Privacy in the Cyber Universe

Edshel Torres Rosa
Master of Engineering in Computer Engineering
Professor: Nelliud Torres, DBA
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— We live in a world where the internet is almost an essential part of our day to day. We are at a point where we cannot divorce humans from technology, or technology from humans, it is part of us. What is most valuable in that interaction from us in the cyberspace, is our personal information data. Data is like gold on this universe and we need to know how to manage and behave in this world. There are threats, vulnerabilities, bad people, and they will do everything possible as long as there is a motivation to steal your data. How much the internet knows about us? How much Google or Facebook know about us? What do we share in the internet and how is that data stored? These are only a few questions related to personal information and how we can manage our data. We are afraid that our identity will be stolen, but we keep managing our passwords the wrong way.*

Key Terms *— Cookies Sniffers, Data Mining, Internet Cookies, Privacy, Social Media.*

PRIVACY IN THE CYBER UNIVERSE

The term privacy is a concept that has been growing in the past decades. By nature, we protect what we value, our family, our homes and other material stuff. Every day when we get out of our homes, we make sure everything, the doors and gates that give access to our property, are locked. Who in this day gets out of their home and leave it open? Nobody. That same concept is one that is needed to recreate in the cyber world. When was the last time you logged off from Facebook or any other social platform? Probably you do not remember, or you have never logged off from the application. This is why people need to be **e**ducated on this concept, "Privacy in the Cyber Universe".

When talking about cyber privacy or internet privacy, it is about the privacy and security level of personal data published in the cyber world or internet. Privacy is something that less users care these days in the cyber world, or in some cases, the user does not know the effect of sharing personal data on the internet.

Let us look at some areas in the cyber world and how the privacy concept is managed. What happens with all our data when it is shared on social media? How is privacy managed with Artificial Intelligence (A.I.)? Is personal data safe with the Internet of Things (IoT)? These are some issues that will be discussed.

Social Media

Worldwide, there are over 2.27 billion monthly active Facebook users for Q3 2018 and from these active users, 1.5 billion are mobile users. Currently less people use their PC to access to social media and more smartphones are being managed to be like a small PC. That is the plan and is something that's been developing in a fast way. Mary Aiken in her book "The Cyber Effect" stated that:

Each time we join a new social network, download an app, pay a bill online, buy our children a new digital device, or meet someone on a cyber-dating site, we are faced with a steep cyber learning curve and can quickly encounter new challenges and risks [1].

There are many things we do not know related to what happens with every picture and information that we post on social media. Facebook for example, gives the option to get a backup of all the data shared by the user on the platform. This process was implemented with an account and it segregated by folders all your conversations on messenger, pictures and all your post. If the user has an SMS application

merge with the messenger app it is different. With this process of downloading data, all text messages will be there. On March 2018 the website "The Verge.com" report that Facebook has been collecting call history and SMS data from Android devices. On this article, they report the issue that Facebook stores every single SMS conversation without the users knowing about it. In the Facebook blog post the company "clarified how the data collection works and that the feature is opt-in, but the company did not say why it needs the data or what it uses it for. The blog post also fails to address why the data is collected under the auspices of a contact upload" [2].

The steps for the Facebook archive are:

1. Click or tap the tiny down arrow in the upper right corner of any Facebook page.
2. Select Settings in the drop-down menu to open the General Account Settings page.
3. Choose Your Facebook Information in the left panel.
4. Click or tap Download Your Information.
5. Select New File and select all of my data or fill in a date range for only a specific period. If you previously started a new file and want to add to it, click Available Files instead, and Facebook searches your computer for the previous backup.
6. Choose to download the information in either HTML format or JSON format and select a media quality level. For the best results, choose High.
7. Put a check next to any information you want to download. The list is extensive and covers every possible information category. For example, in addition to the obvious Posts, Comments, and Photos and Videos, you can select Friends, Messages, Profile Information, Pages, Search History, Call logs, and Locations, among others.
8. Click or tap Create File.

Until this point the user is not aware of what can be found of him and relays that everything that is post on the web will be there forever. Our information is being stored and maybe shared without our knowledge. The illusion is that the cyber environment is safer than real life and connecting with other people online, somehow carries fewer risks than face-to-face contact.

The games applications in social media is other area where education is needed. Social media data mining is the process of obtaining big data from users on social media sites and mobile apps. There is a very good article from Michele Wilson & Tama Leaver called the "Zynga's Farmville, social games, and the ethics of big data mining". Michele and Tama explain:

Every mouse-click aggregates onto a wider body of data that is stored indefinitely, to be queried and analyzed to ends that are boundless at most, and vague at the very least. A social network game can take advantage of a user's extant network to send invitations to join him or her by signing up for the game, thereby authorizing the application to access the user's information. The data from those interactions can be an alternative to straight monetization, as users can receive virtual goods when they invite friends who sign up [3].

One of the many companies related to social media games is Zynga (https://www.zynga.com). This company developed these games:

- Farmville
- City Ville
- Empires and Allies
- Texas Holdem Poker
- Adventure World
- The Pioneer Trail (previously Frontier Ville)
- Words With Friends
- Treasure Isle
- Cafe World
- Mafia Wars
- PetVille
- FishVille
- YoVille
- Vampire Wars
- Hanging With Friends (mobile)

One of the most popular for the last year is the game of Farmville. Playing a game on social media is different from a game that is download form the

play store or the app store. Why is this different? When a game is download from a store it will ask for permissions to access to the player camera, contacts, picture or even microphone. What is the purpose of this? To gather data for statistics, how many people access the application and from where they access. If a person plays a game from social media in most cases, they do not know what they give permission to access or what information is being shared from their profile. For example, these are some of the terms that the player accepts to share when subscribing to Farmville:

- Your basic info
- Your email address
- Your birthday
- Your location

Figure 1
Farmville Terms and Conditions

This app will receive all the basic data, and in most cases, the person doesn't know because they do not read or make a search about what they are playing or in other cases buying. This is one of the problems with this type of subscriptions there is an exchange consciously or unconsciously of the players information. The most interesting part of this is that it is legal, because you are accepting their terms and conditions. This is why the concept of the data mining is affecting many users. One question that one can ask is, how does this company generate money if all the applications are free?

This could be a simple question, but it is not. They already have the player's information, they know how many times they play the game, the next thing is to start sharing the game with friends and then buying additional features in the games. The other strategy is the Ad's (Advertising) when someone is playing this type of game they have constant announcements from other games, banks offers, Amazon and other stuff. This will bring the other concept that is pertinent to discuss, the "Cookies". What are the Cookies? In addition, how your information can be exposed because of cookies?

A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it [4]. The cookie is used to give the website a "memory", enabling it to retain information such as:

- User settings and preferences
- Shopping cart on ecommerce sites
- Browsing activity
- Password details
- Previous purchases

There are different types of cookies [5]:

- Session cookies: temporary cookies stored in the browser until the browser is close.
- Persistent Cookies: longer-term cookies that are tagged by the issuer with an expiration date
- First-party cookies: these are created by the site you are currently visiting
- Third-party cookies: are added by a domain that is not the domain you are currently visiting.

For example, Amazon.com stores more information in the user machine; it creates a user ID and generates a session by each ID. With this ID and sessions, Amazon recalls the users interest items and track their history. It is important to know that a web site can only receive the data it has stored on your machine. How does the "One click buy" option from Amazon works? It works because it creates a cookie with an ID and lets the site keep track of the buyer as they add different things to their cart. Each time they add to their shopping cart it is stored in the site's database along with the ID value.

How can cookies generate privacy issues? The information that cookies store (especially if it is a shopping website) can be sold to others that want to sell similar products [6]. Junk mail works because

the information is sold to others. That is why there need to be some laws related to privacy policy that will let the user know that their information will not be sell or shared with any third-party company.

ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

When we talk about AI (Artificial Intelligence) we refer to a set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data [7]. Machine learning is one of the data analysis methods that automates analytical model building. Machine learning is like a branch of AI. AI is growing fast, and it is like a tree with many branches. In the last decades and in different scenarios, the user's privacy has been exposed to malicious hackers.

Hello Barbie by Mattel

In 2015 Mattel released an interactive Barbie, the Hello Barbie [8]. This doll had artificial intelligence and was able to respond to the child; the doll connected to WIFI and had an interactive application where you could access all the recordings.

Figure 2
Reason to Leave Hello Barbie

This generated many privacy issues; all these recordings were sent to a third-party company named Toy Talk. The company never provided the conversations, but a hacker was able to get to the doll system and steal all the information, to the point of being able to make the dolls say whatever he wanted. The company stopped the distribution of this doll because of privacy issues with the children information [9].

Dolphin Attack: Inaudible Voice Command

The interaction from humans and AI has been growing a lot in the past years. Speech recognition systems like Siri and ok Google are extremely popular because they provide voice controllable systems. The Dolphin Attack is a method that lets the user send voice commands that are incomprehensible to people and can control the system using, for example, a frequency of 20 kHz to make it inaudibility for humans but not for AI devices [10]. With this attack; a call or airplane mode can be activated, FaceTime initiated, and navigation systems manipulated.

This is a powerful attack that is being developed fast. Some labs on how to implement this attack can be found on the internet. Security in the AI area needs to keep growing and more authentication process or security policies implemented to avoid this attack.

Table 1
Tested Devices with the Dolphin Attack

Manufacturer	Model	OS/Version	Voice Assistant	Activation[1]	Recognition[2]
Apple	iPhone 4s	iOS 9.3.5	Siri	Y	Y
Apple	iPhone 5s	iOS 10.0.2	Siri	Y	Y
Apple	iPhone SE	iOS 10.3.1, 10.3.2	Siri	Y	Y
Apple	iPhone 6s	iOS 10.2.1	Siri	Y	Y
Apple	iPhone 6 Plus	iOS 10.3.1	Siri	Y	N
Apple	iPhone 7 Plus	iOS 10.3.1	Siri	Y	Y
Apple	watch	watchOS 3.1	Siri	Y	Y
Apple	iPad mini 4	iOS 10.2.1	Siri	Y	Y
Apple	MacBook	macOS Sierra	Siri	N/A	Y
Google	Nexus 5X	Android 7.1.1	Google Now	Y	Y
Google	Nexus 7	Android 6.0.1	Google Now	Y	Y
Samsung	Galaxy S6 edge	Android 6.0.1	S Voice	Y	Y
Huawei	Honor 7	Android 6.0	HiVoice	Y	Y
Lenovo	ThinkPad T440p	Windows 10	Cortana	Y	Y
Amazon	Echo	5589	Alexa	Y	Y
Audi	Q3	N/A	N/A	N/A	Y

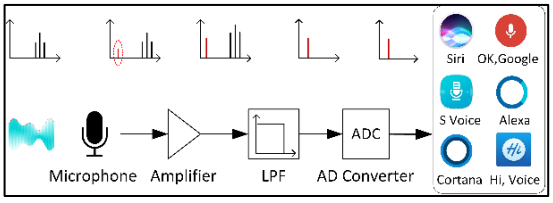

Figure 3
Receiver

SNIFF COOKIES APPLICATION

Searching about the privacy issues in the web and how the internet cookies works, an interesting application can be found that lets the user sniff the cookies traffic and would open the session storage on the cookie and display it in the device, PC or phone. This application is Droid Sheep; a hack tool for Android devices that hijacks social networking accounts on compromised devices. To implement this the phone needs to be rooted [11]. The process of rooting is one that allows the user to obtain root access of the Android operating system and will give administrator credentials to the owner of the phone. What can a person do with a root phone?

