3rd International Conference on Computing: Communication, Networks and Security (IC3NS-2018) ISSN: 2454-4248
Volume: 4 Issue: 3 61 – 65

Botnet of Things: Menace to Internet of Things

Tarini Tyagi

CSE-BDA, CET-MUST, Lakshmangarh *tyagitbkn@gmail.com*

Abstract: The mesh of internet has always been, and always will be a magic box. This necromancy has the propensity to connect every 'thing' to the internet. Emerging from the general stuff similar to smartphone, printer, laptop, desktop, i-pods, i-pads, tablets, webcams, smart watches, baby monitors, drones, thermostats, yoga mats spanning to technology like driverless car, smart home, smart glasses, smart refrigerator, smart fry pans, smart TV and if we talk about implantation of chips in humans and wearable tech than we ourself will be connected to internet. In the race to lay the foundations of a technologically connected world, both the mass-producers and the users have created dangerous side effects known as botnets.

The IoT botnet is a flock of devices connected to the internet and controlled by a chief system. Botnets are getting chunky and mighty simply because the number of vulnerable devices is going up by orders of magnitude over a couple of years. The botnet of things has transfigured our internet of things into the internet of menace. This paper touches on the areas of Cybersecurity, intrusion detection, the major threat to the internet of things, botnet of things and prevention systems. We emphasize the importance of selecting and putting into practice features that can lead to an meticulous method to handle the botnets.

Keywords*: IoT, Botnet, Cyber Security, talking planet, RFID, cloud computing, AI.*

*****

1. Introduction to Internet of Things

Internet of Things gives the impression of being most sought-after word in IT and business at the moment but notion is significantly old. The term was elementally coined by Kevin Ashton at AutoID lab in MIT. He was one of the trailblazer who conceived this conviction as he cast about the ways that Proctor & Gamble could outdo its business by linking RFID information to the Internet. The idea was that if all objects in typical routine life were equipped with identifiers and wireless connectivity, these objects could meet up with each other and administering can be done by computers. The idea was simple but powerful. At that time, this vision required major technology refinements. After all, how would we strap everything on the planet? What type of wireless communications could be built into gadget and what changes would need to be made to the veritable Internet infrastructure to bolster up billions of new devices communicating? There were many queries but no answers to the IoT notion in 1999.

Today not only many of the stumbling blocks are vanished, the technological elevation in IT is commendable. The acreage and cost of wireless radios has dropped tremendously. IPv6 has the capacity to earmark a communication address to billions of devices and many electronics companies are also erecting Wi-Fi and cellular wireless connectivity into a voluminous range of gadgets at a satisfactory cost. Mobile data coverage has improved eloquently with many networks offering broadband speeds. At the present time we are all connected by the internet, like neurons in a giant brain. Starting from the general stuff like smartphone, printer, laptop, desktop, i-pods, i- pads, tablets, webcams, smart watches, baby monitors, drones, thermostats, coffee makers, washing machines, headphones, lamps, yoga mats spanning to technology like driverless car, smart home, smart farm, smart glasses, smart refrigerator, smart fry pans, smart TV, smart car and if we talk about implantation of chips in humans and wearable tech than we ourself will be connected to internet. And almost anything which we can think of can be connected to internet.

Meticulously the **IoT** is the interconnected structure of devices, home paraphernalia, conveyance and other artefact embedded with electronics, sensors, software, and connectivity which fetter these objects for interchanging data. Each 'thing' is uniquely perceptible through its embedded computing system but is in a position to inter-operate within the existing Internet foundations. The IoT empower objects to be sensed or controlled remotely across existing network infrastructure. It creates right set of circumstances for more straight through integration of the physical world into computer-based systems and resulting in improved expertise, exactness and economic benefit in addition to marked down human intervention. Internet of Things had given birth to many proud technologies such as smart grids, virtual power plants, smart homes, smart farm, intelligent transportation and smart cities.

