1. User persona and stories.

* My primary persona is Thom, a busy, friendly, 21 year-old college student looking to make some money by giving tours around Boston when it’s convenient for him. He is interested in the Townie Tours app so he can use it as a tool to help him find customers (tourists) and offer tours to them. Thom is tech savvy, but never reads any of the terms of service when he signs up for tech products.
* My secondary persona is Pearl, a retired, adventurous, 67 year-old who loves to travel and meet new people. Pearl is interested in the Townie Tours app because it will help her connect with locals, learn more about the places she travels, meet interesting people and have exciting new experiences. Even though she loves to try new things, she’s cautious about her privacy and makes sure to read through all of the terms of service for any product she uses.

1. What security requirements apply to users of this application? For example, do they need to authenticate? How often, at what point in the interaction, and with what credentials? (10 pts.)

* Townie Tours users have to authenticate before they can do anything with the app. They must log in through Facebook, Twitter or Google/Gmail to get beyond the app’s login screen. The app relies on OAuth, the open standard for authentication. Townie Tours delegates authentication to those three external providers, who then pass an API token back to the app to confirm that a user is who they say they are.
* Users can opt in to a process to verify their identity through a process similar to the one AirBnb uses (take a photo of your government-issued ID). Some tour guides may want to do this to help tourists feel safer when they sign on for their tours. Some tourists may want to do this because tour guides can also reject customers if they haven’t verified their identity.
* Tourists using the app will have to use a credit card or PayPal account to pay for any tours they book. They can enter their credit card details once and then save the card to use again in the future. They’ll have to add a password/pin so that anytime they check out, they can verify the purchase.
* Tour guides using the app will have to either use PayPal or link a bank account to the app so they can be paid via direct deposit. Their earnings will be transferred to their bank or PayPal account twice a month, so they won’t have to reenter any of that information to get paid.

1. If they have to obtain authentication credentials, how/when/where will this be done?  (10 pts.)

* Users would obtain their credentials through either Facebook, Twitter or Google/Gmail by signing up for one of those services before signing up for Townie Tours. They’ll need to already have an account with one of those services, or they can’t use the Townie Tours app.
* If users opt to pay or receive payment through PayPal, they’ll need to create PayPal credentials beforehand, and then link their PayPal account to their Townie Tours account within the app.

1. How intrusive are these requirements on the user? What is the effect on their productivity? (20 pts.)

* Authenticating through Google, Facebook and/or Twitter should make logging in incredibly easy for the user. As long as they have an account with one of those services, the requirements are very minimal. If though, a user doesn’t already have an account with one of those services, then the burden of signing up for one before being able to sign up for Townie Tours becomes pretty big and intrusive.
* Some users are weary of connecting multiple accounts online because they don’t want Facebook or Google to get any more data on them than those services already have. Users who are concerned about the number of places their data is stored may be deterred from signing up.
* Setting up financial accounts for payment is somewhat intrusive. People tend to be wary of putting any financial information online. Setting up direct deposit is likely to scare some users away, but many users will feel comfortable attaching a credit card to their account since credit card companies offer such great fraud protection. Users may feel more comfortable simply attaching their Townie Tours account to their PayPal account since PayPal offers many consumer protections as well.
* All of these requirements will slow the user down initially, but they’ve also been chosen because they require minimal amounts of time/effort compared to other options. Additionally, they shift some of the security responsibility away from Townie Tours and place it on other companies who are sharing their resources.

1. What is the user’s hassle budget, i.e., how much of this crap are they willing to put up with? What is their most likely workaround when it is exceeded? Now that you’ve thought about this, re-think points 2, 3, and 4. (20 pts.)