- Full customization of the theme and graphic of the phone
- Being able to download any app
- Extended battery life on your phone
- Update to the last version of Android

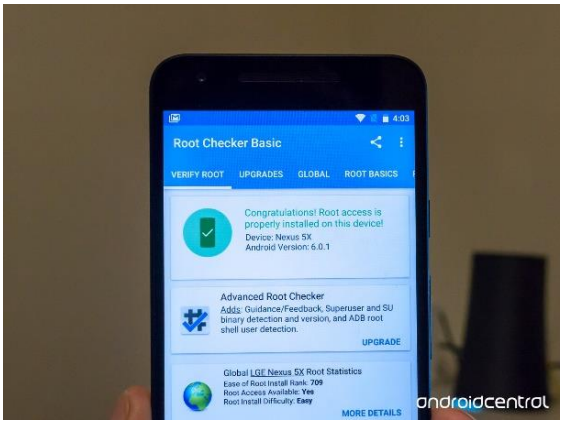

Figure 4
Root Checker Application

These are just some of the privileges with a root phone. However, not everything is awesome with this process. It will have some consequences too like; phone warranty will be lost, and malware and other virus can easily breach your mobile security. Rooting should only be done if the person has full knowledge of how to deal with it. With a root phone Droid sheep can be installed. This application is not in the Google store, it must be found on the web using the file type (.APK). This will give access to the installation file. Figure 5 shows a view of the app.

Figure 5
Droid Sheep Sniffer Output

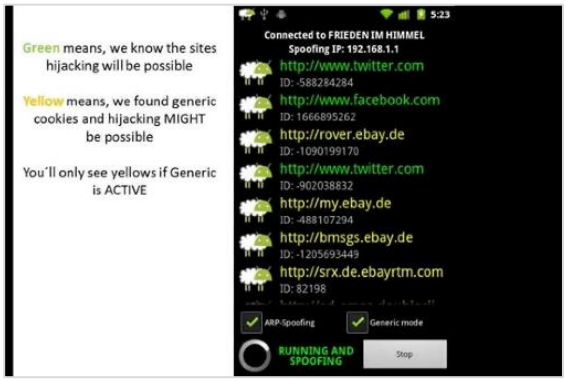

Figure 6
Droid Sheep Sniffer Output Definition

For example, with Droid Sheep a person could open a Facebook session that is stored in the cookies and search the user's profile without their knowledge. This is a big privacy problem because private and specific information can be accessed or even something post, that will affect the owner of the profile.

With all this information, it is obvious that privacy is a big concern today. Technology is growing fast, and users need to keep educated about this and should be more aware of what they share

and download on the web. It is hoped that this project will keep people learning more and more about the Cyber Universe.

REFERENCES

[1] M. Aiken, *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*, New York: Spiegel & Grau, 2016.

[2] T. Warren. (2018, March 25). *Facebook has been collecting call history and SMS data from Android devices* [Online]. Available: https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android.

[3] M. Wilson. (2015, June 10). *Zynga's Farmville, social games, and the ethics of big data mining* [Online]. Available: https://www.tandfonline.com/doi/pdf/10.1080/22041451.2015.1048039.

[4] J. Penland. (2019, January 18). *Browser Cookies: What Are They & Why Should You Care?* [Online]. Available: https://www.whoishostingthis.com/resources/cookies-guide/.

[5] S. Smith. (2010, June 1). *How to stop cookies stealing your personal information* [Online]. Available: https://www.computerweekly.com/opinion/How-to-stop-cookies-stealing-your-personal-information.

[6] B. Marshall. (2000, April 26). *How Internet Cookies Work* [Online]. Available: https://computer.howstuffworks.com/cookie1.htm.

[7] S. Warren. (2018, January 10). *Artificial intelligence and privacy* [Online]. Available: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

[8] W. Meer. (2015, November 11). *Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns* [Online]. Available: https://www.huffingtonpost.com/entry/hello-barbie-security-concerns_us_565c4921e4b072e9d1c24d22.

[9] S. Gibbs. (2015, March 13). *Privacy fears over 'smart' Barbie that can listen to your kids.* [Online]. Available: https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel.

[10] G. Zhang. (2017, October 20). *What is DolphinAttack?* [Online]. Available: https://github.com/USSLab/DolphinAttack.

[11] M. Jansen (2018, November 29). *How to root Android phones or tablets (and unroot them)* [Online]. Available: https://www.digitaltrends.com/mobile/how-to-root-android/.