"Things," in the IoT utility, refers to a voluminous variety of devices such as heart monitoring insinuates, biochip transponders animals, sensors in soil of a smart farm, cameras streaming live feeds of wild animals, automobiles

with built-in sensors, DNA analysis devices for forage monitoring, a JCB on the under construction site or field operation devices that assist firefighters in search and rescue functioning.

2. Impact of IOT on mankind

Nowadays, there are more cell phones than there are people on the globe. By 2020 it is calculated out in advance that 2.5 billion affixed people will be there on social media networking and 50 billion affixed things will be used or accessed by them. This "maniacal-connectivity", known as the IoT, will lend a helping hand in driving $65 trillion in global trade. The precept of the future epoch will be, "Everything that can be connected, will be connected." But why on this globe would you require so many affixed devices talking to each other? There are many examples for what this might look like or what the potential value might be. Say for example after your phone alarm had wake you up in the morning, it will inform your coffee maker for preparing coffee, bathtub to be ready with the water and your closet to be ready with the clothes. While you are on your way to a conference, your car could have access to your calendar and already know the best route to take. If the traffic is hefty your car might send a text to the other party about the picture that you will be late. What if our workplace gadgets knew when it was running short on supplies and automatically re-ordered more? What if the wearable gadgets we put in use in the place of work could tell you when and where we were most spry and high-yielding and dispense that information with other gadgets that we use while working?

On a broader scale, the IoT can be applied to things like transportation networks: **"smart cities"** in which we'll be informed by our car which root to take as per the traffic, in case of accidents near by ambulance will be informed to reach the spot immediately, in case of rash driving, the warning notice along with the video recording of our driving captured by the road camera will reach us and we have to pay the fine. Adapting IOT can help us reduce waste and improve efficiency for things such as energy use and can also help us understand and improve how we work and live.

Impact of IOT can also be seen on agriculture arena by the means of **"smart farming"** Agriculture is the major source of economy of our country and it can be optimized with IOT. Crops will themselves inform their farmer about the water level in field, nutrition in soil, or moisture in air. When the temperature rises and the humidity level in the field goes down the crops will sense it and send a message like "I am Thirsty" to their farmer. The farmer can turn on/off the motor on his field by a phone call to the motor simply sitting at home.

There can be **smart smoke detectors** and we will be receiving warnings on our phone or wearable device when IoT networks detect some physical danger nearby.

We have our **smart fitness trackers** which automatically keep track of exercise habits and other day-to-day personal activity including goal tracking and regular progress reports. Next to them is our **Home automation system** and we had implemented antique versions of this concept like smart light bulbs, plus other devices like wireless scales and blood pressure monitors that each represent examples of IoT gadgets. Wearables like smart glasses and watches are also conjure up an image of future of IoT systems. Prodigious news is in market as our favourite tech giant Google recently publicize that it is partnering with top-tier automakers Audi, General Motors and Honda to brought **Android-connected cars** on the roads. Google at the present moment is developing a new Android platform that will give us the ability to connect cars to the Internet. Very soon in time, car owners will be able to lock or unlock their vehicles, start the engine or even monitor vehicle performance from a computer or smartphone. The idea is to create a **talking planet** by means of IoT. If we combine AI with IoT then imagine all the satellites in outer space are AI and can communicate with each other and with all the systems on earth. **Satellites will themselves learn about the space by the means of machine learning and all the changes will be updated all over the world by the means of IoT.**

3. Probable benefits of IoT to the business world

Business field opportunities are increased: IoT opened to the public the door of chances of advancement for new business and helped companies to advance by sophisticated business models and services which have fully formed new revenue streams. Reduced market time, raised returns on investment and strong business base is the result of IoT based innovations. IoT had transformed the way businesses and consumers approach the world.

Asset utilization is enhanced: Tracking of the precious assets like equipment, machinery, tools, gadgetry and their utilization by the employees is far more easy using sensors and connectivity.

Efficient processes: Being connected with a fairly large number of devices to the internet, IoT allow corporations to be smarter with real-time operational insights and also they get a very wide range of devices to advertise upon. The data accumulated from incomparable network, user's phone, social media network, factory floor, and supply network will help reduce inventory, time to mart and downtime on account of maintenance.

Increase in productivity: In the profitability of any business, productivity has an paramount role and IoT is easy to be adapted by organisations and it offer just-in-time tutoring for employees, ameliorate labour effectiveness, and reduce unsuitably matching of skills hence increasing organizational productivity.

Cost cutting: The enhanced asset utilization, productiveness, and processing efficiencies can save the expenditures. IoT generates a lot of data contributing largely to big data. This data can be used for predictive analytics and real-time diagnostics which can drive down the maintenance costs.

4. Threat to the Internet of Things

IoT had tremendous potential and there is magic in this web of IT. The question arises what stops us from adapting it to the fullest? Why we still resort to these old methods? On this very day, we have close to 5.5 million smart devices across the world connected and talking to each other over the internet. But with its size grows the threat. Cyber Security people worry that hackers will have an almost infinitely larger surface from which to launch new types of attacks as more things get connected to the Internet. The figure of over 1 million malware attacks reported on a daily basis leaves us without any of the question that this threat is real and elevating. This is because devices that are becoming part of the IoT have little or no security protections against network-borne threats and are often easy to exploit.

The blowing up of interconnected devices and the Internet of Things has triggered new indispensable challenges in the zone of internet security, due to the various device vulnerabilities and augmented potential for cyber-attacks. In the race to create a technologically connected world, both the manufactures and the users have created dangerous side effects known as **botnets**. Almost all threats to this web of IT like insecure web interface, insufficient authentication/authorisation, insecure network services, privacy concerns, insecure cloud interface, insecure mobile interface, insufficient security configurability, insecure software/firmware and poor physical security and lack of transport encryption can be easily coined under one roof and that is Botnet of Things.

5. The Botnet of Things

The IoT botnet is a flock of internet connected devices controlled by a chief system. The term is most famous for malicious hacking especially Distributed Denial of Service Attacks (DDoS attacks). In this case, to infect a network resource like websites a hacker uses a large botnet group of internet-connected devices so that licit users cannot outbreak through it. By accessing thousands of devices through a botnet, all with their private distinctive IP addresses, the hacker makes it almost out of the question to stop the attack or distinguish authorized users from hoaxed ones. At the heart of these threats are large numbered lumped hosts sitting in homes, business venture, schools, and government offices around the world. Systems are contaminated by a bot that communes with a bot controller and other bots to form what is often referred to as a zombie army or botnet. With the emergence of IoT botnets, IoT is turning out to be an internet of vulnerabilities for cyber criminals. There's a little or no built-in security in these internet affixed devices. And even if they have then also the basic step of setting a password for them is often neglected by the user making them easy targets for hackers wanting to create and use a botnet.

Internet of things gadgetries are not drafted keeping security in concern and often have almost no way of being patched. Botnets are getting chunky and mighty simply because the number of vulnerable devices is going up tremendously over the next few years. What do hackers do with the bots? Hackers do things like breaking through a system through a **malware** which takes control of webcams, video recorders, and other consumer devices to cause widespread Internet outages. Botnets are also found as a use for committing **click fraud**. Click fraud is a systematic plan to fool advertisers into believing that in huge amount people are clicking on their advertisement. There is a collection of ways to commit click fraud, but the easiest one for the striker is to embed a advertisement of the company in a Web page he owns and then he instructs all the computers which constitute his botnet army to repeatedly visit the Web page and click on the advertisement as Google ads pay a site owner according to the number of people who click on them. Similarly, botnets can also be found of use **to evade spam filters**, which work partly by being cognizant of which systems are sending millions of e-mails. Striker can speed up password guessing to smash into online accounts, mine bitcoins, and do anything else that requires a large network of computers. This is why botnets are big businesses. Cyber-terrorist rent time on them. Political groups use them to tongue-tie the websites they don't like and such attacks will certainly be a gambit in any forthcoming cyberwar.

Mobile botnets are used by a hacker to get control on your smartphone. Infected phones can take pictures, steal user data, delete files, record video and audio, open webpages, send text messages, launch denial of service attacks and preform web injections, if supported. A Mobile botnet is very real and an epic threat commonly hidden in unsuspecting apps found in different app stores. Many browsers also share all your phone data without any user permission with other servers even without encrypting it. It

steals your personal information that can be used to damage reputations or lead to significant financial losses. It's no secret that cyber-security experts have been raising red flags regarding the potential vulnerability of the Internet of Things. But the importance of the topic can only be understood by examples.

On 21 October of 2016 world witnessed a cyber-attack which brought down America's internet. It was accomplished by the botnet tagged Mirai. It encompassed of rated one lack unsecured IoT devices which take hold of an innate internet infrastructure provider DYN, a company that administers much of the internet's domain name system (DNS) infrastructure. As a result, many high-profile and high-traffic websites, including Netflix, the Guardian, Reddit, CNN, Spotify, Github and Twitter, disappeared from the Internet transitorily. Mirai was made up of IoT devices such as DVR players and digital cameras. Merai was much monstrous than normal DDoS attacks because it was done from 100,000 affixed devices making it impossible to trace the head of these bots.

On 12 May 2017 also world encountered an attack which created history. It was the WannaCry Ransomware attack caused by the Wannacry worm which infected computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin currency. It infected around 230,000 computers in over 150 countries. A security researcher, Marcus Hutchins, from England breaks into news and become famous in the cyber security world as he discovered an effective kill switch for this virus. After that Russian Banks, websites of Rio Olympics, Wordpress blog, Clinton and Donald Trump campaign sites also suffered DDoS attack by IoT devices.

Twitter's Charlie Miller had showcased that he was able to take over a Jeep wirelessly by using a laptop with an internet connection miles from the vehicle to grab hold of it. He was able to cut the brakes and transmission at the flick of a switch. It raised weighty questions on car companies how they planned to handle such software flaws. The hack could be very well executed remotely, but it could only be fixed with physical access to the car. In a world where any minute your Google map can be hacked to misdirect you, driverless cars and their security is a matter of great concern as a car without a driver can be taken to any favorite destination of hacker very easily.

6. Prevention Systems

The IoT achievability is boundless, and so is the quantity of devices that it could manifest. In spite of the potentials of IoT, there are good deals of risks that must be contended with. Any of the devices that can be affixed to Internet has a lodge OS installed in its firmware and they are often not prototyped with security as a central consideration so, vulnerabilities exist in virtually all of them. Well, at this moment in time you know that your dependable automated home devices could be transformed into a malicious army of bots. It's perilous for mankind to become aware of the solutions that can intuit, understand and protect infrastructures from the monstrous attack surfaces created by IOT. Listed below are some such measures:

A: Be aware of what's on your network: Be mindful of your sharp-witted devices and also ferret out their security positions and don't connect with and download from unknown sources and use a secure connection.

B: Secure all devices: Modernize all the firmware on your system. Through Microsoft SCCM, you can avail an application such as 1E's Nomad to deal out enterprise approved software safely and patches manoeuvring a peer to peer approach across geographies to thousands of employees. It would also help to bring forth a unique recognition key to each gadget which communicates to your IoT hub to ensure authentication. Manufacturer can be contacted for providing a security certificate for your device.

C: Be conscious of cloud security: Clamp your data in carapace of security as it moves to and from the cloud, use encryption and honeypots to safeguard your data.

D: Start off penetration tests: It is one of the pre-eminent ways that determine whether your gadgets and networks can fend off a possible attack. To simulate a scenario and assess the outcome, routinely conduct penetration tests.

E: Insist on data encryption: Cryptography can be used to encrypt the data. Store your important data in encrypted form.

