Secure Software Development Threat Modeling

Objectives

- Explain the concept of a trust relationship
- Define the concept of a trust boundary
- Explain the concept of threat modeling
- Construct a data flow diagram for a system
- Define associated terms related to threat modeling

Trust Relationship

- Every communication between parties must have some degree of trust associated with it
  - Trust relationship
- For simply communications systems, each system has full trust and allows the other complete access to its communication facilities
  - Not very secure

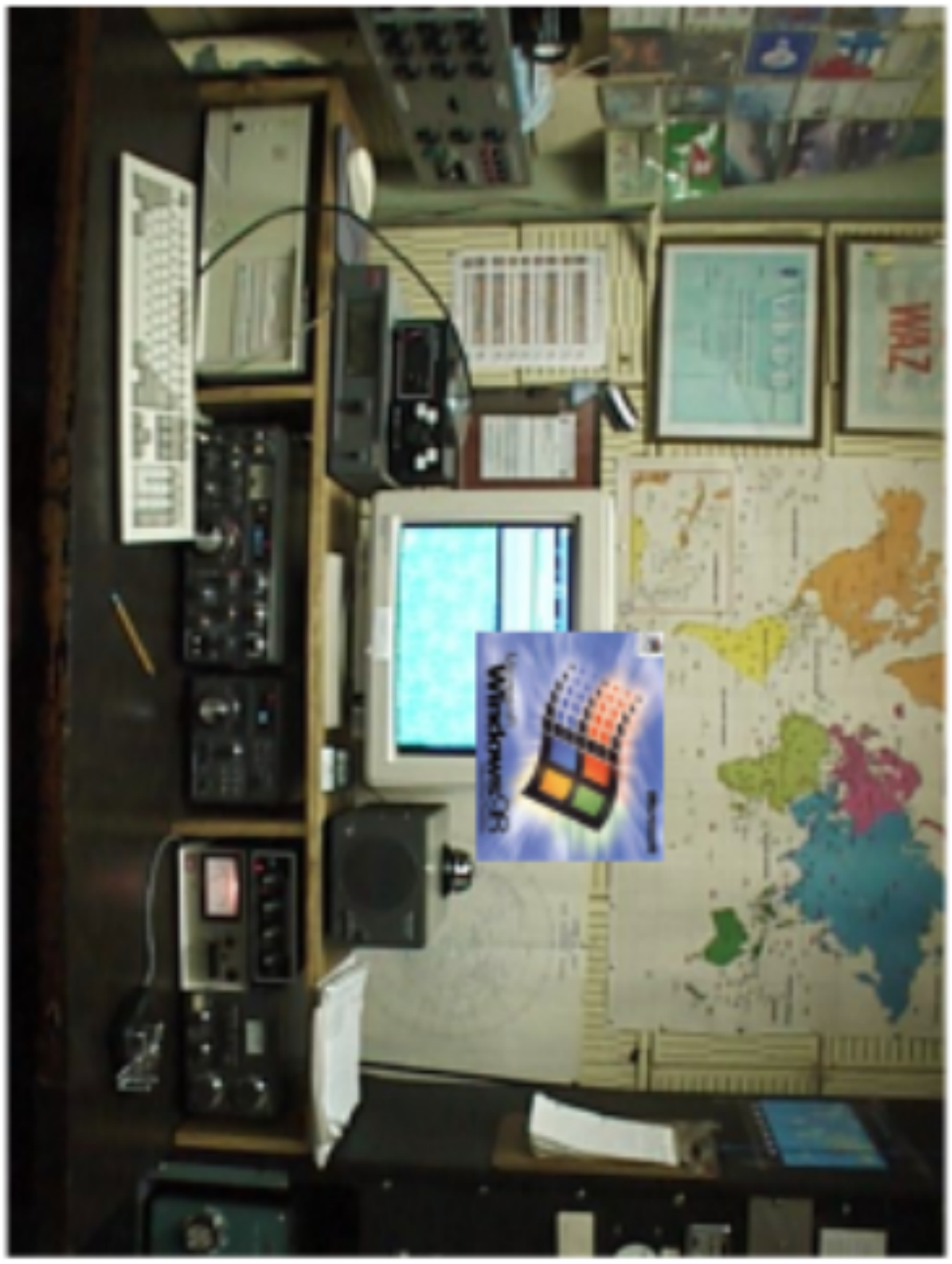
Trust Boundaries

- Distinguishes between regions of shared trust
  - Region of shared trust is a trust domain

