TEAM: Valerie Angulo, Chris Davidson, Adrienne Bouchie, Jingni Liu

---

FINAL TOPIC: Protecting User Data

Rational:
In the past decade, the most common type of data stolen has been User Data. While certain breaches, like the Playstation Network Breach of 2011, just hinder the system's services and limit the availability to users, other breaches are more "successful" by gaining sensitive User Data.

With most apps and websites requesting to access user data these days, this is becoming an even larger problem. How will companies protect this ever present user data?

Many companies are looking at the FTC recent breaches and user complaints to learn from these companies' mistakes in hopes of minimizing the risk for their own company having a data breach. This approach is reactive, not proactive. In order to protect user data from future threats, we have designed the following approach.

Scope: Business and Individuals

Expected Solution:
Have a cloud data management system where users and businesses can store all their data. This management system will utilize multiple cloud services such as Amazon and Google and split personal data up into these different services based on an algorithm, so that users aren't given the chance to store all their data in one cloud. We are using this algorithm so that if one cloud gets compromised, the user doesn't have all of their data saved on that one system. No one cloud will be designated as having more important data than another, so it would be useless to target one system over another. Our data store system

doesn’t store any data, it is the authentication and communication between businesses requesting to store their data and cloud services. Our system provides an algorithm to split data and credentials to access a users info through these various systems. Another optional feature is to have a “kill switch” that will delete all your data throughout the clouds, which you can use if a system is compromised or if you no longer wish to have your data throughout the clouds.

Example of use: Amazon’s cloud service is attacks and a users SSN is compromised, but no name or other information is attached to it so it is useless.

SOURCES:

https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations