The Future and Inside Risks of the Internet of Things

Manisha Choudhary
Department of Management
Vivekananda Global University, Jaipur
Email ID: choudhary.manisha@vgu.ac.in

ABSTRACT: ***The Internet of Things (IoT) has the ability to cover and incorporate a broad variety of connected devices, including home appliances and services, wearable's, residences and corporate buildings, manufacturing processes, medical devices, law enforcement devices, military equipment, and other scarcely conceivable connected apps. "Things" are simply those computerized and networked devices which become part of the IoT in the present context. Some of these items would be directly accessible through the Internet, while others are expected to be concealed behind firewalls and address-translating routers on local networks. There are already several IoT-recognizably linked threats. Some of the threats are old and well known, yet amplified by the IoT's enormous scale; projections indicate tens of billions of items over the next several years. Other hazards may be new, arising from the nature of how these items are designed, what they are used for, how they are implemented and handled (or not managed), and how growth can be influenced by market forces.***

KEYWORDS: ***Cyber Physical Attacks, Distributed Denial-Of-Service (DDoS), Digital Video Recorders (DVRs), Internet of Things (IOT).***

INTRODUCTION

We outline some of these risks in this column and what will need to happen if the IoT is to achieve the benefits it envisages, with a fair degree of trustworthiness. Our message is intended for computer professionals as a wake-up call, but is also applicable as a user to everyone involved [1]. In the IoT, protection and privacy are also highly important, since the possible effects of successful attacks may directly or indirectly affect human lives and safety, and cause death and destruction. Violations of privacy that allow criminals to exploit information about potential victims may also constitute security threats [2].

The ubiquity of vulnerabilities in the current still-primitive Internet of Things has been illustrated by a recent distributed denial-of-service (DDoS) assault. A number of gadgets were hacked and used as unwitting botnet zombies, including closed-circuit TV cameras, cable set-top boxes, and digital video recorders (DVRs). Malware that looks for vulnerable victims, and whose source code has been freely distributed, was used in this significant case [3]. This attack seriously interfered with user access to major services including Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix by targeting the DNS services offered by Dyn. It revealed the tip of only one of several dangerous icebergs in one fell swoop. Although hundreds of thousands of devices had been infected by earlier DDoS attacks using Mirai, this attack seemed to include tens of millions of compromised devices, according to a statement from Dyn. The attack demonstrates some of the risks associated with having very large numbers of inadequately protected Internet-related items, particularly things that are easy enough to be vulnerable to compromise, but capable enough to be part of a distributed attack that floods the websites of the victims with seemingly legitimate requests. Notice that owners or users of compromised devices often do not know that they are using their devices to target other systems [4].

Vulnerabilities

Obviously, many of these devices that unintentionally contributed to that DDoS attack were not necessarily behind some kind of firewall, or else were easily exploited by poor default firewall configurations. In addition, some of the Mirai-infected items were themselves routers for small offices or home offices. Although Mirai directly abused hardcoded passwords that users could not disable for Telnet/SSH services, it is normally reckless to place all the blame on any one weak link when almost all is a possible weak link. Nearly any computer-related device today is likely to be hacked or otherwise easily misused. In depth and width, we have weakness, not power in depth. To make the IoT viable, many issues would also need to be solved. We take some of those issues into account, and some potential remediation. Ultimately, we need an overall system perspective that discusses the possible software vulnerabilities, the supposed protection of the firewall, network links, cloud services (some not even exposed to users), and the Internet itself, as well as all its users and potential malfunctions. The IoT is not an entity per se; it includes and ultimately relies on all of these entities [5].

This recent DDoS botnet episode, we suggest, is merely a harbinger of future events. In the future, IoT risks would be widespread, including the possible breach of trustworthiness criteria. These specifications must address network-wide issues such as human security, safety, efficiency, robustness, durability, functional interoperability, seamless ease of installation and usage, rapid automated remediation of serious defects, privacy, human well-being, and much more, both personal and institutional [6].

Some Illustrative IoT Risks

Denial-of-service attacks are disruptive, but the ability to remotely subvert stuff for arbitrary exploitation must be deemed extremely dangerous. Here are only a few examples of application areas where inherent risks are caused by the use of IoT devices:

1. Things: patient monitors, body scanners, pacemakers, defibrillators, infusion pumps, main and auxiliary power, lighting, air conditioning, and much more: hospitals and healthcare facilities prefer to use devices that are already remotely controlled or available.
2. IoT devices are used as sensors and actuators for automation and remote monitoring and control in critical infrastructure industries, such as electric power, oil, natural gas, manufacturing and transportation. The controls themselves may be available on the Internet.
3. Self-driving and automation-assisted interconnected cars need to be clearly seen as stuff, especially in the future of automated highways. Just a few of the threats are demonstrated by recent demonstrations of the capacity to remotely take over vital vehicle controls.