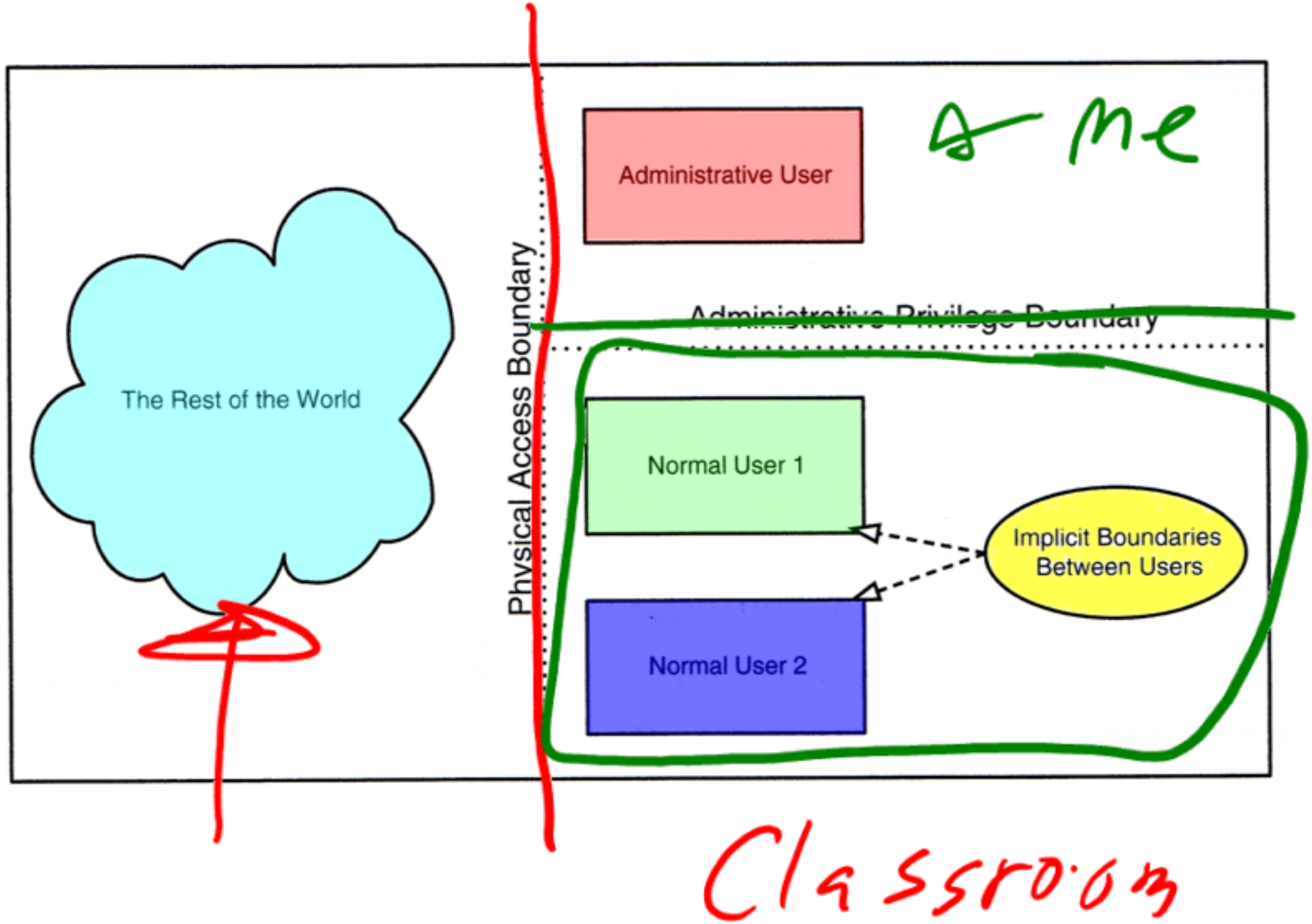
TSA

MSOE

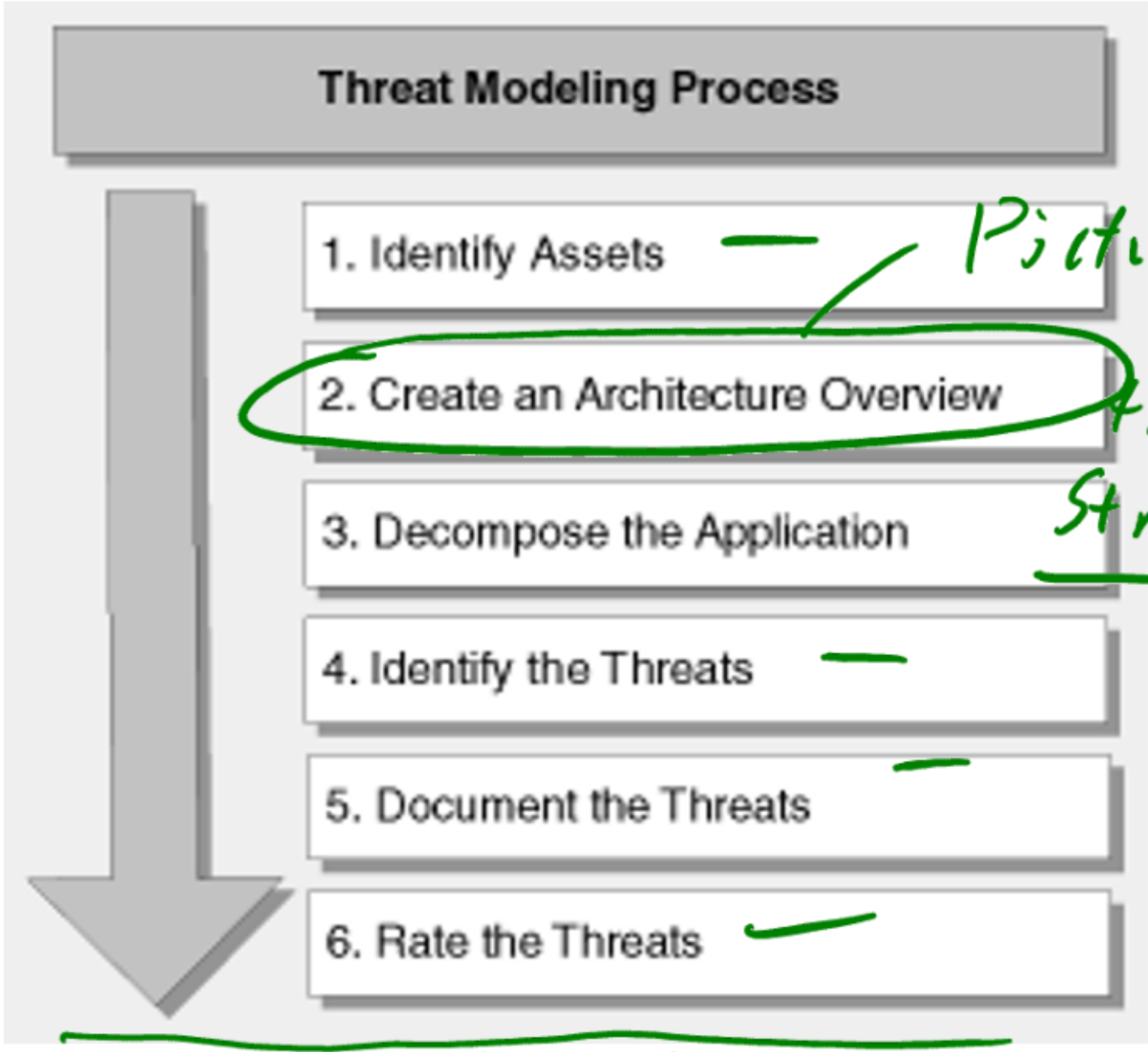
Windows 98 Trust Boundary Example



Simple trust relationships

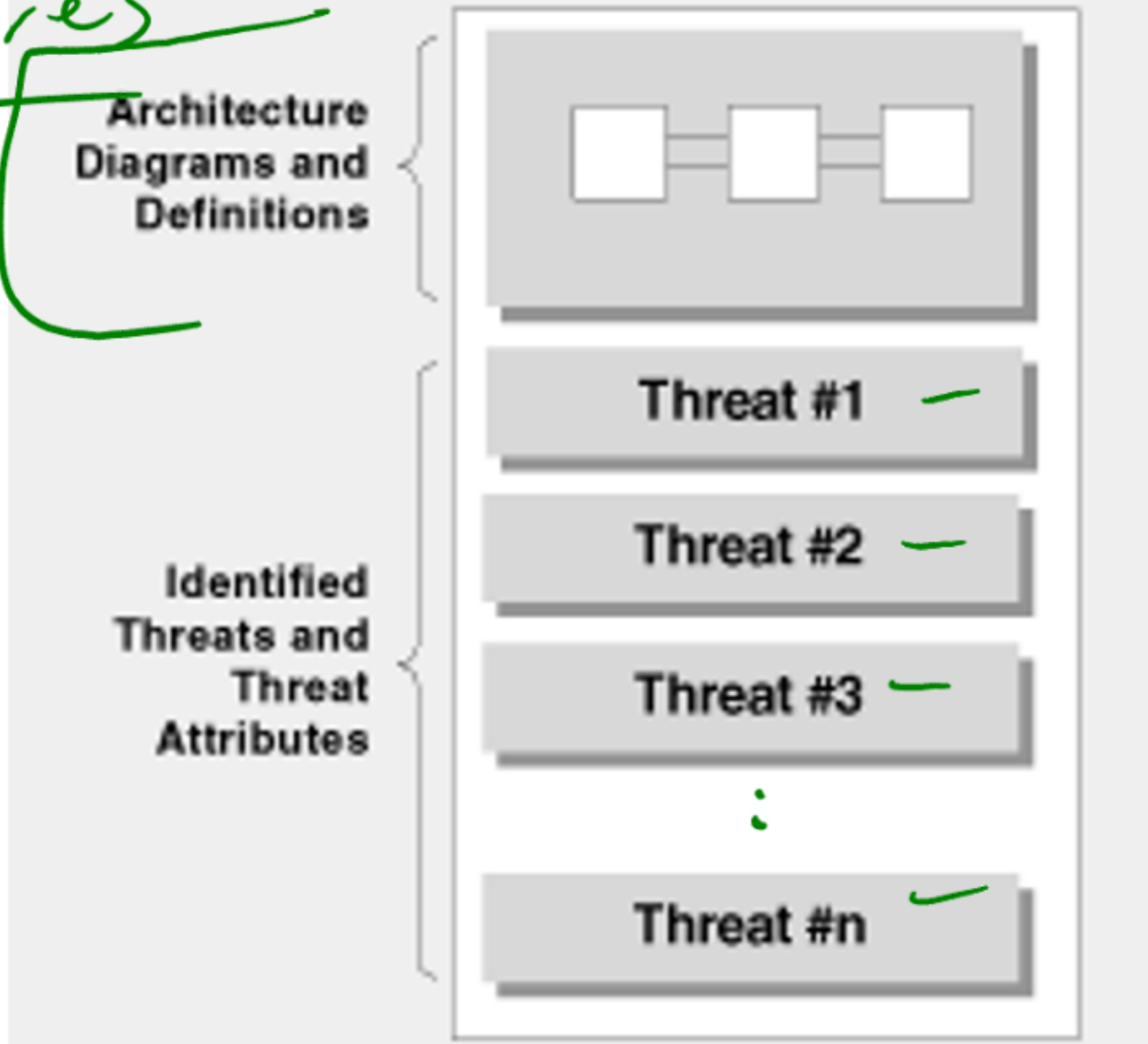


Threat Modeling

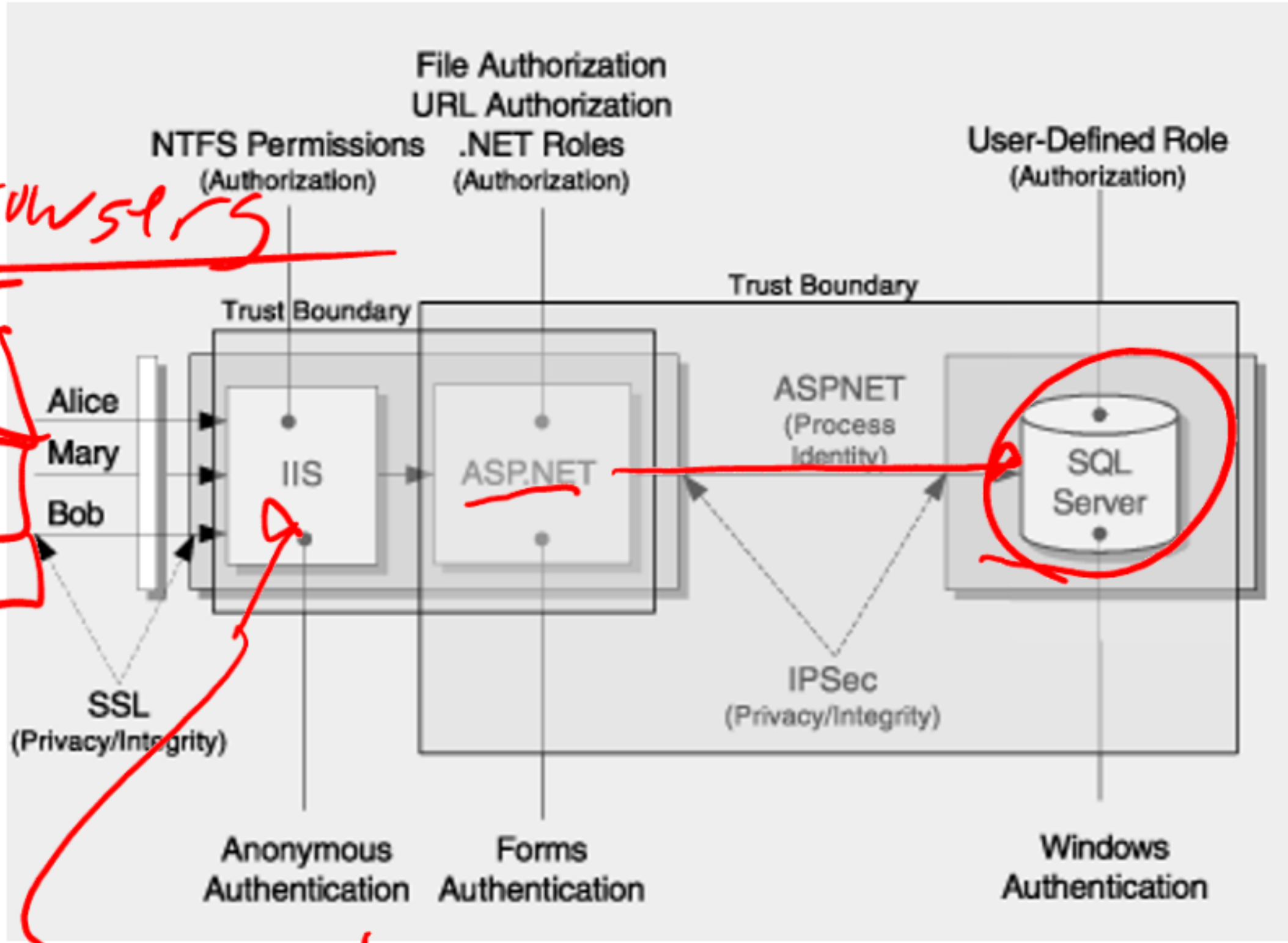


Threat Model Output

Pictures



Create an Architectural Overview



Technology Identification

Technology/Platform	Implementation Details
Microsoft SQL Server on Microsoft Windows Advanced Server 2000	Includes logins, database users, user defined database roles, tables, stored procedures, views, constraints, and triggers.
Microsoft .NET Framework	Used for Forms authentication.
Secure Sockets Layer (SSL)	Used to encrypt HTTP traffic.

Decompose the Application

Application Decomposition

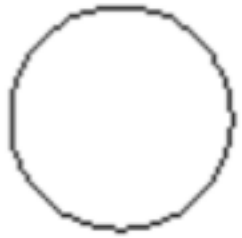
Security Profile		Trust Boundaries
Input Validation	Session Management	Data Flow
Authentication	Cryptography	Entry Points
Authorization	Parameter Manipulation	Privileged Code
Configuration Management	Exception Management	
Sensitive Data	Auditing and Logging	

Decompose the Application

- Identify trust boundaries.
- Identify data flow.
- Identify entry points.
- Identify privileged code.
- Document the security profile.

what we care about.

