Internet of Things Security Top Articles

Top 10 IoT security challenges

AnnaMGerber

Published on November 17, 2017 / *Updated on November 17, 2017*

6

As more and more IoT devices make their way into the world, deployed in uncontrolled, complex, and often hostile environments, securing IoT systems presents a number of unique challenges. According to Eclipse IoT Working Group's 2017 IoT developer survey, security is the top concern for IoT developers.

Follow along as I describe my top ten challenges for IoT security:

1. Secure constrained devices
2. Authorize and authenticate devices
3. Manage device updates
4. Secure communication
5. Ensure data privacy and integrity
6. Secure web, mobile, and cloud applications
7. Ensure high availability
8. Detect vulnerabilities and incidents
9. Manage vulnerabilities
10. Predict and preempt security issues

#1 – Secure constrained devices

Many IoT devices have limited amounts of storage, memory, and processing capability and they of
operate on lower power, for example, when running on batteries.

Security approaches that rely heavily on encryption are not a good fit for these constrained device
capable of performing complex encryption and decryption quickly enough to be able to transmit d

These devices are often vulnerable to side channel attacks, such as power analysis attacks, that c
engineer these algorithms. Instead, constrained devices typically only employ fast, lightweight en

IoT systems should make use of multiple layers of defense, for example, segregating devices onto
using firewalls, to compensate for these device limitations.

#2 – Authorize and authenticate devices

With so many devices offering potential points of failure within an IoT system, device authenticati
critical for securing IoT systems.

Devices must establish their identity before they can access gateways and upstream services and
many IoT devices that fall down when it comes to device authentication, for example, by using we
authentication, or using passwords unchanged from their default values.

Adopting an IoT Platform that provides security by default helps to resolve these issues, for exam
authentication (2FA) and enforcing the use of strong passwords or certificates. IoT Platforms also
authorization services used to determine which services, apps, or resources that each device has
system.

#3 – Manage device updates

Applying updates, including security patches, to firmware or software that runs on IoT devices and
number of challenges. For example, you need to keep track of which updates are available apply u
across distributed environments with heterogeneous devices that communicate through a range c
protocols.

Not all devices support over-the-air updates, or updates without downtime, so devices might need
accessed or temporarily pulled from production to apply updates. Also, updates might not be avai
particularly older devices or those devices that are no longer supported by their manufacturer.

Even when updates are available, the owners of a device might opt out of applying an update. As p
management, you need to keep track of the versions that are deployed on each device and which
for retirement after updates are no longer available.

Device manager systems often support pushing out updates automatically to devices as well as m
update process fails. They can also help to ensure that only legitimate updates are applied, for exa
digital signing.

Read more about securing IoT devices and gateways on IBM developerWorks.

#4 – Secure communication

Once the devices themselves are secured, the next IoT security challenge is to ensure that commu
network between devices and cloud services or apps is secure.

Many IoT devices don't encrypt messages before sending them over the network. However, best p
transport encryption, and to adopt standards like TLS. Using separate networks to isolate devices
establishing secure, private communication, so that data transmitted remains confidential.

Read more about securing IoT data over the network on IBM developerWorks.

#5 – Ensure data privacy and integrity

It is also important that wherever the data ends up after it has been transmitted across the netwo
processed securely. Implementing data privacy includes redacting or anonymizing sensitive data b
using data separation to decouple personally identifiable information from IoT data payloads. Data
required should be disposed of securely, and if data is stored, maintaining compliance with legal a
frameworks is also an important challenge.

Ensuring data integrity, which may involve employing checksums or digital signatures to ensure da
modified. Blockchain – as a decentralized distributed ledger for IoT data – offers a scalable and re
ensuring the integrity of IoT data.

Read more about what blockchain means for IoT in this blog post.

#6 – Secure web, mobile, and cloud applications

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

When developing IoT applications, be sure to apply secure engineering practices to avoid vulnerab
OWASP top 10 vulnerabilities. Just like devices, apps should also support secure authentication, b
themselves and the users of the applications, by providing options such as 2FA and secure passw

Read more about security best practices for IoT applications on IBM developerWorks.

#7 – Ensure high availability

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

For example, in connected cities, IoT infrastructure is responsible for essential services such as tr healthcare, IoT devices include pacemakers and insulin pumps. To ensure high availability, IoT de against cyber-attacks as well as physical tampering. IoT systems must include redundancy to elim failure, and should also be designed to be resilient and fault tolerant, so that they can adapt and r problems do arise.

#8 – Detect vulnerabilities and incidents

Despite best efforts, security vulnerabilities and breaches are inevitable. How do you know if your compromised? In large scale IoT systems, the complexity of the system in terms of the number of the variety of devices, apps, services, and communication protocols involved, can make it difficult incident has occurred. Strategies for detecting vulnerabilities and breaches include monitoring ne and activity logs for anomalies, engaging in penetration testing and ethical hacking to expose vuln security intelligence and analytics to identify and notify when incidents occur.

Read more about how to protect your IoT devices from malware attacks on IBM developerWorks.

#9 – Manage vulnerabilities

The complexity of IoT systems also makes it challenging to assess the repercussions of a vulnerab breach in order to manage its impact. Challenges include identifying which devices were affected, were accessed or compromised and which users were impacted, and then taking actions to resolv

Device managers maintain a register of devices, which can be used to temporarily disable or isola they can be patched. This feature is particularly important for key devices such as gateway device potential to cause harm or disruption, for example, by flooding the system with fake data if they h Actions can be applied automatically using a rules engine with rules based on vulnerability manag

#10 – Predict and preempt security issues

A longer-term IoT security challenge is to apply security intelligence not only for detecting and mit occur, but also to predict and proactively protect against potential security threats. Threat modelir to predict security issues. Other approaches include applying monitoring and analytics tools to co visualize unfolding threats in real-time, as well as applying AI to adaptively adjust security strateg effectiveness of previous actions.

Conclusion

Adopting a multi-layered security-by-design approach to IoT development is essential for securel and mobile and cloud-based IoT apps and services, as well as dealing with threats or issues as the

Incorporating security by default – where security features are configured at their most secure se including before, during, and after development enables you to maintain data privacy and integrity available IoT data, apps, and services.

by AnnaMGerber

Website

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.

6 comments on"Top 10 IoT security challenges"

Carl Sanford • December 22, 2017

IoT systems really need of security, this is really good information about the iot security challenges.

Reply

Madumidha • January 02, 2018

Very Useful information for researchers.... Thanks

IoT security is the biggest challenge for developers.

Reply

paul cook • January 11, 2018

Thank you for sharing this informative and interesting article. Keep up the good work! https://goo.gl/c9d

Reply

Brian Brin • January 23, 2018

Great Article, grat advices keep up the work. There are also other very interesting sources for this topic
* Industry Best Practice for IoT Security (PDF) – https://www.iot-architect.de/iot-security-industry-best
* 5 Easy Ways To Better IoT Security – https://www.iot-architect.de/common-ways-to-secure-your-iot-s

Reply

Jayaraj Chanku • February 14, 2018

Amazing and very useful information as IoT faces various security challenges. Thanks a lot for sharing tl

Reply

Lokesh Sharma • April 17, 2018

Why we have IoT security issues

It infers mind boggling and dispersed frameworks, with a tremendous wide range of (now and then out
programming dialects, and equipment.
Notwithstanding building up a straightforward application for an IoT gadget can be non-minor.
Securing the applications is even less simple in light of the fact that the assault surface is colossal (any
passage point), and characterizing all the potential dangers in advance all the potential dangers is to a g

Reply

Join The Discussion

Your email address will not be published. Required fields are marked *

Enter your comments...

Name *

Email *

Website

Recent Posts

- Call for Code is growing – We want you to be part of it
- Anatomy of a Kafka CVE
- The RTP Summer Intern Experience Blog: Executives, Emails and the Electronic Rug
- The RTP Summer Intern Experience Blog: The Land of Projects
- The RTP Summer Intern Experience Blog: Ramping Up Our Work

Categories

Select Category ⌄