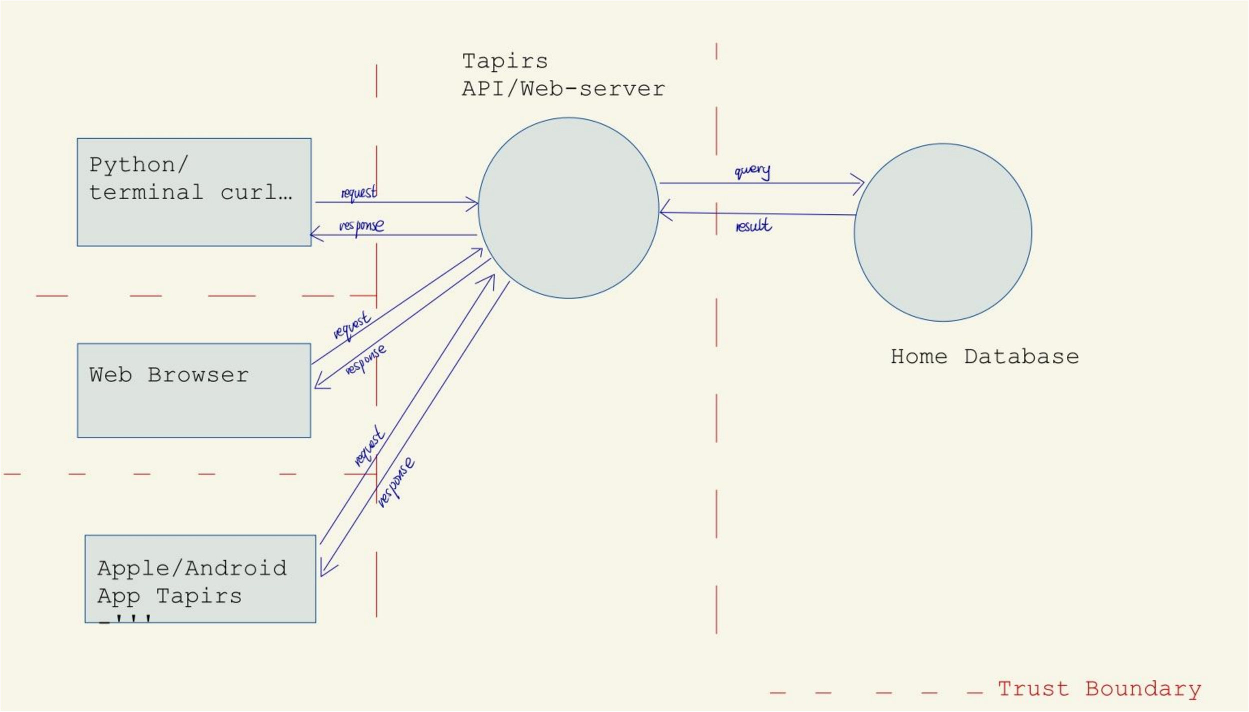
STRIDE

Author: Lily Li
Conferred with: Jeff Ondich

Data Flow Diagrams:



STRIDE type	Threats	Mitigations
Spoofing	Creating a software which mimics TU (And actually connects to the TU API server) with a similar logo, luring people to believe they are using the actual TU app, entering all their credentials/information	Always pay attention to this type of APPs, upon discovery, report to authorities.
	Email phishing: making people believe they are logging into their Tapirs Unlimited to gain access to their passwords/emails	Alert users of phishing in APP. Mandatory for users to login with authorized third parties/devices: emails, phones (enter the temporary PIN to log in)....etc

Tampering	Unauthorized changes to the user database (a person)	Make sure that computer is always in a safe location, and that any change/login to data-base requires multi-factor authentication
	Unauthentic queries to database to request a change in some data (not from the web server itself)	Third party authentication (i.e. CA)/Digital signatures to make sure it is certainly the TU web-server’s authentic query/request to the database.
Repudiation	Uses someone else’s devices to log into TU user account secretly	Double/multi factor authentication
	Unauthorized party logs into web server/ makes changes to source code	Enable email notifications/automatic logs for every change, login in the web-server/database
Information disclosure	Revealing user/database information/structure in error messages/logs	Make sure that all error messages/logs are clear of sensitive information
	Eavesdropper on user's network reads user's interaction with the TapirsUnlimited web server or eavesdropper reads interaction between web server and database	Disable use of HTTP, only HTTPS. Make sure all communications between *Trust Boundaries* use TLS.
	Backup and Unreferenced Files from Leaking Sensitive Information (i.e, a php backup .bak leaking source code/ forget to delete the detached/unreferenced branches on github which contains AWS password)	Make sure backup files are in a safe and secure location, branches with problems are completely erased on github. If there is even a slight/potential security concern, immediately change password and communicate with everyone on the team.
	The genius idea of Tapirs	Founders of *TapirUnlimited*

	was exposed before *TapirUnlimited* blew up and someone else launched a Tapir app before TU.	should swear not to tell anyone this idea until they get a patent/ the app has 1 million users.
Denial of service	DDoS attack which floods web server with internet traffic by bots	Move to large cloud platforms, where many servers are not located in the same place
	Database filled up by user information	Regularly check database to make sure it has enough space, especially for *TapirsUnlimited* as it may blow up in a short amount of time
	App not compatible with the latest/earlier IOS system	Make sure to regularly update IOS/Android Apps so it catches up with the latest system but also is functional using earlier previous system versions
Elevation of privilege	Database manager's wife borrows her husband's laptop, and is able to gain access to all user data	Make sure that there are clear/specific regulations regarding user data and only the authorized can gain access to it even when in possession of the device (always double factor authentication…etc).
	A third party with other information of the user (name, birthday, passwords on other websites) able to guess the user's password/username on *TapirUnlimited*	Prohibit passwords made up of words/names. Mandatory inclusion of Capitalized letters, lower case letters, numbers, and special characters.