Data Flow Diagram (DFD): Symbols



Represents a task that the driver performs.

Represents an entity that is external to the driver, such as a user, user process, or operating system component.

Shows the flow of data between components.

Represents a data store: a file, a device register, a data structure, and so on.

Represents a boundary between driver code and external entities.

http://www.microsoft.com/whdc/driver/security/threatmodel.mspx

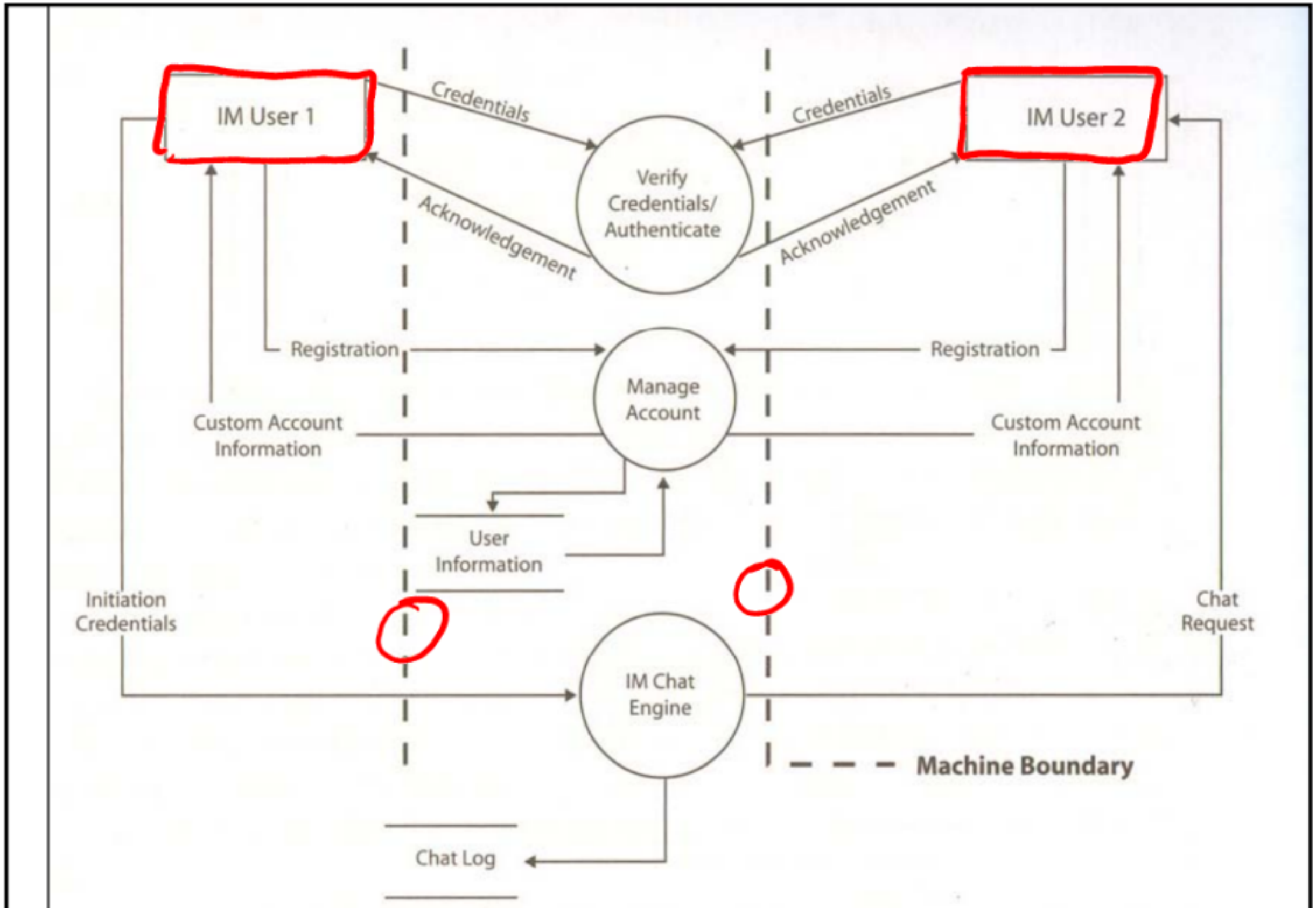


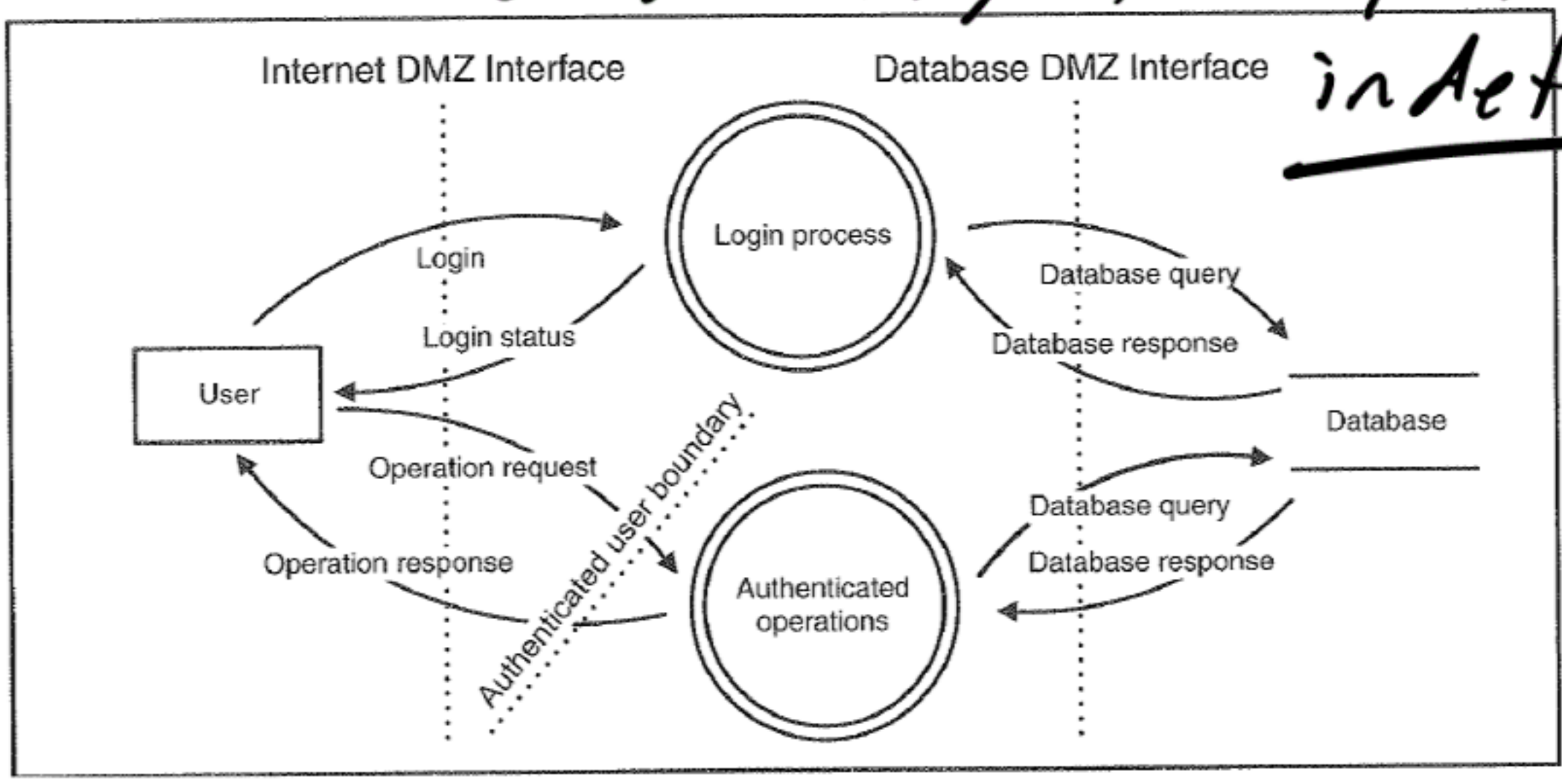
Figure 4-4 IM sample data flow diagram with trust boundaries

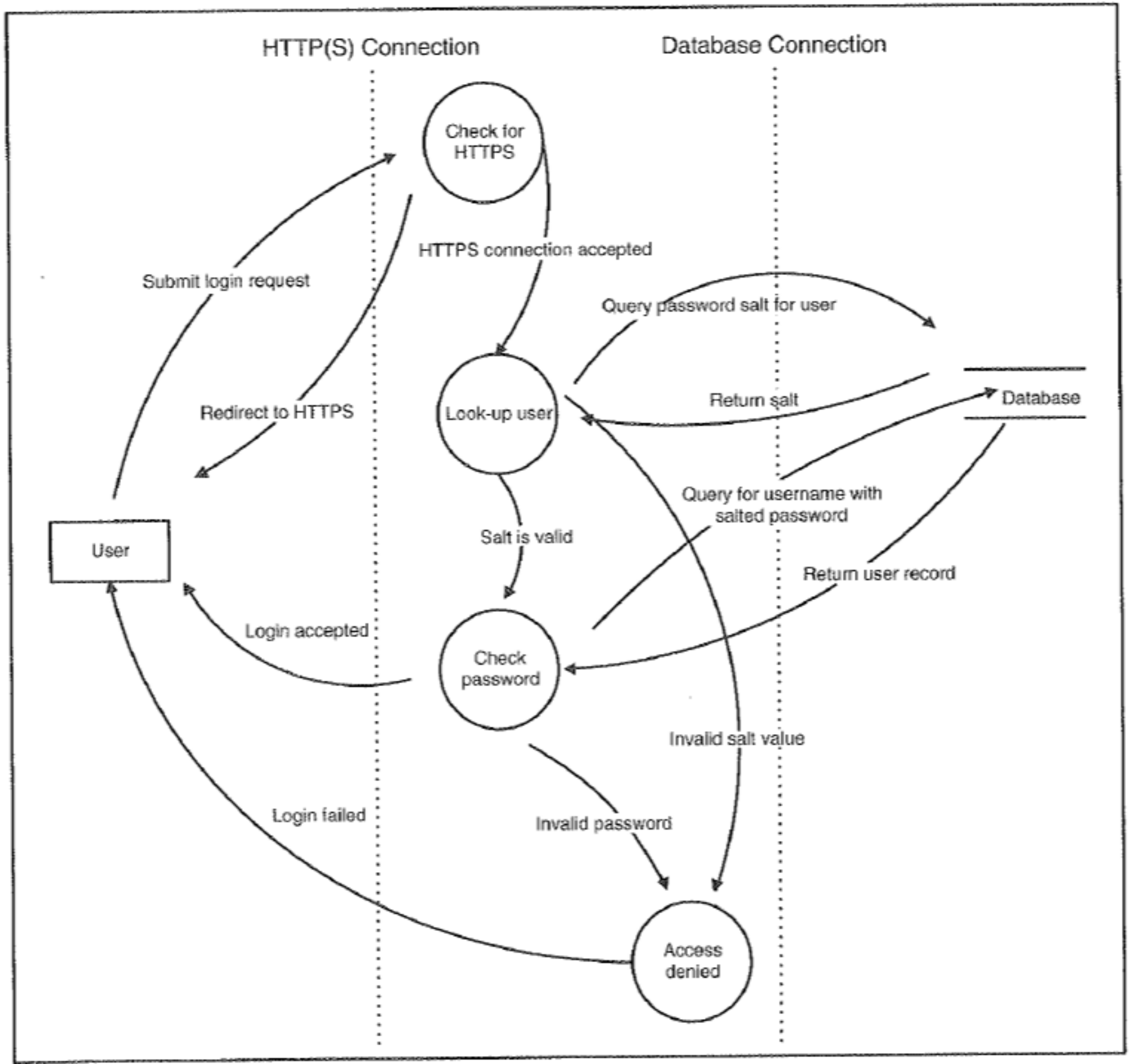
The Microsoft Threat Modeling Tool

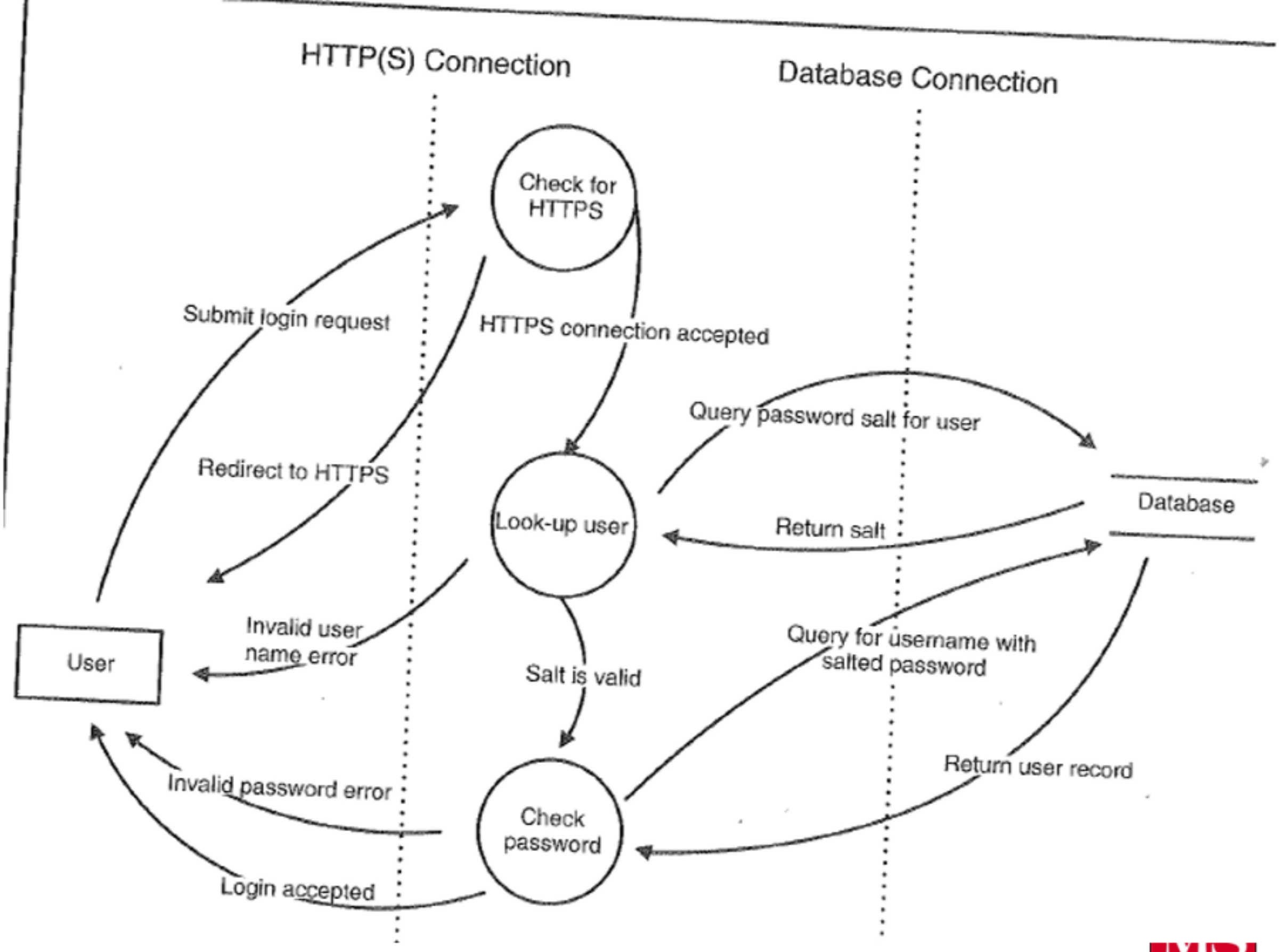
- http://www.youtube.com/watch?v=G2reie1skGg

Target Security Breach

Extra examples we didn't go through these in detail




HTTP(S) Connection
Database Connection
Check for HTTPS
HTTPS connection accepted
Submit login request
Redirect to HTTPS
Query password salt for user
Look-up user
Return salt
Database
Query for username with salted password
Salt is valid
Return user record
User
Login accepted
Check password
Invalid salt value
Login failed
Invalid password
Access denied


HTTP(S) Connection
Database Connection
Check for HTTPS
Submit login request
HTTPS connection accepted
Redirect to HTTPS
Query password salt for user
Database
Look-up user
Return salt
User
Invalid user name error
Salt is valid
Query for username with salted password
Return user record
Invalid password error
Check password
Login accepted

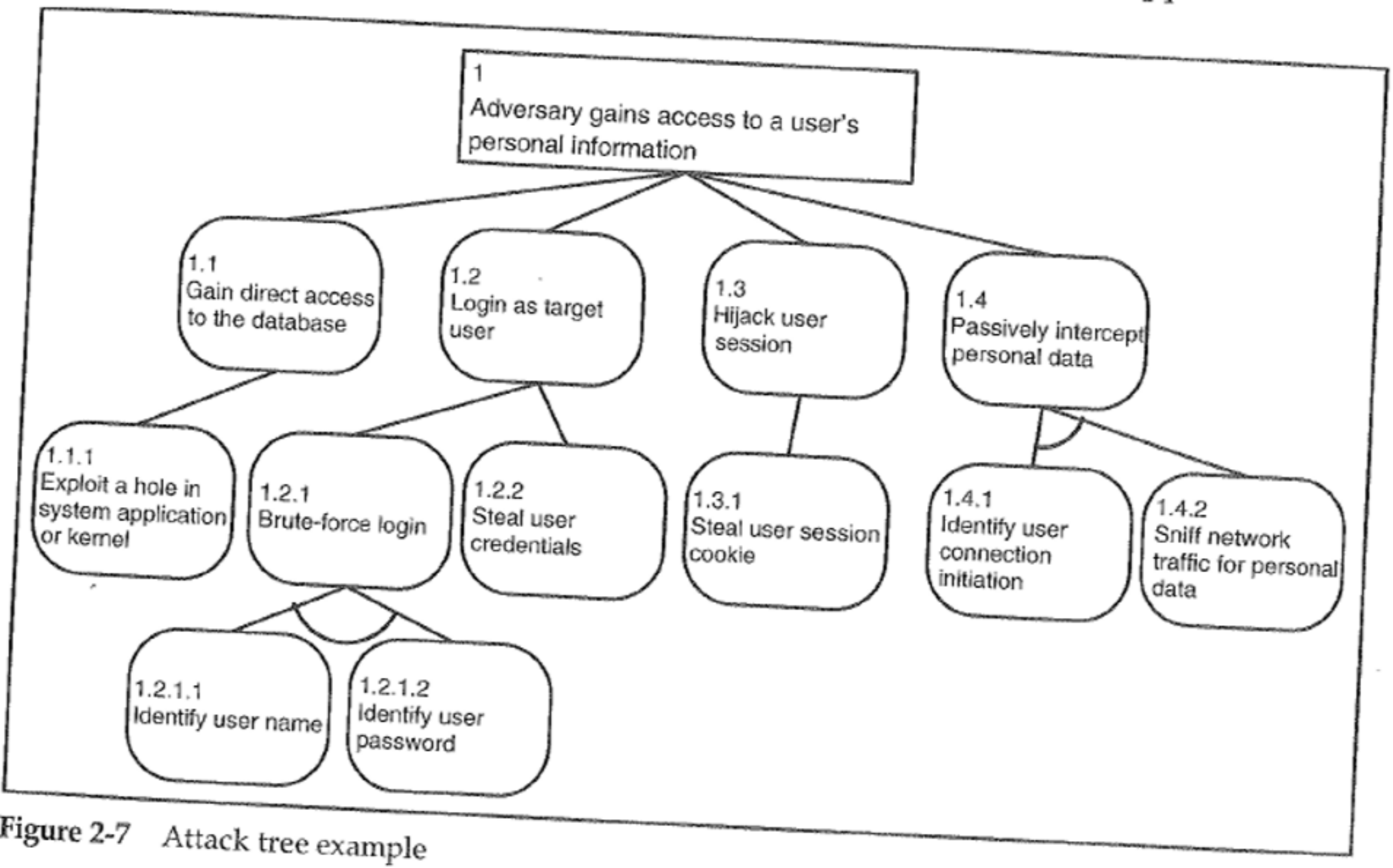


Figure 2-7 Attack tree example

Identify the Threats