Jonathan Dyer
CS 1699: Privacy in the Electronic Society
Homework 1

1. Google Maps navigation

EVENT:

I used Google Maps to navigate to a friend's house this week. It was turn-by-turn on my smartphone, so I had constant updates about traffic patterns as I went. It was during rush hour, so I decided it would be better to avoid the highway and indicated such in the application options menu.

DISCLOSURES:

Quite a bit of physical information was given up in the course of this interaction, as well as perhaps some behavioral information. Specifically, I gave up information about my physical location (or at least the location of my phone) *and* the location of my car. In specifying that I wanted to avoid highways I also gave up information about my preferences--it is easily inferred from this behavior (especially when repeated over time) that I would rather be moving--even through twisting residential streets--than waiting in standstill traffic on the highway. All of this information is not just associated with my physical device but with my actual identity (name, birthday, education, gender, etc.). This information was passed directly (we suppose) to Google's servers, which utilized this info along with real-time information from other phones/vehicles in order to direct me most effectively. If my location information is being shared by Google with anyone else (say, in order to provide some service such as local Yelp reviews or shopping information), then they also have it, along with any third-party providers of information storage.

THREAT MODEL:

In order for this activity of navigating through Google Maps to be "worth it" for the average user, several assumptions must be made. Firstly, in order for this information sharing to be **safe**, we must assume that Google and any associated parties that are given access to location info are not malicious in intent. We must also suppose that they are competent and secure enough not to allow unauthorized access to the info. If we don't want to feel **spied upon**, we also assume that Google and any third-party associates are not using such location information to actively take advantage of users or bring about any negative effects for them.

EVALUATE THREAT MODEL:

It would be a little too optimistic to suppose that Google and others are not leveraging this information for *some* kind of financial gain. However, Google in particular is a large enough company, serving enough people, that I (and certainly the average user) believe that they are competent enough to keep my information safe from **other unauthorized parties**. However, the average user is likely not totally aware of who precisely has their info, and perhaps would be more wary about using the service if they knew that the security assumptions above are implied.

IMPROVEMENT IDEAS:

One idea I have for decreasing the necessary trust in the system is de-linking the location data with your account, and instead associating it with the physical device being used to navigate. This would have the advantage of not risking personally identifiable information on a potentially risky site or company. This would allow us to relax the assumptions surrounding the security of each party involved in acquiring, storing, and processing the location information. I think that following this idea while still consistently providing personalized services is simply not as valuable for Google. They would be giving up precious marketing information, and it would be harder for them to develop a comprehensive picture of your preferences and habits, which is simply not as lucrative in areas such as advertising.

2. Street Parking in Pittsburgh

EVENT:

I parked in a paid parking zone in Oakland recently, which required using the electronic meters provided by the Pittsburgh Parking Authority. I used a credit card to pay for the parking time, which totaled to about two hours.

DISCLOSURES:

A surprising amount of information is given up in this seemingly menial interaction with a parking meter. Firstly I had to enter my license plate number, which is associated with my identity, and even the fact of my usage of the system indicated that I was not at home, but rather at a parking meter in Oakland. Additionally my payment amount (according to the parking time desired) revealed how long I planned to be at that location, or at least how long I planned to leave my car there. Finally, my credit card number was stored/processed so that payment could be made, revealing that I was making a purchase and what it was for.

The explicit information about my license plate and the implicit information about my location and short-term travel plans were given to the PPA, likely along with my card information. That (credit card) info was also transmitted to some kind of payment processing service, where it was verified and then recorded by my credit provider.

THREAT MODEL:

In order for this interaction to be “worth” the disclosures mentioned above for the average user, they must assume that the parties involved (Pittsburgh Parking Authority, credit processing, even the local electronic system) are not malicious in intent nor compromised in their data security. The information about where someone’s car is parked could have implications for their (physical) safety, and thus should be presumed confidential in order to feel **safe**. Obviously the matter of **convenience** is an important factor when considering this trade-off between disclosure and privacy--allowing card payments enables quick and easy parking experiences. Thus the user must assume that this is the best cost-effective way of performing the function of these meters.

EVALUATE THREAT MODEL:

No way do I believe the PPA is benevolent--they hand out parking tickets like candy. All jokes aside, I have no reason to suppose that they are secretly harvesting credit card numbers (or for that matter that they even keep such numbers on file), or leaking info about user locations. I think the average user would probably believe the above assumptions, since the action of paying for a service with a credit card is fairly standard, as is the action of charging for street parking in a city. I also think they are probably aware of such assumptions and their necessity in order to feel safe in a modern parking society.

IMPROVEMENT IDEAS:

One way to reduce the information disclosure is to change the parking scheme somewhat. Rather than having general “zones” for parking, the spaces along the street could just be numbered/divided at regular intervals, and then users could be identified by the physical spot their vehicle occupies rather than by their license plate number. This would eliminate the need to store/transmit/reveal the license plate to anyone (electronically, at least). However, I think this would be prohibitively expensive for the parking service to implement, as it would require a lot of physical work and a revision of how people park in Pittsburgh, which may also affect usability as people adjust to the new system.

3. Lastpass Password Manager

EVENT:

I used the popular password manager LastPass at least a dozen times in the last week to log on to various websites/services.

DISCLOSURES:

I disclosed the fact that I was accessing my usernames/passwords (to LastPass), and for each site I added to my account or logged onto using LastPass I also revealed the username/password itself--since the browser extension had to be able to copy it to the appropriate location. Additionally, for each of those services I logged onto, I revealed that I was accessing them (to LastPass).

THREAT MODEL:

There are a number of assumptions inherent in use of LastPass. In order for it to be "worth it" (which here means **secure** or **relatively risk-free**) for me to reveal all of my passwords to such a service, I have to suppose that the service has state-of-the-art cryptographic security protecting my data (both at rest and in transit), with properly implemented security protocols and policies, and with an active development/testing/improvement of these security measures. In short, they must be competent at their job. Additionally, a basic assumption to feel **safe** using the service is simply that LastPass is a trustworthy business, and that even when using their free service I will not be subject to any kind of exploitation or similar harms.

One other indirect actor for my interaction with LastPass is the Chrome Web Store, where I acquire the LastPass browser extension that performs the bulk of the service for me. The web store provider (Google) is in a powerful position, since it could issue a false update/extension that enables information leakage. So I assume that the vendors/websites where I get the LastPass functionality are legitimate and benevolent.

EVALUATE THREAT MODEL:

The average user must carefully consider the assumptions implicit in using a service such as LastPass. I personally must believe the above assumptions are true, else I wouldn't rely on the service for some of my very important information. The average user of LastPass must adhere to the same assumptions, on the premise that LastPass is more secure/effective/convenient than other password management systems. Since security and safety are the goal of using LastPass, it seems that all users of the system must believe in these assumptions to some extent.

IMPROVEMENT IDEAS:

One exemplary way to relax the assumption that LastPass knows what they're doing (and simultaneously beef up security) would be to require a second form of authentication in order to access passwords. This would put less trust in the system LastPass already has and more trust in established crypto/security protocols. Multifactor authentication takes much more time and effort, however, and it may simply affect usability too much for the users. This would cost LastPass in terms of users and hence business, which is why I think they don't use it already.