The Online Murder: Death via Hacked Internet Connected Technologies

Nishtha Girotra*
Raghunatha Sethupathy**

Abstract

Recently it was specified in the newspaper article that the first online murder is expected to take place in the end of 2014, but fortunately there was no such incident. After this news, everyone in this world really wanted to know about online murder and the events which are associated with it. So this research is an attempt to study about the online murder and its consequence where the researchers have adopted a theoretical review of various documents available in the globe. The authors have made use of the online articles for carrying out this particular research and this is non-quantitative research adopted by reviewing the existing literature.Online murder is one among the gravest cybercrimes and it is predicted by the European police office (Europol) that in near future one such murder will soon occur. So the paper lays its great deal of emphasize on online murder which is classified in this paper as Direct and Indirect murder. The researchers have also focused on the conversion of the society from Internet of Things(IoT) to Internet of Everything (IoE.) The paper focuses on the security aspects of online murder with special emphasize on the Indian Scenario.

Keywords: Online Murder, Internet of Everything, Europol Report

Introduction

The time was called as 'age of machines' of late 19th and 20th century and then came the 'age of information' which was when the period of computerization began .Now, it is the era of 'internet of things' and within few decades there will be a time when the internet will be connected to everything and it will said as the era of 'internet of everything'. With the increasing accessibility and connectivity to internet, heinous crimes are also increasing and the biggest crime i.e murder, can now be done by a person sitting far away, by just cracking into the somebody's system and that too, just with a press of a button. He can then stop the functioning of any system or enter some malicious codes and thereby, taking all control in his hands, he can endanger the lives of innocent people. Online murder is one among the gravest cybercrimes and it is predicted by the European police office (Europol) that in near future one such murder will soon occur [1].Cybercrimes are increasing at a rapid rate and there is an urgent need to check this .If proper steps are not taken, some easy cheap tools and services will help nefarious people to execute their plans easily. The authors have made use of the online articles for carrying out this particular research and this is non-quantitative research adopted by reviewing the existing literature.

Nishtha Girotra
Student, Campus Law Centre, Delhi University
E-45, Kamla Nagar, New Delhi

Raghunatha Sethupathy
Student, Campus Law Centre, Delhi University
8/61, Vijay Nagar Double Storey, New Delhi

Internet of Everything

In the virtual world, there is an easy connectivity to physical items around us but the unfortunate part is that the hackers can easily step in the working of these systems and then hack, control, and create and cause issues, due to low cyber–security. With the help of Radio Frequency Identification (RFID) and sensor network technologies everything from automobiles, home appliances to medical devices all will be soon connected. This is easily evident with the increasing use of wifi and wireless internet connectors. Today, around nine billion devices are connected to internet, and the number is increasing at such a fast pace that

probably by 2020 around twenty billion appliances will be connected. From exercise machines, electric toothbrushes, sewing machines, electricity meters, washing machine and thermostats etc. all are connected to networks and rest appliances will also be soon in communication with these.

Death by Internet

Homicide caused through internet can be done in two ways –

3.1. Indirect murder
3.2. Direct murder

Indirect Murder

Killing through the use of internet has become a common piece of news since 1990's. All corners of the earth are connected today and this connectivity like any other advancement has also come up with the frightening crimes. Earlier in early 90's the crimes were carried on by publishing advertisements in newspapers and inviting deceitfully naïve people to submit to the cruelty of the criminals. The trend changed with the growth of the use of internet which has become the fertile ground to cheat people. There have been many cases of extortion, blackmailing through internet. Also online dating, chat rooms, online marriage bureau, and advertisements are the tactics used by the notorious criminals to commit murders .This is an easy weapon for them and their enemies are an easy prey of this. The below given few examples will make it clearer:

1. The planned murder of OfirRahum, Palestine Liberation Organization, took place after a long conversation of the criminal with the victim through ICQ where the victims came for romantic purposes;he was shot down on coming to Jerusalem. [2]
2. Michael JhonAderson, a resident of Savage, Minnesota, whousedCraiglist, was convicted for calling a lady for babysitting job and then shooting her [3].
3. In 2009, Christian Goother, who was believed to be 'first German internet killer', confessed that he had killed women using chat rooms [4].
4. In 2011, a girl student from IIM, Bangalore has put herself to death after her boyfriend who was an alumnus of IIT,Roorkee posted a hurtful message about their breakup in his facebook wall [5].

According to The Dailymail report, around one Facebook crime occurs in every 40 minutes.

Direct Murder

New kind of murders is predicted to take place in near future where a person can be killed easily by the use of networks. This is more easily evident in the case of medical devices. It is believed that many devices like the insulin pump, heart pacemakers etc.can be easily hacked and mishandled resulting in an over dosage or an explosion. This particular concept of online murder, is not new but in a report by a medical cyber -security pioneer, Kevin Fu and his partners, this idea was brought forward in 2008, where he mentioned that the medical devices like pacemakers can be hacked [6]. In case of insulin pumps, a security researcher, named Jay Radcliffe, has shown how by the use of strong antenna, the device can easily be hacked. This hacking would have the potential to kill the victim and the criminal can do this even by being half a mile away from the site .The connected insulin pump is used to have controlled frequency and amount of dose for a better treatment. The data entry is given by an external blood glucose device and this advanced continuous glucose monitor uses sensors which can also be hacked and then misused to the extent of causing death [7]. Baranby Michael DoughlasJack, was a New Zealand computer security expert who showed that a laptop which is 50 feet away can easily hack a pacemaker and create a shock of 830 volt by increasing the jolt of electricity in the device. He also brought forward the way how one can onboard firmware can be rewritten and the device can be corrupted. The servers can now be diseased with malicious firmware and that would be capable of infecting pacemakers and ICDs. He said in his blog that "We are potentially looking at a worm with the ability to commit mass murder [8]." A highly controversial issue is the murder of Rolling star and Buzfeed hero, Michael Hastings, who died in high-speed car driving and it was believed that it was a case of cyber-attack. The Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Richard Clarke, also said that 'the car accident was consistent with cyber-attack and the

reason is that, the intelligence agencies actually know how to catch hold of the control of the power of the car. Also before the accident, Hastings had informed other journalist through an email that FBI had an eye on his activities.

Security

When the two computers were connected for the first time, the data protection issue arose and security measures were taken. Then with the advancement and use of networking, the security was needed to be strengthened. Today, an era is about to come when internet will be well connected to everything i.e both virtual and physical world and we would need to be little more careful about cyber-attacks which otherwise would become an easy weapon to commit evils. To have a safe environment around proper security should be maintained. Failing to address these issues, things such as nuclear reactor to cars would be hacked by the Cyber-Criminals, thereby leading to Mass-Murders as it appears in Video Games.

Crime as a Service

Europol have mentioned in its meeting about the increasing cybercrimes services but the question arises as to what it is all about? This is actually a service provided by the underground criminals to people who do not even if have much technical knowledge, can commit cyber –crimes by just paying money for the tools and skills. The arrangement of money for a criminal attack is done by all customers together. By this way the service providers can earn a lot of money and the demand of these notorious customers are also fulfilled, with the small investments and without even having any expertise in it. This service now seems to be very attractive, with more and more people entering into it since profit earned out of this business is more than that of an amount, which the hacker gets from hacking and also investments made by the users, is comparatively smaller. So because of these things, a hacking is no more a big deal and these underground service is also a good market, an easier, cheaper and a simple channel to all crimes.

Indian Scenario

Recently, the Government of India has come out with the Digital India and Smart City Initiative Project which has many proposals and one of the proposals is the constitution of National Cyber Security Coordination Centre where the Government has proposed to spend around 11,000 Crores by 2015. So this proposal of the Government of India is an initiative in combating against large scale cybercrime including online murder. One of the important step taken in the Digital India Program of the Government which focuses at 'transforming India into digital empowered society and knowledge economy' is expected to provide a development of the IoT industry ecosystem in the country. Since India is converting itself from Internet of everything (IoT) to Internet of Everythings (IoE), the incident of online murder is not so far from the future.

Conclusion & Suggestion

In an article by Joseph Stienbergh, a columnist of cybersecurity, he mentions that the appliances we use today from television, laundry machines, telephone, medical devices, mobiles, and thermostats and even hand guns can be hacked. They can spy on us and collect all our data easily [9].

The following are the suggestions which can be done on an individual level:

1. One should not open unnecessary links which are popping from unknown websites and e-mail attachments received from unknown sources.
2. One should always keep their security software updated as by doing this, the security can be increased and viruses can be removed. New Viruses are discovered every day and based upon which anti-virus system are enhanced and strengthened.
3. One should avoid keeping the same password for all accounts as these in some or in the other way leads to hacking of the accounts.
4. Instead of using public wifi connection, one must invest in virtual private internet connection and securing the wifi connection is also an important task which has to be kept in mind.

On the other hand to control these cyber-attacks, changes must be made to security and legal systems. One of the reasons why these wireless devices are facing problems is that they were not built keeping in mind

the security issues. The systems used in the hospitals are running old windows version which can be easily hit by virus attacks. The real problem is that these systems [10] are not even allowed to update their versions due to regulatory restrictions. By loosening the restrictions on the equipment and bringing a change to legal protection issues, some good changes can be brought. The cyber-criminals are not just limited to a particular or native country but they are present everywhere around the globe. According to a report by the head of European cybercrime Centre, Paul Gillen has suggested that there should be collaboration among the nations to stop these activities. The report also states that these cyber-attacks can be committed internationally and so the working of all nations and collectively becomes more important thing. The medical devices and all physical appliances connected to the network, should have a tighten security which needs to be constantly updated and access to the information of the data, must be disallowed as these may sometimes leads to Cyber-attacks.

References

1. The Times of India Correspondent,"*first online murder may happen by the end of the year: experts*" Times of India retrieved on October 6,2014 at, http://www.thehindu.com/sci-tech/technology/internet/first-online-murder-may-happen-by-end-of-year-experts/article6475534.ece.
2. Hersham Tania , "*Israel's 'First Internet Murder'001,*" New York daily news, 19 January2011
3. Michael John Anderson, *"Craigslist Killer Michael John Anderson*", New York Daily News, April 21, 2009
4. London Telegraph, *" Internet killer' admits murdering women he met in online chat rooms"*, January 15, 2009
5. NDTV Correspondent, *"IIM student commits suicide amid disturbing Facebook messages"*, NDTV (2011) retrieved on 12 January, 2015 at http://www.ndtv.com/article/cities/iim-student-commits-suicide-amid-disturbing-facebook-messages-134966
6. Kevin Fu and partners, *"Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses"*, symposium on Security and Privacy.
7. Jerome Radcliff, "*Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*", symposium on Security and Privacy,(2008)
8. Darlene storm, "*Pacemaker hacker says worm could possibly 'commit mass murder*", Security is Sexy, 17 October, 2012
9. Joseph Stienberg, "*these devices may be spying on us(even at our own home)*", Forbes, 2013.
10. Website, *Department of Electronic and Information Technology, Ministry of Communications and IT, Government of India* retrieved at http://deity.gov.in/content/internet-things on 14, January, 2015