Vicente Bobadilla Riquelme
Seth Romanenko

Threat Scenarios:

- “Eavesdropper on user's network reads user's interaction with the TU web server”
    - Solution: Use HTTPS to ensure an encrypted connection to prevent outside snooping of packets.
    - STRIDE: Information Disclosure
- “Mal tries to claim that they are someone else and attempts a password resent”
    - “Password retrieval requires answering security questions.
    - STRIDE: Spoofing
- “DoS attack from too many requests from bad actors”
    - Solution: block IP addresses of attackers after a certain amount of requests/ frequency of requests
    - STRIDE: Denial of Service
- Database is hacked and Mal has access to all data
    - Passwords should be stored as hashes and salted. Any other sensitive data should also be encrypted and obscured. This way MAl isn’t able to read or change the data.
    - STRIDE: Tampering
- Mal attempts to change values in database in order to give himself more money.
    - Only authorized superusers (Admins) can change values and even their power is compartmentalized.
    - Stride:Tampering
- “Mal changes logs in the database in order to remove traces of something (a monetary transaction of his, for example)”
    - Solution: The logs are stored and hashed with a key signature so Mal cannot alter or forge anything without the exclusion of this signature being obvious
    - STRIDE: Repudiation
- “Tapir unlimited publishes private information. This could happen through accidentally making an administrator directory public, revealing sensitive data or information that an attacker can maliciously use”
    - In addition to administrators being cautious about what they do or do not publish, it is important that those with access to particularly sensitive information are not able to “write down” into publicly accessible directories. Clear labeling of data as private, public, confidential, etc.
    - STRIDE: Information Disclosure

- “Mal makes it so IOS app connects to wrong database/server”
    - Solution: Use certificates/signatures to ensure the identity of servers. This way no data is sent to a bad actor.
    - STRIDE:Spoofing/Information Disclosure
- Mal sends phishing email to user, pretending to represent Tapirs Unlimited and gains access to their credentials by asking them to log into an imposter site
    - Tapir Unlimited can occasionally send out emails warning of such attacks and make the user aware of the potential dangers. Other than this, the responsibility to avoid such attacks falls on the user
    - STRIDE: Spoofing
- “Mal is somehow able to change database permissions and gain admin access to all of the files and data stored there”
    - Solution: Permissions are regulated elsewhere so no one takeover of any component gives complete system control.
    - STRIDE: Elevation of Privilege

Data Flow Diagram: