Social Computing and Information Assurance

Balaji Chandrasekaran
School of Computing, Informatics and Decision Systems
Arizona State University
Tempe, Arizona
bchandr6@asu.edu

***Abstract*—The interaction of people with computers are increasing exponentially day by day. It paves way for various kind of threats and cheating due to the increased interaction of humans with their gadgets. Social Computing is a paradigm that deals with interaction of users with each other through a computing device. Many a time the social computing is the target of hackers. In this paper, we deal with various sub divisions of social computing and study each one of them in depth. We also try to find various weakness present in it and propose solutions to them if there is any. We also talk about the preventive measures that could be taken for securing information and study several case studies to achieve the same.**

Keywords—Social Computing; Bluetooth; Wearables; Social networking; video games;

I. INTRODUCTION

Social Computing is the new paradigm of computing that is increasing exponentially day by day. Each user spends hours of their time in the social computing paradigm one way or another. The social computing paradigm comprises of many things including Online Gaming – Steam games, Warcraft, Dota 2, Social Networking – Facebook, Twitter, Instagram, Snapchat, Wearables – Smartwatch, glass, VR etc. There several other social computing sources as well, in this paper we are going to elaborately study these three sub categories. As we can see form the above example of social computing, it is something that is not going to perish and as long as human life exists on this planet there is going to be an exponential increase of users in this paradigm day by day. As the users increase the number of peoples that is the hackers who are trying to exploit the environment also increases. Information is the new wealth of humans and the new currency. Information can either make you a billionaire in overnight or bankrupt your business. As we humans always do when it comes to matter of such important things it is necessary in this case also to thorough study of the information theft and we should take all the necessary steps to protect our information as it is a matter of life or death. We will study in depth of the various mechanisms that could be used for stealing information and analyze each one of them. In wearables, we study about the security of the medium of communication, security of the device itself and role of individual in protecting his/her information. In social networking, we study regarding various spams, user pro activeness, user prevention measures, we talk about the various ways users can be cheated in Social gaming, the need for protecting the servers and identity theft. We study several case studies like the second life [1], Age of cannon [2], Polaris Bot [3], AFS Software Card Shuffling Algorithm [4], Absolute Poker Insider Attack [5]. We acquire certain knowledge from these case studies and use them to prevent future mishaps.

II. SOLUTION EXPLANATION

The introduction we dealt with three paradigms that we are going to do in depth study about. All the three paradigms are affecting the lives of humans one way or another. The prime most important thing is that all these paradigms are growing day by day and they are made up of information that is always at the risk of being attacked by hackers. We should deal with the various threats that the paradigms face and the concerned creators should also be proactive in eliminating future threats.

We will do a thorough security assessment on each of the three environments that we will be studying and provide with some feedback on the same. We will then be providing some of counter measures to mitigate those threats and give us a view of what are the root causes of them. We will also be providing to users with some information about the pivotal importance of their role in these environments to safeguard their information.

A. Online Gaming Industry.

Online gaming industry is something that makes up the life of several individuals. I myself am aware of many individuals whose life is all about gaming. There is a multibillion dollar industry revolving around the online games platform. There are several different famous online multiplayer games whose main objective is to provide a social environment and culture which makes people to enjoy themselves. We all would have heard of Dota 2, counter strike, league of legends etc. Dota 2 conducts international tournament in which all the teams in the world participate [6]. It happens in Seattle gaming arena each and every year. The prize money is collected from the users itself who buy tickets to watch the event online for free, last year's prize pool for the game was somewhere around tens of millions of dollars and each ticket just costs $7 which shows how big of a user base it has. Online gaming Industry is so vast that people do it as their full time for living, it has become their source of income. People do live telecast of their game play as well every day via several streaming sites like Twitch, YouTube gaming etc. All these tells us the importance of data that gaming industry revolves around and provide us a greater cause to safeguard it from various threats that are present. A study shows that almost all age group people get involved in one or another form of video games which involves playing online with various known and unknown people. ZeniMax media Inc

is a company responsible for analyzing various gaming companies and provide them with information assurance [7]. This company is responsible for several successful stories in the gaming industry. It is always a good idea to obtain helps like this whose main goal is to provide advice and solutions to various security concerns and issues that are present. This is so because even though there could be an internal team of well qualified testers and creators there could be something we can miss as we are all humans. To avoid such situations, it is always a great advantage to seek the help of such huge companies whose primary goal is to find and seal bug in the product like quality testing. The few of the common loopholes or the common security issues that we identified in gaming industry are.

- There is not a proper way of checking attacks like the Man in the Middle attack or eavesdropping etc. The server and client interact whenever there is a information required from the server or there is a need to communicate with another client. There should be some check done by the gaming companies with respect to such medium of communication.
- One of the most recent mess are the ads which the gaming companies post without proper background check which could lead to users being redirected to malicious sites which could steal any kind of information from their personal information to the credit card.
- There is improper encryption in place for data transfers between clients and server-client.

There should be proper measures need to be taken to reduce the number of threats that are present. Every gaming company should shift their importance towards the development of security feature rather than development of new interesting games. A loss or an attack on the games that the company as is equivalent to losing their customer base and their reputation.

B. Wearable Devices.

Wearable devices are the most recent technology advancement. Even though they are the most recent ones the user base and the users involved in it is huge. We do see videos posted on YouTube every day with respect to their amount of run they recorded on Fitbit or the number of calories burnt on their apple watch etc. Wearables does not stop over there but they also get extended in medical field. Wearables are saving lives of millions of people who are having serious medical conditions and cannot survive with the support of technologies. The information that the wearables handle is very sensitive and important as they include huge amount of personal information from location to medical condition.

Wearables can be attacked in several different ways as they are involved in several different environments. Broadly speaking 1) We could either attack the medium of communication between the wearable device and the mobile device. 2) We could attack the medium of mobile device and the server or the wearable and the server and steal huge amount of information. 3) We could also attack the server itself and steal information that is stored in the server and which is used for historical purpose. Even though there are several ways in which a wearable and its information could be compromised the most frequent one that is under attack would be the Bluetooth connectivity of the wearable and the mobile device. The Bluetooth connectivity is under attack very often due to the reason being it is the most fragile one in the world that the Wearables live in. Bluetooth cannot include lots of security features and it is very limited in processing power and battery power which is one of the main reason they are always under attack.

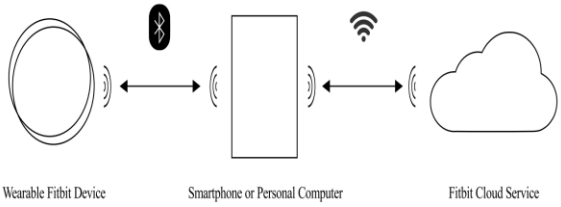

Fig. 1. Werable Device Communication. [8]

Bluetooth is just a standard of wireless communication which is used for communication between devices in a short range. There are several kinds of attacks with respect to Bluetooth which being denial of service (DoS), Man-In-The-Middle-Attack(MITM), eavesdropping, modification of messages etc. It is important that we study the security of Bluetooth in general and provide various solutions that could be used for all these kinds of attack.

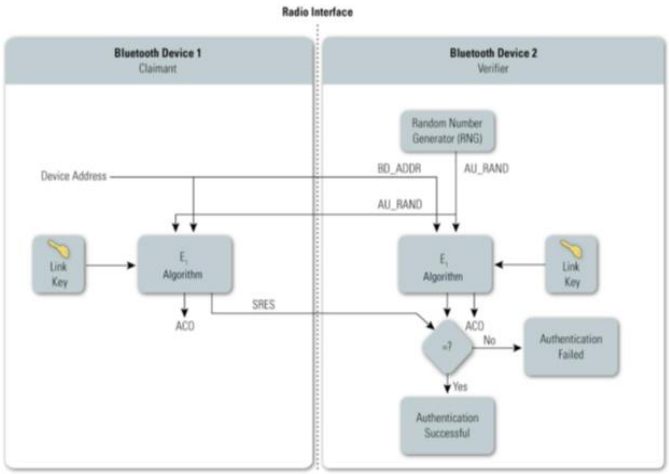

Fig. 2. Authentication Of Bluetooth Device. [9]

There are three broad spectrum of security features provided by the Bluetooth technology, these are the three different modes in which a Bluetooth device can operate. These modes are Mode I, Mode II and Mode III [9]. Mode I involve very little to no security and thus it should never be used when manufacturing the Bluetooth device. In this mode, there is no security feature which is used for authenticating the connectivity thus any device can send any data to any other device and they communicate. This mode also lacks the data encryption mechanism thus when two devices communicate all the information are transferred as native text. The Mode II as medium security features, this mode is also known as the

service level security mode. The mode is called as service level security mode because the security feature is incorporated into the device by the application and not the device itself. Thus, if there is no security with respect to the application which handles the Bluetooth device then there will be no security. This way of handling security we could skip several security threats or just cannot implement counter measures for them in this way. Mode III is the security mode which as the highest level of security feature and this mode should be the one which would be used by all the device. This mode provides security mechanism for both authenticating the devices for connectivity and also for encrypting the data to transfer between the devices. Even though there are these modes available but there always the flexibility or the decision to choose the mode rests in the hands of the manufacturer. This should not be the case and the importance should be given to the security and there should a rule that all devices follow the security Mode III which could help resolve lots of problem related to information theft.

C. Social Network Medium.

Social Network is the new medium of communication between humans rather than in person, one of the main reason behind this is the number of features that it brings to the users table when two of the users who want to stay socially connected are miles apart, the accessibility it provides to the user for connectivity which makes the user to connect to another any time and date given. There could not be a single person in the world who do not own a social networking account. There are several types of social networking platforms that are available like Facebook, twitter, myspace, hangouts, etc. Users who use such social networking medium shares huge amount of information with each other which are very sensitive and important. There are several kinds of attacks that could take place in social networking platform like phishing, Clickjacking, Sybil attacks etc. Users play a very huge role in avoiding several of these threats and it should be the responsibility of each of the user to protect his or her own information.

III. DESCRIPTION OF RESULT

There are several recommendations that should be implanted in each of the three environments that are under study to make it a safer tomorrow.

A. Online Gaming Industry.

It is the duty of both the game developers and the users to safe guard their information and to use the platform in a proper way so that one can avoid information theft.

- Users should be cautious while sharing their information. They should also take extra care on with whom they are sharing their information with.
- Users are advisable to maintain a separate identity from their email address to everything so that the attacker would not be able to easily track them and exploit them with their information.
- Users should be extra cautious and try to avoid sites which are they not aware of for payments etc.
- The companies should train and provide proper ground rules to all the employees of the company so that they can follow them for advanced security measures.
- The main object or goal of the company should be to maximize the security level of the application and handling of information within the company.
- All the games should be carefully monitored, tested and examined in a beta testing environment before deploying it into production.
- There should be proper encryption when it comes to information exchange via a medium with respect to the product.

B. Wearable Devices.

Wearables are very important part of human survival just like the mobile phones for communication. Wearables improve the living standard of several individuals in their day to day life activity from fitness tracking to monitoring their heartbeat. They cannot be eradicated but for the future industry of wearables there should be a proper platform and ground rules deployed so that one can avoid past and future security threats.

