**Privacy and Security**

EC601 A1 Project 3

Renyu Jiang U18427594 [renyu26@bu.edu](mailto:renyu26@bu.edu)

Once upon a time, people used paper or other physical objects to convey information. At that time, data amount is quite small, even with dozens of tons of paper, the amount of information carried is not even as much as a hard drive today. With the generation of massive data, there are more and more privacy and security risks. This paper is mainly focus on these two aspects.

First, we start with privacy. Privacy is one of the most important concepts of our time, yet it is also one of the most elusive [1], It is almost impossible to figure out the legal definition of privacy, so in this paper, we simply defines privacy as information that is not intended to be known to others. There is already a while since people start talking about protecting privacy, but situation has changed a lot, especially in this decade. There are two main ways that people leak their privacy, one is from people themselves, and the other is from companies that provide various services.

People always sign up for various social accounts, and they post information about their lives on these social platforms, such as travel vlogs, showing off new cars, etc. These behaviors seem not to be harmful and have nothing to do with privacy, however, this is a completely wrong view. Posting home’s pictures is such a good example: If people choose to send original picture to website, then they tell everyone who sees the photo their precise latitude and longitude. Even if they erased the EXIF (Exchangeable image file format), the content of the picture itself may also reveal privacy, for example, the shooting area of the photo can be inferred from the scenery features outside the window, and the family's economic conditions can be evaluated from the decoration of the home, etc. There is a TV series called *You*, which tells a story about privacy and the consequence if privacy leaked. Although it is very ideal, it is still worth watching.

Privacy leaks from individual action are serious, however, the privacy breaches caused by those large corporations are much larger than those caused by individuals. If you search the company name with the keyword data breach, you will find that almost all large companies have had data breaches. More than 80% of these data breaches are caused by hacker attacks or program flaw, and a small part is caused by insiders selling data. Some of these data breaches can cause life inconvenience, while others can cause serious personal or national security concerns. In 2016, Adult Friend Finder Networks data breach caused 412.2 million records leaked, including names, email addresses, and passwords, the stolen data came from six databases with 20 years of information. Most of the passwords were protected by the weak SHA-1 hashing algorithm, which resulted in 99% of the credentials being posted by LeakSource.com in 2016[2]. This data breach has caused embarrassment and family conflicts for many people. In addition, data breaches are the most direct form of privacy breaches, but not the most common: These data-holding companies can legally sell your data as a product or service. A lot of user data trade are for better advertising, for example, when you search for a certain item in a search engine, such as smartphone, then you can easily see ads for related items like iPhone, Pixel Phone elsewhere. This kind of transaction used to be a legal blind spot and did not require users to be notified, but now more and more regions have laws to protect user privacy, such as California’s CCPA, which requires companies to notify users before selling user data and clearly show Do not sell my data option. In addition to obtaining user consent, many regions require that data sold must be desensitized or anonymized, which is also a useful method to protect privacy.

Then, we move to next topic: Security. Once, confidential documents were stored in secure locations where most unwelcome visitors could not even get to the front door of the storage facility. But now the internet makes it possible for everyone to go to those storage interfaces and have a try. Therefore, devices connected to internet takes all measures to protect themselves. Among these security measures, permissions and encryption are two of the most basic methods.

Modern computer systems, such as Linux, Windows, etc., have used permissions to protect data since their inception. In our computer, running programs sometimes requires different permissions, high-level permission users can execute more commands, while users with lower-level permission have more restrictions. A secure operating system usually gives users the minimum required permissions, for example, write a paper on windows computer doesn’t need Administrator permission and account using Facebook on Android devices doesn’t have to be a root user. If you come up to a recipe app which requires your location permission, then you have to be careful. When a program gains access to data it does not need, there is a risk of data leakage. Considering that the way a computer authenticates permission is usually username and password matching, setting a strong password is an effective security measure.

Although permissions can provide users with privacy protection, permissions still have their disadvantages: Almost all permissions are assigned by people, so there is a risk of privacy leakage caused by people. For instance, the administrator of a website has the highest authority, then once his account information is leaked, all the data of the entire website will be stolen. Therefore, we need additional security measures: Encryption. If permission looks like an administrator, then encryption is like a lock. The current mainstream encryption methods can be divided into two types: Symmetric encryption and asymmetric encryption. These two encryption methods are not replacements, they have their own advantages and are used in different occasions.

Symmetric encryption uses the same key for encryption and decryption, so encryption is fast and can encrypt large amounts of data. Symmetric encryption algorithms like AES take billions of years to crack using brute force attacks, therefore, the US government uses the AES algorithm to protect its confidential documents, which require 128-bit keys for secret documents and 256-bit key for top secret. However, the key transport of symmetric encryption is its biggest weakness, if key leaked, data leaked. Then, we talk about asymmetric encryption. A key pair for asymmetric encryption consists of a public key and a private key (many key pairs can be used). The private key decrypts the public key encrypted data, and the public key decrypts the private key encrypted data. This method is slow in encryption but has little risk of key leakage, so it is only suitable for encrypting small amounts of data. Due to the properties of symmetric encryption and asymmetric encryption, people use them in combination, using the asymmetric encryption algorithm to encrypt the key to the symmetric encryption algorithm, and then use the symmetric encryption algorithm to encrypt the data itself. Https protocol is one of their classic combination applications, it uses the RSA algorithm to establish a secure channel and transmits the key of the AES algorithm, thereby realizing encrypted data transmission. Hardware dynamic banking PIN device is another example.

In addition to technical issues, users and device manufacturers have other factors that affect privacy protection and security, such as law and ethics. In many countries, local laws will require technology companies to accept government supervision and hand over certain user data, and privacy protection and laws are in conflict. The most well-known instance of the latter category was a February 2016 court case in the United States District Court for the Central District of California. The Federal Bureau of Investigation (FBI) wanted Apple to create and electronically sign new software that would enable the FBI to unlock a work-issued iPhone 5C it recovered from one of the shooters who, in a December 2015 terrorist attack in San Bernardino, California, killed 14 people and injured 223. Unlocking a shooter's phone for police to investigate a shooting is the right thing to do legally and morally, but once it's unlocked for the first time, there are concerns over whether the method could be abused. Apple didn't unlock the shooter's iPhone in the end, but that doesn't mean other companies won't either. To avoid this conflict between security and law or ethics, many companies now take a "we're willing to help, but there's nothing we can do" attitude: they claim that the user's device is completely under the user's control, and that cryptography-based techniques prevent everyone including the device manufacturer access device. But this is only a temporary compromise, and the security and privacy conflict between lawmakers, tech companies and users will continue.

To sum up, with the advancement of computer technology and the development of the network, users face more privacy risks and security issues. Although the technology used to avoid privacy leaks and security breaches is also advancing, some factors other than technology can also affect privacy and security, and laws and ethics are not consistent with users' desire to get absolute privacy protection and security.

**References:**

1. Solove, Daniel J. "Understanding privacy." (2008).
2. <https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time>
3. <https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute>