Towards Threat Modelling for Internet of Things(IOT) Environments

***Abstract*:** The Internet of Things(IOT) by its very definition refers to a network of interconnected physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and the deliberate and persistent connectivity with which these objects relate and exchange data. In this paper we propose the basic tenets of how we could go about modelling threats within these IOT devices as a part of a system administrator controlled environment. We devise a two layered system for treating with the recognition of threats in these devices, Namely IOT in a (i) physical environment, and IOT within a (ii) cloud or Fog based cyber physical environment. The identification of security threats between these two types of IOT environments have different concerns and this paper's contribution seeks to make the readership aware of these concerns as a conceptual evaluation.

***Keywords*:** IOT, Cloud, Fog, threat, modelling, cyber-physical, security

I. Introduction

By definition threat modelling for intelligence purposes speaks to the organized, and analysed review of information that can sensitize the system administrator with respect of potential attacks. To an organization the purpose of modelling threat intelligence is significant with respect of informing the organization with respect of the risks to the environment. The concerns become pervasive as there is wide scale adoption of IOT devices within our social and business environments. This paper posits the need for a scheme that maps how to treat threat modelling for intelligence purposes within IOT devices using Cisco's six pillars for same [1]. According to [1], the need to assess where an advanced persistent threat would exist is tied to concerns including (i) Network Connectivity - : where there is in built routing, switching, over both the wired and wireless appliances of various form factors.(ii) There is issue as to whether or not the IOT device is physical or within a cyber physical environment for which some possible attack needs to be detected and the need for increased protection for both the physical and digital assets within such environments(iii)Then there is data analytics for these IOT devices for which. As a matter of context we would need to assess whether or not the IOT system for which we need to model the advance persistent threats(APT) is built with an infrastructure that allows for data collection from central or disparate sources that can be used to inform intelligent analysis about the APT.(iv) The ease of use with which to visualize APT collected and analysed data as apart of a managed automation plane. This will allow for the system administrative team to be able to support enhanced security controls for containerized finctions for supporting the IOT system. (V) Application integration across a common interface using APIs will need to pay attention to various interactive third party IOT products for which there would be a need to understand where the possible threat sources may avail themselves. (VI) The consideration of many IOT devices are now Fog based devices where, where the Fog allows for distributed data to be collected locally from these devices by leveraging cloud based services.

It is well understood that for the physical environment, a device contains a basic IP and MAC address. However, when we consider a cyber-physical environment like a data cloud or Fog based service, there are levels of meta abstractions away from the physical device. There is consideration for the Fog based device, that the IOT resource will be accessed via a virtual machine emulator, and where these virtual machines are mapped by logical addresses in paged memory. These logical machines are indexed by logical IP addresses referred to as CPU_WORLDID addresses, where these addresses across a distributed network may be connected across several storage area networks globally, and for which the corresponding IP addresses and MAC addresses may be situated geographically on physical or other virtualized storage area networks which may be outside the scope of the system administrator's control.

Where the IOT physical devices for which collection of data relating to cyber-attacks could already be in a distributed network, for which security access and control has its own nuances of concerns, the problem becomes exacerbated when one seeks to carry out threat detection analysis for the logical cloud based networks.

.

II. Conceptual Mapping of IOT Threats

To appropriately track the threats, the next steps for designing a suitable framework for determining where an IOT threat source may occur is to develop a Threat matrix based on Cisco's six pillar [1] approach explained earlier. Further we will need to have an IOT Threat layered approach where the IOT device for which we seek to map an APT has to be separated into (i) Physical layered or embedded IOT layered device (ii) IOT Fog layered base device

Once the above mapping is established threat modelling for intelligence purposes will require at first data collection into one or both IOT threat layers given one or more of the six purposes outlined based on the Cisco pillared framework [1].

Our next step is to carry out a full case study that evaluates this blueprint, to show as a proof of concept the strengths and weaknesses of our approach

iII. Conclusion

This paper proposed the basic definitions of how we could go about modelling threats within these IOT environments. We proposed a two layered system for treating with the recognition of threats in these devices, Namely IOT in a physical environment, and IOT within a cloud or Fog based environment. The identification of threats between these two types of IOT environments have different concerns and this paper's contribution provides the conceptual matrix for parameterizing these concerns.

References

[1] K. Briodogah, "Cisco Six Pillars" July 1, 2015. Retrieved from http://www.iotevolutionworld.com/iot/articles/405981-cisco-unveils-six-pillar-iot-system-15-new.htm.