Building Greater Iot Security And Trust

S.Blessy Deva Priya,
Assistant Professor,
AnnaiVelankanni's College For Women, Saidapet, Chennai, Tamilnadu, India.

Abstract: Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and discusses opening security issues of IoT.

1. Introduction

The internet of things (IOT) is on the rise to such an extent that it can be understood as the next industrial revolution. MarketsandMarkets forecasts that the internet of things will grow at a steep 26.9 percent compound annual growth rate (CAGR) from 2017 through 2022. During that time, it will expand from $170.57 billion to $561.04 billion. IDC projected that global spending on the IoT will be almost $1.4 trillion in 2021. . Lack of security confidence is one of the top concerns enterprises have about the Internet of Things (IoT). Despite the IoT's promise, it has had a reputation for quite some time as a problem area for security. There are various steps that you can take to reduce your risk so that your business can leverage the IoT to its full potential. (To learn about how IoT is affecting business, check out The Impact Internet of Things (IoT) is having on Different Industries.)

These IoT security concerns are not just isolated to businesses; they also plague consumers. Smart, Wi-Fi-connected consumer products such as televisions, phones and wearable are fast becoming a threat to personal privacy. For example, some "always on" consumer devices can surreptitiously record consumers as they communicate in their homes. This may constitute unlawful surveillance under federal wiretap law, according to the Electronic Privacy Information Center. In addition, many consumers have no idea how much of their personal data is being collected by these devices or how it is being used.

2. Use Protections Against DDoS Attacks

One of the security risks of the IoT is in its botnets. In this manner, IoT devices are being utilized by cybercriminals in distributed denial of service (DDoS) attacks. Web access is key for organizations in today's economy, with firms depending on it for business continuity. The need for the internet to be live and functional at all times is becoming ever-more-pertinent as mobile, software-as-a-service, and cloud technologies are continually integrated into businesses. The good news about DDoS is that it is a threat that has been present for some time – allowing the industry to develop DDoS defences plans that contain various layers. ISP-based or cloud tools should be used in addition to protections implemented on-site.Tech moves fast! Stay ahead of the curve with Techopedia!Join nearly 200,000 subscribers who receive actionable tech insights from Techopedia.

2.1 Update The Passwords.

Security standards will be similar to the internet of things as they are in other settings, and one of the key security steps to take is to outlaw default passwords. First, note that you do not have to create your own passwords since there are tools available to create strong passwords for you. If you do it yourself, basic rules for strong password security are as follows, per the non-profit Privacy Rights Clearinghouse:

- Avoid identical passwords for different accounts.
- Avoid personal details.
- Avoid dictionary words.
- Avoid repetition or sequential numbers/letters.
- Include a few special characters (symbols).
- Go long (since brute force can easily crack a password of seven or fewer characters).
- Consider a password built with the first letter of each word in a song title or phrase.
- Store passwords on paper in a locked location.
- Implement a password manager (such as Firefox's, per the PRC).
- Change any weak passwords, and regularly change all passwords. (For a different view on password safety, see Simply Secure: Changing Password Requirements Easier on Users.)

2.1.1Ban Auto-Connection.

Ensure that you do not have any IoT devices that will connect to open Wi-Fi hotspots automatically, as indicated by an April 2018 report from the Online Trust Alliance (ONA) covered by Jon Gold in Network World.

2.1.2 Use Security As A Part Of The Buying Process.

Factor in the risk of IoT products as you think about its value. Connecting a refrigerator might not be a good idea. Since there is inherent risk in connecting any device, make sure that adding it to your network brings sufficient value to justify the risk. "We need to appreciate that every connected device is a computer with an operating system and applications that potentially have vulnerabilities," noted Darren Anstee, CTO of Arbor Networks. To decide whether the connection of a particular device is worth it, consider the cost of learning how to properly protect it.Once you decide it does make sense to connect the type of device, consider security within the device as you look at options prior to buying. Explore the manufacturer to see if they have a history of weaknesses – and if so, how rapidly they moved to patch them.

2.1.3Perform Secure Endpoint Hardening.