- Each of the manufacturer must provide the users with proper awareness about their device and what will be their responsibility to use the device in an effective and hassle free manner.
- Each of the manufacturer must do an internal check on regular basis and improve the security measures that are in place and check whether they are being followed properly.
- There should be proper maintenance of the inventory of the devices that are being sold and which are active and which are not so that it would be easy for tracking and identifying the bug in a future perspective.
- The Bluetooth devices must always use the highest level of security feature that could be incorporated.
- The level of range a Bluetooth device as should be very minimal which avoid the range needed by the hackers for hacking the device there by reducing the hackers as well.
- Security PIN on the Bluetooth device must change often so that to avoid easy hacking of the device.
- The password that is present for protecting the Bluetooth device must not be same as the other ones the user use and must not be easily predictable.
- The data transmitted should always encrypted with high level of encryption.
- There should be possibility of inducing biometric security feature into the device for the extra layer of security.

C. Social Network Medium.

- Users must change their password on a regular fashion.
- Uses must use the two-factor authentication feature if it is present to be able to provide the extra layer of security feature for protecting from the hackers.
- The information shared via social networking sites should not be very sensitive ones.
- Do not get hacked by clickjacking. Make sure you click the proper and known links and use a search engine to access the same link rather than becoming a victim of clickjacking.
- Always add only those people whom you are aware off and ignore unknown profiles.

IV. Contribution To The Project

The project and team was subdivided based on the three main environments of study and each sub team where given with a topic of research. The team that I belonged to was wearables. The goal of our team was to study about the newest trends in wearables and the security issues concerned with the same. We choose a single topic which would be the sub topic of wearables and built upon the project on it. The topic that I chose was Bluetooth Security and I was responsible for researching on it. All the subtopics and information provided under Bluetooth security was a research work of me. I was also responsible for the recommendation part for wearables and I wrote the conclusion and recommendation for wearable devices. I had to research six papers and several online resources to provide my team with solid information regarding the wearables and its connectivity. The topic of Bluetooth security was spoken by me during presentation and the slides regarding Bluetooth security was prepared by me.

V. Knowledge Acquired

The project provided us with vast amount of knowledge regarding information assurance. The project thought us on the importance of Information security, the drawbacks present in current trends and human life with respect to information security. The project provided great insight into security of wearables, the Bluetooth security, the connectivity, the data in cloud security etc. It gave us insight into information assurance on social gaming paradigm. The importance protecting information in social networking etc. It provided us with knowledge on the role of myself as a developer in the developer community and measures that I need to take to protect my software and the data of users involved with my software.

Acknowledgment

We thank professor Stephen S. Yau for giving such an opportunity to do a research project which helped a lot in understanding the importance of information assurance in daily life. We thank teaching assistant Tamalika Mukherjee for helping us in completing the project.

References

[1] Create Virtual Experiences. (n.d.). Retrieved March 23, 2017, from https://www.lindenlab.com/

[2] Action Adventure and Massively Multiplayer Online Games (MMOG). (n.d.). Retrieved March 23, 2017, from http://www.funcom.com/

[3] Davis, S. B. (2009). Protecting Games: A Security Handbook for Game Developers and Publishers. Course Technology PTR.

[4] Hoglund, C., & McGraw, G. (2008). Exploiting online games: cheating massively distributed systems. Boston: Addison Wesley.

[5] How Online Gamblers Unmasked Cheaters. (2009, June 28). Retrieved March 25, 2017, from http://www.cbsnews.com/news/how-online-gamblers-unmasked-cheaters/

[6] Dota 2. Accessed April 12, 2017. http://blog.dota2.com/.

[7] Mohr, S., & Rahman, S. S. (2011). It Security Issues Within the Video Game Industry. International Journal of Computer Science and Information Technology,3(5), 1-16. doi:10.5121/ijcsit.2011.3501

[8] Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security Analysis of Wearable Fitness Device (Fitbit). Retrieved from http://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf

[9] Bouhenguel, R., Mahgoub, I., & Ilyas, M. (2008). Bluetooth Security in Wearable Computing Applications. 2008 International Symposium on High Capacity Optical Networks and Enabling Technologies. doi:10.1109/honet.2008.4810232