F: Protect your network from strikers: IT policies and the technology needed to nullify any possible attack on your network needs to be strengthen and also ensure that web interface is not susceptible to XSS, SQLi or CSRF and that the credentials are not wide open without any protection in internal or external network traffic.

G: Erect firewalls: CCTV cameras and business systems need to be secured by firewalls at all times.

H: Disable Plug and Play: Strong attack can also be thwart by turning off the universal plug and play feature on your routers and smart devices that are connected to the network.

I: One password for one device: Do not use the same password for all the devices to avoid any disguised effect on your network and change them over a period of time. Password recovery mechanisms should be powerfully built and should not make available to an attacker with information indicating a valid account. Ensure that weak passwords are not allowed and system should lockout after

3-5 failed login attempts.

J: Use 'guest' network to protect 'home' network: Create a guest network first and if you simply use devices with known vulnerabilities connect them to that network. That way the guest network would remain quarantined and detached from the home network even if they fall prey to an attack.

K: Vulnerabilities in the network services: They can be administer by making certain that only necessary ports are within easy reach and that the services are not vulnerable to buffer overflow and fuzzing attacks. Check that the services are not vulnerable to DoS attacks which can exert influence on the device itself or other devices on the local network or other networks.

L: Privacy related Issue: By the assemblage of personal data without any bona fide protection, privacy concerns are generated. Privacy concerns are plain sailing to track down by simply inspecting the data that is being accumulated as the user sets up and activates the device.

7. Conclusion

No matter how fascinating is the implementation of IoT still we can on no occasion avoid the dangerous side of the coin which it shows up when it comes to misuse. After each and every layer of security also when it comes to computing we are always hackable, the only difference will come in the time it will take for a hacker to break through a system. So, think of the internet as a public place. Don't leave your details lying around. Use strong passwords, two factor authentication, anti- malware and anti-virus for your devices. Keep your software updated. Switch off all the internet connectivity when device not in use. Avoid opening unknown links from your mails. For enterprises the message of safety is pretty simple that identify your critical information assets and isolate/protect those. Traditional security controls here are still effective and always know that you will get breached! Ensure you have a way to detect this and respond on a **24x7** basis.Taking these precautions you can keep your device out from the botnet skin.

These things scare and excite us both at the same time. But if you are from information technology stream, like me, then don't hate the hacker, hate the code.

References

[1]. McKinsay Global Institute, "Unlocking the Potential of the Internet of Things", June 2015, Source: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

[2]. Anna-senpai, Mirai Source Code on GitHub, September 2016, Source: https://github.com/jgamblin/Mirai-Source-Code

[3]. Level 3 Threat Research Labs, "Attack of Things!", August 2016, Source: http://blog.level3.com/security/attack-of-things/

[4]. Infodox, "Hydra IRC bot, the 25 minute overview of the kit", 2011, Source: http://insecurety.net/?p=90

[5]. "Verisign Distributed Denial of Service Report Volume 3, Issue 2 - 2nd Quarter 2016," in Verisign. Source: https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf.

[6]. Akamai, "State of the Internet Security Q3 2016", 2016. Source: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3

[7]. C. Herberger, "As Cyber Security Programs Lose Their Moorings to Ransom-DoS: Radware Introduces the Ultimate Guide to Cyber Ransom", 2016. Source: https://blog.radware.com/security/2016/09/radware-ultimate-cyber-ransom-guide/.

[8]. M. Mimoso, C. Brook, and T. Spring, "New IoT Botnet Malware borrows from Mirai," Threatpost, 2016. Source: https://threatpost.com/new-iot-botnet-malware-borrows-from- mirai/121705/.

[9]. Uzair Amir, "Thousands of CCTV Devices Found DDoSing Small-Business Websites", June 2016, http://www.securityweek.com/thousands-cctv-devices-abused-ddos-attacks

[10]. B. Krebs, "Did the Mirai Botnet really take Liberia Offline?," in KrebsonSecurity, 2016. Source: https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/