Improving Security of IoT Devices on SDN

Jonathan Ramirez, Computer/Electrical Engineering

Mentor: Dr. Amir Esmailpour

The rapid advancements of Internet of Things (IoT) technology have caused an exponential growth in connectivity of different devices to the internet. Securing such complex, different networks and diverse access protocols is a real security risk. Software Defined Network (SDN) is an umbrella term encompassing several kinds of network technologies aimed at making networks as agile and flexible as the virtualized server and storage infrastructure of the modern data center. It allows network engineers and administrators to respond quickly to changing business demands.

I focused on connecting IoT on a SDN and improved it's security. Due to the complexity of the objects and networks in IoT; traditional authentication and authorization methods may not be applicable. Also, the resource constrained devices in IoT restrict the usage of complex security mechanisms. Some of the security challenges around IoT are privacy and authentication. Data sensed by various physical nodes in IoT needs to be collected and analyzed. Encryption and decryption of the data needs to be performed. The resource constrained devices like sensor nodes in IoT are incapable to perform such complex security cryptographic operations creating holes in data privacy and integrity. The traditional public-key cryptosystems cannot fit in IoT ecosystem. Authenticating and authorization through cryptographically pre-shared keys is not applicable with old means. The growing number of objects will make the key management a difficult task in IoT. Lack of a global certification authority (CA) in the IoT is the main problem that is holding us back from securing these devices. The cryptographic algorithms are normally heavy and require huge memory prints that restrict their usage in memory constrained in IoT devices. Working on a more secure method of transferring data between the connecting nodes while still maintaining a high level a security and using SDN to improve and route IoT devices in a specific way will improve security.

It is possible to authenticate, encrypt, and protect privacy. With the use of post requests on html you can have a simple encryption for sending data to a server. Adding another layer of encryption to the post request will increase security but also add weight to the overall program. Therefore, the amount of space available on the device will determine the complexity of the algorithm used to secure the device. So imbedding the certification authority onboard in eeprom would be one idea.

Acknowledgements: Mark Morton, Computer & Electrical Engineering Department

BIO:

Hello,

My name is Jonathan Ramirez I am a Computer and Electrical Engineer who was born and raised in Pennsylvania. I am a Test Engineer, currently employed at Fiber Mountain and I am developing solution to improve testing products, and researching new methods of transmitting data. I have had a passion for technology since I was very young.