Project Tools & Information

Location

* GPS: Global Positioning System.
  + Run by the US Military.
  + On mobile, location data is sent to the provider of a cell phone company. This is to ensure the location data can be sent and received quickly by the phone provider.
* GPS: Workings.
  + Listens to certain frequency of radio signals.
  + Satellites send time coded messages at the selected frequency.
  + Content of a message on the frequency consists of:
    - Time.
    - Current satellite positions.
    - Other.
  + The stream speed of GPS is slow. Usually takes up to 30-60 seconds. This makes it easier for receivers to pick up the frequency.
* AGPS: Assistance Global Positioning System.
  + Cell Phone company feeds information to a GPS receiver, based on what the cell phone towers can ‘hear’.
  + Switch from cellular receiver to GPS receiver for O.1 seconds to collect data.
  + Phone company processes data, then sends location data back to your phone.
* Open GTS
  + An open source project designed for web-based GPS tracking.
  + Supports a variety of GPS tracking devices (Sanav, Aspicore, TAIP, NetGPS).
  + Uses technologies such as:
    - Java.
    - MySQL.
    - Apache Tomcat.
    - //May run on modern OS’s.
* Geolocation
  + API used in Google Maps to generate map images and visualise GPS data for a user.
* Windows Location API
  + Microsoft owned API that can be used to develop location aware applications.
* Tracking
  + Cookies?
  + Google Analytics: could be used on mobile platforms.
  + These could be used for recommending services to users?

Accounts

* Encryption:
  + Scheme.
  + Plain text encrypted using an encryption algorithm.
  + Uses a cipher to generate cyphertext that can only be read if decrypted.
  + Usually uses a pseudo-random encryption key generated by an algorithm.
* Two Types:
  + Asymmetric:
    - Public key cryptography.
    - Uses one public (shared) key and one private (secret) key.
  + Symmetric:
    - Uses the one key to encrypt and decrypt data.
* Cryptographic hash function:
  + Used with digital data signatures.
  + Used with digital data integrity checks.
  + From an electronic file, cryptographic hash functions generate a short digital finger-print of content called a message digest or hash value.
* DiskCryptor
  + Possible tool for encryption.
  + Can use AES, Two Fish or Serpent (tools).
  + Can work with windows (supposedly).
* Azure Storage Service Encryption:
  + Built in Azure encryption service
* Account Creation:
  + ASP.NET MVC frame work:
    - Built in account functionality.
    - Compatible with Mobile and Azure.
  + Account functionality could also be custom built in MVC.
* Testing:
  + Android Emulator:
    - Can be used to test the compatibility with android devices.
    - Built into Android Studio. Will need to get access to that too.
    - Emulator allows you to share code on phones, tablets, electronic watches, etc.
  + Apple SDK:
    - IOS version of Android Development Kit.
  + Forms can be custom built using C#.
* Database:
  + Likely relational. This will recognize relationships as stored items. NoSQL database basically the opposite.
  + Oracle/MySQL.
  + Needs to be accessible on the cloud.
  + May need to be accessible via the application itself?
  + Will likely use Microsoft Azure, or AWS. Application will be stored on one of these cloud services.
* Azure:
  + Can use containers.
  + Can use virtual machines.
  + Can use scalable servers.
  + Data centres will store data gathered.
  + Integration with Visual Studio IDE.
  + Possible student offer?
  + Cloud would use public model. PAAS (Platform As A Service).