VILLAGE COMPUTER

INSPIRED BY STL JOBS CLINTION PEABODY

JUNE 2018

ISSUE #6

Top 10 IoT Security Challenges

Intro By Nick Curlett, Computer Village

The IBM developerWorks Blog featured an article of the associated title,

covering areas that I am going to put in laymans terms with some definitions to help us get an understanding of the serious nature of being safe and secure.

The IoT is utlilized by leaps and bounds at an exponential rate. For evevery good there is a bad that follows so we are going to simplify the dialog and hopefully peak your curiosity.

–Computer Village

Anna M. Gerber published this article in November of 2017, using Eclipse IoT Working Group's 2017 developer survey, she summized these top 10 developer concerns.

The influx of more IoT devices create "unique challenges to address uncontrolled, complex, and often hostlite environments. Listed below are the top to challenges:

1. **SECURE CONTRAINED DEVICES**

   A. A constrained device is a small device with limited CPU, memory, and power resources, such sensors, smart objects ad devices, they depend heavily on encryption and can't do complex encryption or decyrpt it fast enough to transmit data in real time.

2. **AUTHORIZE AND AUTHENTICATE DEVICES**

   B. Influx of devices offer potential points of failure within the IoT system. The most popular device authentication system is 2 factor (2FA) example: you type in your pasword, and they send you a text with a unique number to enter.

3. **MANAGE DEVICE UPDATES**

   C. Applying updates, including security patches, to firmware or software that runs on IoT devices and gateways presents a number of challenges. For example, you need to keep track of which updates are available and apply updates consistently across distributed environments with heterogeneous (unrelated or alike) devices that communicate through a range of different networking protocols.

4. **SECURE COMMUNICATION**

   D. Once the devices themselves are secured, the next IoT security challenge is to ensure that communication across the network between devices and cloud services or apps is secure. This is done through to transport encryption of TLS (Transport Layer Security)

5. **ENSURE DATA PRIVACY AND INTEGRITY**

   E. Implementing data privacy includes redacting or anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. Data that is no longer required should be disposed of securely, and if data is stored, maintaining compliance with legal and regulatory frameworks is also an important challenge.

6. **SECURE WEB, MOBILE, AND CLOUD APPLICATIONS**

   F. Web, mobile, and cloud apps and services are used to manage, access, and process IoT devices and data, so they must also be secured as part of a multi-layered approach to IoT security.

7. **ENSURE HIGH AVAILABILITY**

G. As we come to rely more on IoT within our day-to-day lives, IoT developers must consider the availability of IoT data and the web and mobile apps that rely on that data as well as our access to the physical things managed by IoT systems. The potential for disruption as a result of connectivity outages or device failures, or arising as a result of attacks like denial of service attacks, is more than just inconvenience. In some applications, the impact of the lack of availability could mean loss of revenue, damage to equipment, or even loss of life.

H. For example, in connected cities, IoT infrastructure is responsible for essential services such as traffic control, and in healthcare, IoT devices include pacemakers and insulin pumps. To ensure high availability, IoT devices must be protected against cyber-attacks as well as physical tampering. IoT systems must include redundancy to eliminate single points of failure, and should also be designed to be resilient and fault tolerant, so that they can adapt and recover quickly when problems do arise.

8. **DETECT VULNERABILITIES AND INCIDENTS**

I. Despite best efforts, security vulnerabilities and breaches are inevitable. How do you know if your IoT system has been compromised? Strategies for detecting vulnerabilities and breaches include monitoring network communications and activity logs for anomalies, engaging in penetration testing and ethical hacking to expose vulnerabilities, and applying security intelligence and analytics to identify and notify when incidents occur.

9. **MANAGE VULNERABILITIES**

J. The complexity of IoT systems also makes it challenging to assess the repercussions of a vulnerability or the extent of a breach in order to manage its impact. Challenges include identifying which devices were affected, what data or services were accessed or compromised and which users were impacted, and then taking actions to resolve the situation.