IoT systems can be more closely aligned with the physical world, unlike general-purpose computers. While there have been relatively few instances so far where physical damage has been purposely caused by computer compromise, this is likely to be a possibility of serious IoT concern [7]. Cyber physical attacks have exploited weaknesses that are characteristics rather than defects, from the known instances of programmes in the 1960s that could exercise disc weapons to cause drives to self-destruct, to the 2007-2010 Stuxnet attack that appeared to be intended to harm nuclear enrichment centrifuges (and allegedly succeeded). Most things have batteries, in addition to the things that power switches, valves, and engines, suggesting the possible ability to remotely cause those devices to overheat enough to cause a fire or explosion. If malicious attackers remotely take over cars or medical equipment, individuals may be injured or killed by anyone clicking from anywhere on the Internet. By causing chemical spills, disrupting energy systems, or misrouting vehicles, sensor manipulation or introducing misinformation may indirectly trigger other health hazards. Therefore, for all kinds of things, human protection must be a basic issue [8].

Confronting the Risks

Next, we will try to outline some measures that might be ideal. We have a significant need to understand risks in the sense of overall processes, as has been stated in previous Inside Risks columns. The Internet of Things needs a much deeper concern for the trustworthiness of the total system, of which the security of Things is only one aspect, particularly because in computer systems and networks there is essentially no real security at present. The problems of assuring trustworthiness are obviously made even more complicated by this fact. Here we mention only a few of the steps for developers, administrators, and users that may be helpful. We specifically warn, however, that this summary is just a necessary and ultimately incomplete beginning. It may not be surprising that what is required is more or less consistent with, including most recently, the series of studies from the National Academies' Computer Science and Technology Board over the past few decades. In addition, essential engineering aspects are discussed by NIST's Special Publication 800-160, Computer Security Resource. In the IoT context, we also need to emphasize several subjects that have been addressed more widely in the Inside Risks series and that are highly important here [9].

Some Specific Efforts

It is highly important to study a few kinds of stuff, such as designing research and development prototypes, to try to ensure that at least all acceptable risks have been addressed. To pave the way for how this could be achieved in the future, we would learn from a few very good cases. For anyone else operating in the IoT marketplace, the combination of device engineering, hardware and software engineering and careful application development, maybe with some systematic analysis to provide better assurance, would be extremely useful. Thus, for other developers, a few well-designed, well-developed, and trustworthy systems that are well recorded will provide wonderful examples. A move in that direction is the recorded example of a principled safety concept for a fictitious wearable fitness monitoring device developed under the auspices of the IEEE Cyber-security Initiative by the IEEE Center for Secure Design. Providing developers with the resources and expertise to create protection, privacy, reliability, and other aspects of trustworthiness into the systems they construct will also be very critical. This is especially important for IoT systems developers who may have far less experience in security than conventional software developers. We have recognized this need and are active in several efforts, including the new IEEE Cyber-security Development Conference and SRI International's strategic independent R&D initiative on IoT security and privacy, to resolve the situation [10].

CONCLUSION

The issues and potential risks associated with the emerging Internet of Things have been identified. Whether the IoT and its stuff will burgeon (grow and flourish as the way of the future) or sturgeon (sometimes, if not captured, survive competitively for up to two decades) or be more like female salmon remains to be seen (with very short lives once they spawn). We need a lot more than a surgeon to repair problems, in any case (and Things). Incremental reform (indeed, it has been unsuccessful for so many years) is not likely to work, and some form of drastic change might be required.

T Unless proactive attention is paid to determine the items can be wisely introduced realistically, and which may be simply too dangerous, the future could be rather murky. We must then ensure that these useful items can be incorporated into the requisite overall trustworthiness of the system (which we do not yet have). Therefore, we need to urge the IoT to be fully functional, and then move on to ensure that it happens with sufficient faith.

REFERENCES

[1] G. Gan, Z. Lu, and J. Jiang, "Internet of things security analysis," in *2011 International Conference on Internet Technology and Applications, iTAP 2011 - Proceedings*, 2011, doi: 10.1109/ITAP.2011.6006307.

[2] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the Internet of Things," *Futur. Gener. Comput. Syst.*, 2017, doi: 10.1016/j.future.2017.04.045.

[3] P. Radanliev *et al.*, "Future developments in cyber risk assessment for the internet of things," *Comput. Ind.*, 2018, doi: 10.1016/j.compind.2018.08.002.

[4] H. Aldowah, S. Ul Rehman, S. Ghazal, and I. Naufal Umar, "Internet of Things in Higher Education: A Study on Future Learning," in *Journal of Physics: Conference Series*, 2017, doi: 10.1088/1742-6596/892/1/012017.

[5] J. Green, "The Internet of Things Reference Model," *Internet of Things World Forum*, 2014.

[6] H. S. Birkel and E. Hartmann, "Internet of Things – the future of managing supply chain risks," *Supply Chain Manag.*, 2020, doi: 10.1108/SCM-09-2019-0356.

[7] R. Kirk, "Cars of the future: The Internet of Things in the automotive industry," *Netw. Secur.*, 2015, doi: 10.1016/S1353-4858(15)30081-7.

[8] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things*, 2020, doi: 10.1016/j.iot.2019.100081.

[9] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in internet of things: A survey," in *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*, 2017, doi: 10.1109/ISNCC.2017.8072001.

[10] D. Bastos, M. Shackleton, and F. El-Moussa, "Internet of things: A survey of technologies and security risks in smart home and city environments," in *IET Conference Publications*, 2018, doi: 10.1049/cp.2018.0030.