* Many apps force users to sign up for an account before they can do anything else. Users should be willing to put up with clicking on a Twitter, Facebook or Google button to sign-in. Most users will already have an account with one of those services, and it’s likely they’ll be logged into those services already. This makes it hassle-free to create an account.
* Some users may not trust Twitter, Facebook or Google or may not use their services for other reasons. If a user doesn’t want to link one of those accounts to their Townie Tours account, or if they can’t for some reason, then there needs to be another way for them to sign up for the app.
* If they can’t sign up easily, they’ll simply refuse to use the app, there isn’t really a workaround option for them. To appease these users, I’d offer the option for users to create an account directly through Townie Tours.
* Including PayPal as a payment option also reduces hassle for everyone. For people who don’t want to use PayPal and who don’t want to link their credit cards or bank accounts, I’d offer additional payment options. Users could have the option to keep funds in their accounts until they earn a large enough some (say $500), and then have that amount mailed to them via a check. We could also use the APIs from other companies like Google wallet, Venmo, Apple pay, Android pay, LoopPay, Square Cash, Tilt, Tab, LevelUp, Blockchain, etc.

1. In what way might a layered approach to security lower the everyday burden on users? For example, Amazon stores credit card numbers in your account to lower the burden of each interaction, hence increasing sales. But if you want merchandise delivered to a new address, or even an existing address that you haven’t used for a while, Amazon makes you re-enter your credit card number. (20 pts.)

* We’ll use a layered approach to reduce the burden of our customers.
* Users will only have to sign into their accounts once. As long as they’re signing in again from a recognized device, they won’t have to login again when they open the app.
* If users want to make a purchase, once they’ve set up their payment details, they’ll only be asked to enter a short pin/password to confirm a purchase.
* Payments to tour guides’ accounts will be made automatically so there’s no effort required. If guides want to change where their payments go, a greater level of security will be required, and they’ll have to verify their identity through two-factor authentication. That will help keep the user burden down on an everyday level, while also helping keep their account and money secure.

1. What government or other regulations apply to user security and privacy of this application? (10 pts.)

* There are many federal and state regulations around privacy that could apply to users of the app. The app would need to have a detailed privacy policy in order to avoid legal action coming from the FTC (which has gone after many tech companies in recent years). The app may be somewhat susceptible to privacy and security issues since it relies on authentication from other apps (Google, Facebook, Twitter). A few regulations that might apply to the app regarding privacy are:
  + The US Privacy Act
  + The EU Privacy Directive
  + State privacy and data protection laws
  + Section 5 of the Federal Trade Commission (FTC) Act, 15 U.S.C. § 45(a)
  + Gramm-Leach-Bliley (GLB) Act covering financial data
  + Children’s Online Privacy Protection Act (COPPA) covering data collected by children under 13
  + Cable Communication Act of 1984
  + Omnibus Crime and Control Act of 1968
* Security-related regulations might include:
  + Computer Fraud and Abuse Act of 1984
  + Fair and Accurate Credit Transactions Act of 2003
  + Federal Information Security Management Act of 2002 (FISMA)
  + Identity Theft Assumption and Deterrence Act of 1998

1. How much are you requiring the user to think in order to get the security and privacy behavior that is correct for this application?  How can you reduce that load? (10 pts.)

* One of the main reasons the app uses OAuth is that it reduces the work a user has to do. Instead of requiring them to remember a username and password, they simply have to click on an icon to login through a service they already have access to (and one they’re likely already logged in to), which requires very little thought. They’ll literally only have to click on an icon to log in.
* Tourists’ user profiles will only be viewable by the tour guides who they’ve signed up to tour with. Tour guides profiles will be visible to anyone who is browsing through tours they’re interested in. These privacy settings are configured by default, giving the user no control, but also keeping the number of things they have to think about to a minimum.
* The app is designed to be secure but to also require little thought from users. Some users who are more diligent, might end up spending time reading over and thinking about terms of service and privacy notices. Due to the large number of other apps that would be integrated with this one, some users could end up spending a lot of time reading different companies’ policies.
* One way to reduce the amount of thinking users have to do would be to create few, short policies and terms for users to read/agree to. Doing so though, may leave the company vulnerable to litigation if the policies weren’t thorough enough.