Often there will be IoT devices that are operating unobserved, which represents vulnerability. It is wise to make this equipment tamper-proof or tamper-evident, noted veteran engineer and IT executive, Dean Hamilton. By taking steps to prevent tampering, you can often keep out hackers so that they cannot take your data or exploit your hardware in a botnet.

In order to achieve endpoint hardening for IoT, you will want to have various layers in place – so that unauthorized parties have to get through numerous defenses to enter your system. Address all known vulnerabilities; examples include unencrypted transfer, code injection via web servers, open serial ports, and open TCP/UDP ports.

3. Apply All Updates to Devices as they are Released.

When the manufacturer solves bug issues, those solutions should be immediately evident in your IoT network. Whenever a couple of months go by without any software updates, it is time to start being concerned and figure out what is going on. Manufacturers can go out of business. If they do, the device's security is no longer being maintained.

3.1 Partition Off The Iot From The Rest Of Your Network.

If you can, use a different network specific to your IoT presence. Set up a firewall to defend it, and proactively monitor it. By separating the IoT from the rest of your IT environment, you can make sure that the risks inherent to the IoT are blocked from your core systems. One simple way to do that is by setting up cloud infrastructurewithin a hosting data centre approved by the American Institute of Certified Public Accountants (AICPA) – i.e., audited to meet the parameters of Statement on Standards for Attestation Engagements 18 (SSAE 18; formerly SSAE 16) Service Organization Controls 1 and 2 (SOC 1 and 2).

3.2 Harden the Network.

Assuming you are using your own IoT network, it is critical to be certain that it has proper defences implemented to ward off threats. You need powerful access controlmechanisms, as well as a conscientiously designed user authentication process so that intrusion is prevented. As mentioned above, passwords should be complex and long enough that brute force efforts do not allow cybercriminals entrance. Two-factor authentication (2FA) or multi-factor authentication (MFA) should be used – so that you have to take an additional step beyond the password (typically a code sent to a mobile device).You also wants to have adaptive or context-aware authentication in place for the internet of things. This approach leverages machine learning and the specific context to continually assess the threat landscape in a manner that does not interfere with a strong user experience. Also mentioned above is encryption. You want to have encryption to secure protocols at both the transport and network layers.

4. Building Greater IoT Trust

New IoT privacy standards and architectures for deploying IoT infrastructures may help mitigate some security issues. However, the best way to improve IoT security is to have a method to monitor or observe IoT traffic "on the wire" in real-time and a way to report on-network flow anomalies and status. These can be achieved with an "IoT audit point."

4.1 Iot Audit Point

An IoT audit point is a foundational building block for establishing trust in an IoT solution. This system sits at the epicentre of IoT interconnections, constantly observing networks for the normal, predictable states that define traffic consistency. When abnormal flows are detected, an IoT audit point would have physically protected links and backend secure connections for transparent reporting. The components and requirements of an IoT audit point include:

- A platform for network flow and/or wire data observation
- Access to public and private networks
- Interconnection to platforms for data storage and wire data analytics
- Interfaces for scalable, on-demand, real-time anomaly reporting

To ensure the highest level of security, an IoT audit point should be independently operated outside of vertically contained IoT platforms or networks that depend on public Internet transit and transport. This means direct and secure interconnection is vital for a trustworthy IoT audit point. There are many software solutions available for network/wire data monitoring and capture and analysis, and each address the task in their own way. However, where these tools are deployed in the system and how they interconnect is critical to the applicable function of an IoT audit point. This is where globally distributed IoT audit points with proximity to enterprise IoT interconnection hubs are vital. IoT audit points must be placed in physically secure locations (see diagram below) and uniquely positioned for rapid and scalable deployment of network wire data tools with east/west visibility of:

- private and public network-to-cloud
- cloud-to-cloud

- private network-to-partner

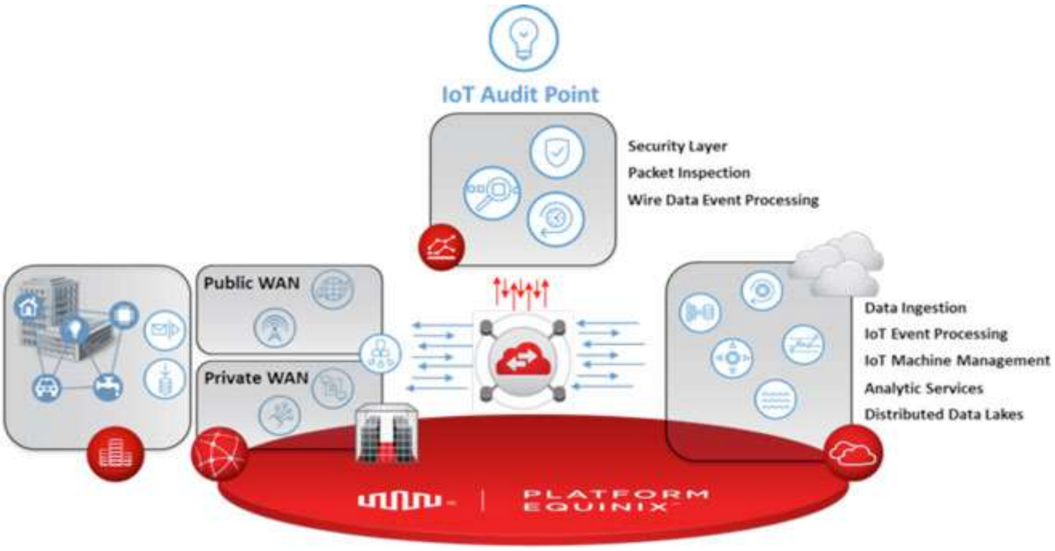

Fig.1: privatenetwork

4.2 Building Greater IoT Trust

The Online Trust Alliance (OTA) is well known for its online security initiatives and has expanded its focus to the IoT. Their goal is to develop a security, privacy and sustainability trust framework for IoT devices, potentially with a certification program. Standards groups and forums such as the IETF, ITU, IEC and the IIC are each working to tackle these issues from their vantage point, and each are contributing components to address the IoT security concerns. However, these components need to be integrated and the final solution must be able to observe “out of the ordinary” activity. The standardization and certification of secure technology implementations may be enough to build confidence, but not enough to in still trust. Trust in IoT can only be gained by reducing security breaks. And the best method for identifying these breaks is to use an IoT audit point to analyze end-to-end network traffic flows, from client to trusted service.

An IoT audit point needs to remain instantaneously and hyper-aware of when anything, other than well-defined network flows, is modified, added to or mis/redirected. These key and fundamental wire data Meta profiles are the best leading indicators of anomalies. Correlating and reporting outliers and anomalies within typical network traffic flows by means of a simple scale or binary normal, versus a distressed data flow, is a huge step toward providing transparency and building trust in IoT. In the Gartner report, “Use Data- and Analytics-Centric Processes with a Focus on Wire Data to Future-Proof Availability and Performance Management”, analysts Vivek Bhalla and Will Cappelli said, “While logs and APIs will still be the dominant data sources, use of wire data will become increasingly important.”

5. Conclusion

The internet of things is becoming an increasingly important part of the way that we do business across the industry. Device, network and data security are paramount. Take the above steps to reduce your risk and ensure that the value of the IoT is not overshadowed by a credibility-undermining, costly intrusion.

The ability to transparently observe, monitor and report IoT data anomalies and breaches via IoT audit points will be paramount to in still business and consumer security, confidence and trust in the Internet of Things.

References

1. https://www.techopedia.com/10-steps-to-strengthen-your-iot-security/2/33447.
2. https://blog.equinix.com/blog/2016/09/21/how-to-build-up-your-iot-security-confidence-and-trust..
3. https://www.zdnet.com/article/how-to-create-a-security-strategy-for-iot/
4. See,for example, AT&T Insights, Volume II, The CEO's Guide to Securing The Internet of Things; https://www.corp.att.com/cybersecurity
5. How The Internet of Things Could Be Fatal, CNBC.com (March 4, 2016) http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.htm