Information & Security: An International Journal

Dobrin Mahlyanov, v.39:2, 2018, 175-182 https://doi.org/10.11610/isij.3915

INTERNET OF THINGS – A NEW ATTACK VECTOR FOR HYBRID THREATS

Dobrin MAHLYANOV

Abstract: The means of conducting hybrid warfare are rapidly changing. IoT is a recent sphere of activity, opening new opportunities for hybrid influence. Consisting of three main building blocks, IoT inherits all security problem specific to each one of them and introduces some new ones. This article describes in brief the main issues concerning security in IoT and ways of using it for creating hybrid threats. All of the described problems can be used for escalation in different areas. The article presents also a simple definition of what is a (relatively) secure IoT system and an original concept for reducing vulnerabilities in the IoT environment.

Keywords: hybrid threats, Internet of Things, IoT, security in IoT, attacks against IoT.

Hybrid Threats

The term 'hybrid threat' is a metaphor that brings complexities related to a changing global environment. It is often used interchangeably with references to hybrid war, to capture the interconnected nature of challenges, multiplicity of actors involved and diversity of conventional and unconventional means used. Taking into account different levels of intensity of a threat and intentionality of actors involved, it is possible to distinguish between hybrid threat, hybrid conflict and hybrid war:[11]

Hybrid threat is a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat.

Hybrid conflict is a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.

Hybrid war is a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic).

IoT and Its Place in a Hybrid Threats Environment

Conventional military and security threats nowadays are supplemented by the use of new technologies. The advent of "cyber threat" serves as an example for the use of new technologies within the scope of hybrid threats. Cyber threat refers to a possibility for sustained computer based cyberattack by a state (or non-state actor) against the information technology infrastructure of a target state. Usually, one of the requirements for a successful cyberattack is to have control over a significant computing power. And one of the most proliferating technologies, concerning computing power, is the Internet of Things (IoT).[5] The Internet of Things revolves around increased machine-to-machine communication; it is built on cloud computing and networks of data-gathering sensors; it is in a mobile, virtual, and instantaneous connection, and is developed to make everything in people's lives, from streetlights to seaports, "smart."

Currently, one of the best definitions is that IoT is the following:

> The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[3]

The basic building blocks of the IoT can be divided into three main components:[4]

- *"Things"* – these are all elements that are responsible for data collection and dispatch. Also "things" must be able to accept feedback, i.e. to create influence over the environment;
- *Communication network* – this is the environment that allows "things" to be interconnected. In general, it is the online environment, but individual cases can consider all possible connections – Radio-Frequency Identification (RFID), Wireless Fidelity (Wi-Fi), Bluetooth, optical codes like Quick Response Code (QR code), Internet Protocol version 6 over Low Power Wireless Personal Area Networks (6LowPAN), etc.;[8]
- *Computing Systems* – they have the ability to process incoming data from the "things," from the communication network, and send the processed information.

Security Issues for IoT

With the increased functionality of the new smart mobile devices, end users now have the ability to monitor and control their home systems, to operate with their cars to monitor their health and vitality status. Combination of user data and its systems

data is stored, processed and distributed for reading without human intervention.[2] This convenience has its price. In the most general case the price is security. Manufacturers of components for IoT are focused on performance and functionality, often compromising security. The increased number of interconnected devices and the emergence of new infrastructure, which could be critical, establish new, unforeseen risks. These could be new forms of blackmail (such as ransomware for smart homes or cars), identity theft, physical injury or even death, new types of botnets, and more.[7] In the world of technologies that are "always on" and insufficient awareness of the risks of end users, the question of carrying out a successful attack against an element of IoT should not be 'if,' but 'how' and 'when.'

Nevertheless, some of the techniques used by attackers may be predicted and some measures for their protection can be developed. Below are listed some key challenges to security issues in IoT related to protection from attack:

- Replacement of identity element of IoT (*IoT spoofing*) – in this case, an attacker aims to communicate on behalf of a legitimate element of IoT, using its identity to achieve their objectives;
- *Eavesdropping* – each element of IoT is in constant communication with other elements. Most often they communicate by a public communication infrastructure, where an attacker could gain access to the information exchanged;
- *Data forging* – while eavesdropping is a passive way of attacking, counterfeiting data is an active way. By using it, already intercepted data can be replaced, which will lead to a change of decision making based on the data. Usually victims of this type of attack are sensors for gathering primary data;
- *Access control* – almost every element of IoT is designed on the principle that it should be able to be controlled remotely. In the security area, this can make meaningless most of physical security measures, which are put in place to minimize any security holes (e.g., implementation of physical security in the perimeter around communication channels with high levels of electromagnetic radiation);
- *Collection of personal data* – data elements of IoT could lead to the disclosure of personal information for the end user, such as health status, habits and life patterns, location, financial information, etc.;
- *Use of malicious code* – each component of the IoT can be considered a device, created to process and transmit information; therefore, from an attacker's point of view, they represent potential targets for compromise. IoT elements use different software, hence each one of them could be infected by certain malware in order to be manipulated and controlled. On the other

hand, the possibility of using elements of the IoT as part of botnets should not be underestimated. Those elements, which could communicate through standard internet protocols, would become the perfect bots to perform distributed denial of service attacks;

- *Accessibility and denial of service* – in its classic form, the elements of the IoT, even when connected to different networks, appear to be a tough target for attacks with denial of service, especially on a large scale. Their integration into a single system, especially if it is IP-based, could increase the possibility of successful attacks against them. In this case it is correct to say that the attacks would be directed to communication environment and computing systems, rather than directly to multiple sensors.

The above-described types of attacks are the ones that are likely to be used against IoT systems. As experience from practice has shown, the most effective protection is the prevention and, therefore, it is advisable to take precautions to minimize the risk in the phase of implementation of system. The very nature of the IoT, however, creates some new challenges:

- *Scalability* – each defined system in IoT is supposed to be spread over a considerably large area and will include a significant number of IoT elements, even if at the beginning that may not be the case. The need for proper selection of scalable solution for unequivocal authentication for these elements is an issue. When using a small number of elements, such solution is not a problem, unlike the situation using a large number of heterogeneous devices;
- *Mobility* – most of the elements of the IoT have no permanent location (phones, cars, wearable elements, etc.). This leads to a constant need for a reliable authentication and secure communication in a changing environment (communication channels, environmental factors, human factors, etc.);
- *Deployment* – when carried out in practice, the physical deployment of elements of the IoT may pose a threat as it is possible that some of them are set in places without a possibility of implementing physical security measures. This can lead to an increased risk of physical unauthorized access. In this case, it is necessary to find a way to prevent unauthorized access by detecting any attempt to tamper with the data from such isolated elements of the IoT;
- *Legacy systems* – when an IoT system is to be included in a system, implemented in an earlier period, this legacy system may offer very little security level due to the use of independent communication channels. This is a sig-

nificant problem in cases where, for various reasons, the old systems cannot be replaced or upgraded in order to support the selected security solutions;

- *Limited resources* – in mass production of components for IoT, manufacturers usually compromise with resources which are limited. This would lead to difficulties of ensuring the desired level of security when applying some standard solutions;
- *Heterogeneity* – achieving secure communication from end to end is a challenge in terms of non-compliance of the technical parameters of the IoT elements (computing power, memory, communication bandwidth, delay, etc.) and the used Protocol (IP and non-IP);
- *Interoperability*, i.e. achieving secure transmission of information between two elements using different types of communication protocols. With a large diversity in the system, more resources are necessary to achieve interoperability between its elements;
- Loading initially necessary information (*Bootstrapping*) – implementation of initial resources, which are necessary to carry out reliable secure communication (cryptographic keys, algorithms, etc.) for a small number of elements of the IoT, may not be a big problem but with the increasing numbers this will become a challenge.

An Approach to Solving the Security Problem in IoT

Due to the enormous growth in size and complexity of the IoT systems, protection of the elements and networks through which they are linked is a complex problem. The solution should begin with the protection of the individual element, then to secure the networks to which it is included and, finally, to reach the end user.[1]

A common practice among manufacturers, creating elements of the IoT, is to consider that security should be the user's concern. However, there are developments that allow an increase in the level of protection still on the production line. Such an example would be a built-in module for protection against malicious code. While the minimum level of protection, provided by the manufacturer, could only be changed with a change of the legal framework, users are not limited in their choice of security measures. For each device they want to use, they can change security settings on the basis of instructions and lessons learned to achieve their required balance between security and convenience.

Networks used for communication should also be protected. A good starting point for creating network security in IoT is setting restriction limits.[6] IoT systems should develop and implement policies and procedures, including restrictions that refer to usage of devices. When there is a failure to comply with restrictions, corresponding de-

vices simply should not be included in the network. A good example of practical implementation is to set a limit of the number of unsuccessful attempts to authenticate, or prohibiting the inclusion of devices unable to transmit information in an encrypted form.

Many experts believe that the weakest link in the security chain is the human, yet organizations often do not invest sufficiently in training people. Many people, even those who are involved in electronic security, state that they do not have control over the way their personal information is collected and processed. In the IoT environment, end users should be aware of the risks and responsibilities for inclusion in systems of IoT. To limit the risk, consumers and organizations should work together.[10] While measures to limit personal data, collected by organizations, focus on controlling which part of the data should not be exposed on the Internet without the knowledge of the person, the joint limiting, involving the participation of an organization and the end user, focuses on determining which devices need personal data to operate effectively in the interests of the consumer. It is a must that all end-users should be provided with knowledge of proper operation of the devices, especially when these devices are interconnected as in the IoT.

Protected IoT Systems

Should an IoT system be secure, it must be able to provide users with certain services related to security:

- *Confidentiality* ensures that the information, whether stored, transmitted or processed, is only available for the intended user;
- *Integrity* ensures that the resulting information is not modified in an unauthorized manner;
- *Authentication* is the ability to verify the legitimacy of the inclusion of each element of IoT, based on its unique identifier;
- *Authorization* is the ability to ensure that the authenticated element is authorized to perform only certain tasks and/or have access to certain resources;
- *Privacy* ensures that any information related to the end user, whether raw or passed through any stage of processing, cannot be obtained by third parties without explicit consent and will only be used for the purposes intended.

There is specificity only for IoT domain – the missing quality “Accessibility” from the information triad. The reason is that while information accessibility is a constant element of security, in IoT accessibility is something more than that. It is an element of existence.

Considering the security IoT as a set of services is one of the methods for determining the successful level of protection for a given system. Each service can acquire a certain multiplier and the overall level of protection is calculated as a sum of multiplied values of different services.[9] This model is not specific, because in different systems, different services may have different priorities. While for a weather station service confidentiality can be neglected at the expense of integrity (correct data from the sensors have priority), in the military field, IoT system confidentiality will be an objective of paramount importance.

Conclusion

IoT is a world in which every object is implanted with one or more small computers or sensors capable of transmitting data streams in a common environment. Life in this world can bring many conveniences, but the medal always has two sides. The opposite side here is security. IoT always compromises between convenience and security. The discussed problems of security show that this choice should always be done in terms of awareness of potential threats and inconveniences arising from them. Providing a predetermined level of security should be a priority in the construction of each IoT system.

References

1. Adrian McEwen and Hakim Cassimally, *Designing the Internet of Things*, (Chichester, United Kingdom: John Wiley and Sons, 2014).
2. Christian Légaré, "Designing the Internet of Things: Part 1 — IoT Devices and Local Networks," *EDN Network*, February 10, 2014, http://www.edn.com/design/wireless-networking/4428131/Designing-IoT-Part-1-IoT-Devices-and-Local-Networks/.
3. Cuno Pfister, *Getting Started with the Internet of Things* (Sebastopol, CA: O'Reilly Media, 2011).
4. Francis da Costa and Byron Henderson, *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything* (New York: Apress, 2014).
5. Marcelo Hector Gonzalez and Jana Djurica, "Internet of Things Offers Great Opportunities and Much Risk," *ISACA Journal* 2 (2015), https://www.isaca.org/Journal/archives/2015/Volume-2/Documents/Internet-of-Things-Offers-Great-Opportunities-and-Much-Risk_joa_Eng_0315.pdf, accessed October 18, 2018.
6. Matthew Monte, *Network Attacks and Exploitation: A Framework* (Chichester, United Kingdom: John Wiley and Sons, 2015).
7. Nitesh Dhanjani, *Abusing the Internet of Things: Blackouts, Freakouts and Stakeouts* (Sebastopol, CA: O'Reilly Media, 2015).

8. Olivier Hersent, David Boswarthick, and Omar Elloumi, *The Internet of Things - Key Applications and Protocols* (Chichester, United Kingdom: John Wiley and Sons, 2012).
9. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu, "Security of the Internet of Things: Perspectives and Challenges," *Wireless Networks* 20, no. 8 (November 2014): 2481–2501.
10. Robert Martin, "The Internet of Things (IoT) –Removing the Human Element," *Infosec Writers*, 28 December, 2015, https://infosecwriters.com/Papers/RMartin_IoT.pdf, accessed October 18, 2018.
11. Sascha-Dominik Bachmann and Håkan Gunneriusson, "Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Peace and Security," *The Journal of Terrorism and Security Analysis* 9, no. 1 (Spring 2014): 26-36, https://doi.org/10.2139/ssrn.2252595.

About the Author

Major Dobrin MAHLYANOV holds a bachelor degree in Computer Systems and a master degree in Psychology and Military Science. For six years he has worked as cyber security expert in the Ministry of Defence of Bulgaria. Currently, he pursues a PhD degree with research on "Internet of Military Things."