10. **PREDICT AND PREEMPT SECURITY ISSUES**

K. A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to predict and proactively protect against potential security threats.

CONCLUSION

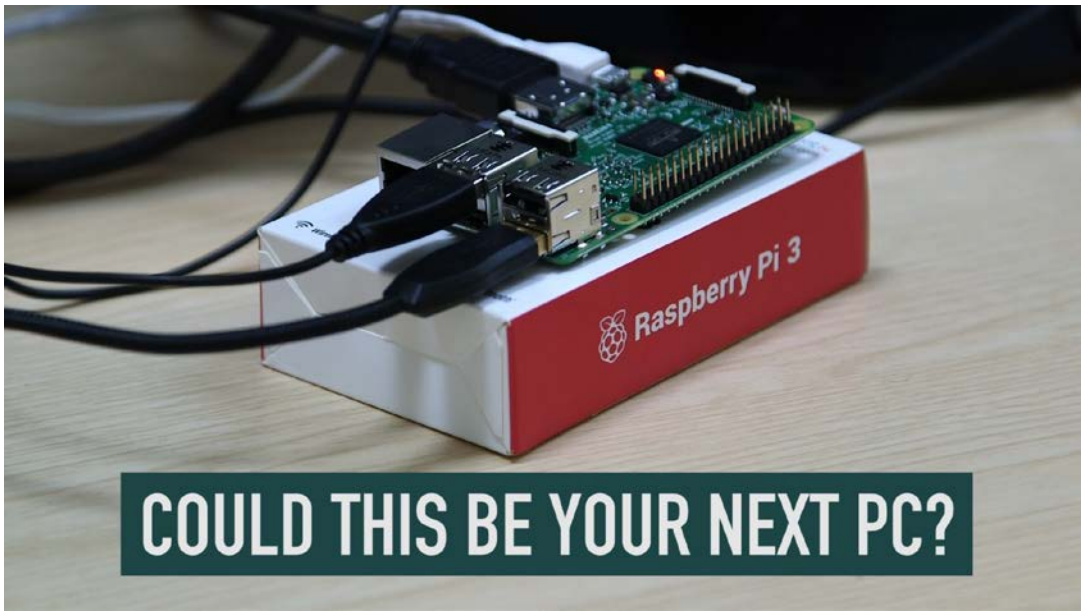
Adopting a multi-layered security-by-design approach to IoT development is essential for securely managing devices, data, and mobile and cloud-based IoT apps and services, as well as dealing with threats or issues as they arise.

by AnnaMGerber

Anna Gerber is a software engineer and maker based in Brisbane, Australia, and one of the organizers of NodeBots AU. With over 15 years of experience, Anna is currently a developer at Console Connect.

Full Article Link

https://developer.ibm.com/dwblog/2017/iot-security-challenges/



Are you interested in creating your own computer no bigger than the size of a deck of playing cards? It also has the functionality of a fully operational PC, allowing you to watch movies, play video games, access the internet and utilize various applications, multiple operating systems, and APK's. This particular model has built in WiFi and Blue Tooth. No I am not pulling your keyboard. Call Don Holt at Computer Village and inquire about joining a class. The email and telphone addresses are on the bottom page.

Computer Village
Executive Director, Don Holt

Don has been on the battle field for youth development and education for over 30 years. Retirement from Xerox only gave him more time for his passion. Don Holt is an “Unsung Hero” and advocate for youth, education and the black community.

“Don continues to stress the importance of IoT as a major component for the growth of young people associated with job stability in our community.”

VILLAGE COMPUTER

INSPIRED BY STL JOBS CLINTON PEABODY

Main Office
“Where People and Technology Come Together”
4411 N. Newstead
St. Louis, MO 63115
P: (314) 533-1900
E: cvillagestl@gmail.com

Don Holt
Executive Director
E: don.holt-cv@att.net
Home: 314-741-4854
Mobile: 314-537-0274
5404 Sun Trail Drive
Florissant MO 6313