between components often identifies user-supplied input or transactions that may not have been inspected for security.

