Cybersecurity Concerns due to the 3D Attack Surface in the IoT Environment; IT, OT & Devices Vulnerabilities; Assessment & Mitigation for the Industrial Enterprise

Technical Report · August 2017

CITATIONS
0

READS
128

1 author:

Suresh Sundarrajan
St. Petersburg College
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Cybersecurity Concerns due to the 3D Attack Surface in the IoT Environment

By Suresh Sundarrajan, Cybersecurity & IoT Solutions Architect

Makerspace Award Winning Paper, April 2017

IoT is a new technology opportunity that has developed in the last few years.
Today, there are currently 10 billion interconnected devices and this is expected to grow to 50 billion by 2020, and that is only 3 years away. With that many devices it makes for a highly vulnerable network with billions of vulnerabilities that can be exploited by determined hackers. Today, we are using smartphones as a swiss army knife, and we are embracing smart homes, smart cars, self-driving cars, smart factories, smart hospitals, smart airports, smart cities, etc and the list is growing bigger day by day.

In evaluating security needs for enterprise IoT, I will have look at the entire technology stack which is comprised of three different areas: IT, OT and Devices. IT is typically office based computing environment; OT is operational technology and Devices is the Smart Device environment that consists of all types of connected sensors. All three have different features, functionality and applications.

Consequently, they have entirely different security features and the security has to be addressed differently for each type of technology, IT, OT and Smart Devices. Plus, to make sure we are not subjected to new vulnerabilities, we also need to address BYOD security issues which form part and parcel of this environment.

The IoT network will include not only smart devices that will be developed and installed to measure things like pressure, temperature, movement, vibration, etc but it will also include legacy systems like PLC controllers, SCADA systems, etc that have been used for decades in industrial environments.

MDM, BYOD and other technologies exist to manage systems using mobile device management and Bring your own devices. Millenials employees themselves could be an insider threat.

To address the effects of the IoT on security we have to address numerous problems and new threat vectors. Situational awareness must come first. We must develop SA. and then address mitigation. We must know what we have in the building in terms of devices and develop a policy for various systems in the environment.

IoT creates a 3D attack surface for many reasons. Previously, the the number of protocols have were 6. It has not gone up to over a over a 100. Now, the CIO is not responsible for them and the CSO does not even know they exist. In the past we had Port 80 and Port 43 which were most vulnerable. Now, we have dozens of ports and they may be used by devices and we don't even know what devices we have and where they exist!
So, the sttack surface multiplies

Some examples of attacks that we can expect include: RF attacks and Device attacks; addressing vulnerabilities of lower power and lower bandwidth requirements; addressing RF data leakage; addressing different protocols and different frequencies which could use AM and FM frequencies used to exfiltrate data from a network (for example a printer was used to extract data from a computer network by hacking the firmware, Defcon 2015).

Other forms of hacking are emerging and we need to address them for IoT. For example, cellular hacking, rogue WIFI networks can play man in the middle and send a password reset request for a bank account for example.
These were some of the examples of IoT Hacks demonstrated at Defcon, 2015 and 2016.Defcon. A rogue cell station can be built for $500 today, which would have cost $500,000 ten years ago. This can lead to Man in the middle attack using Rogue Cell stations.

Other attacks could include: Proxy Ham at Defcon which can attack the new Hybrid model of connected systems. So, we have all kinds of new threat vectors. At Defcon, Samsung premiered a Smart Fridge, and the Smart Fridge was programmed to log into the users Google Calendar. But, the Smart Fridge lacks into Google Calender without SSL certificates Then we have an example of an Armored car network which was transmitting driver coordinates via HTTP without security and encryption. We even had an example of ethiccal hackers who put a ship can be put out of service by using a $1,000 toolkit that an expert called :Somali Pirate Toolkit".

So, we have all kinds of new devices from laptops to tablets to wearables and all kinds of connected smart devices connected to legacy devices like PLCs, SCADA systems, etc. We don't even know what we are up against and we have to constantly assess, monitor and develop new security products, systems, test them and deploy them, while doing routine security risk assessments and conducting ongoing training for the staff.

Assuming I was put in charge of enhancing security for IoT platforms for an enterprise with locations nationwide, I would take this approach to achieve the mission and goals.

First, conduct a comprehensive Security Risk Assessment
Perform an inventory of all connected devices and systems
Evaluate all vulnerabilities to cyber threats such as open ports, etc
Review all policies and procedures for using computers, cellphones and smart devices
Review the connected ecosystem, secure each subsystem and test the complete system
Conduct vulnerability testing and penetration testing using smartphones and software
Develop new software and hardware to develop secure mechanisms to provide data & systems
BYOD policy needs to be reviewed, developed and implemented
Enterprises should look at IoT policy and BYOD policy separately
Build an IoT policy and BYOD policy keeping the millennials in mind vs. the baby boomers

In sum, we have to be extra vigilant in dealing with Internet of Things, being mindful that we have opened up our entire connected network to the global Internet and hackers from the US or across the

globe can hack into our systems, hold us at ransom, steal our secrets, our valuable data, credit card data, SSN numbers and any number of valuable information that can expose us to vulnerability. We have a real job ahead of us in IoT security.