OVERCOMING ZERO-TRUST ENVIRONMENTS FOR SMART CITY DATA AND DEVICES

Hebberly Ahatlan
Intertrust Technologies
www.intertrust.com
400 N McCarthy Blvd Suite 220, Milpitas, CA 95035, USA

ABSTRACT

Trusted interoperability for IoT devices is the backbone for today's smart cities. How can smart cities orchestrate disparate IoT networks into a unified secure working environment where data and devices can be fully trusted? We discuss the challenges and solutions to create or enhance trusted IoT and data fabrics in smart city ecosystems.

KEYWORDS

Device Interoperability, Data Security, IoT Orchestration

1. INTRODUCTION

Smart cities run on trusted data. Without it, many of the key advantages, fueled by a highly intricate web of interoperable systems, devices and data are either lost or can be compromised (Hamilton & D'Souza, 2022).

However, a significant number of IoT devices used in smart cities today are legacy devices. These devices were created before modern security practices and standards were widely adopted; hence, they often lack basic security features such as encryption and authentication (Gold, 2019). In some cases, these devices may no longer receive security updates or patches, making them vulnerable to attacks.

While modern IoT devices can be designed and manufactured with security in mind, they are only as strong as the weakest link in the data fabric they occupy. Traditional methods of protecting connected devices use connection-oriented protocols, like VPNs and TLS, and are all about securing the lines of transmission. In zero- or low-trust environments, this approach breaks down.

How can smart cities orchestrate disparate IoT networks into a unified secure working environment where data and devices can be fully trusted? In this paper, we discuss the challenges smart cities face while trying to implement infallible IoT security. We suggest a holistic IoT systems protection approach to securing IoT devices and the data they generate–from edge to cloud, in transit and at rest, and in any public, industrial, commercial, or private setting.

2. TRUST CHALLENGES IN IOT DEVICE INTEGRATION FOR SMART CITIES

Smart cities are complex systems of heterogeneous entities all of which need to interact and rely on one another (Ammara, et al., 2022). This vast, intertwined network of devices, applications, resources, and people are responsible for operating all manner of functions within the city.

Smart cities host heterogeneous IoT devices, such as traffic lights, parking meters, air quality sensors, and public safety cameras, which are supported by connectivity protocols, such as Wi-Fi, 5G, and low-power wireless networks like LoRa, ZigBee and Sigfox (Bauer et al., 2021). These entities represent a complex mix of manufacturers, platforms and formats optimized for fast data throughput, but not for protection of data in transit or at rest. Furthermore, legacy IoT fabrics go largely unauthenticated (Weinberg, 2021). Many data

platforms are not set up to validate the integrity of the data they process–much less the authenticity of the devices the data came from.

Diverse IoT fabrics create hyperconnected environments where thousands of IoT devices send raw data where their trustworthiness cannot be assured because of the disparate technologies implemented by modern and legacy IoT devices (Thomas, et al., 2019). Furthermore, IoT meshes not only collect data, but bridge cyber-physical integrations where devices function as actuators to, for example, shut off grids, industrial robots, or cameras. Unprotected hyperconnectivity and vulnerable cyber-physical integrations are serious problems associated with poorly harmonized IoT networks composed of legacy and modern devices (Zetter, 2021).

2.1 Failure of Session-level Security

Session-level or endpoint security may be adequate to protect simple data and IoT fabrics, but what happens when data traverses multiple endpoints and is invoked by multiple sessions involving distinct communication protocols? Because there are no standard security protocols in place for IoT fabrics, session and endpoint security has a narrow protection scope. In addition, many IoT devices have limited computing power and memory, which makes it difficult to implement robust security mechanisms.

Vast numbers of legacy IoT devices - and even modern IoT devices, do not receive regular security updates, which leaves them vulnerable to new attacks. Moreover, some devices may not have the capability to receive updates at all. To make matters worse, in some cases, the data transmitted between IoT devices and servers may not be encrypted, making it vulnerable to interception and tampering. Data is not always protected in transit or at rest regardless of the number of networks or cloud ecosystems it traverses.

2.2 Lack of Data Interoperability

With a variety of IoT devices from different manufacturers, interoperability is a big challenge. Different devices may use different communication protocols, and it can be difficult to make them work together. Scaling cyber-physical networks is challenging, especially as different types of data or data commands may need to be processed in different ways.

2.3 Limited Network Connectivity

IoT devices can only connect to a network within a certain range, which can be a challenge when deploying devices in large or spread-out areas. Wireless signals used by IoT devices can be disrupted by physical objects or electromagnetic interference, leading to connectivity issues. Large volumes of IoT devices can put a strain on the network, leading to issues with connectivity and latency. IoT devices may use different communication protocols which can make it challenging to connect them to a common network.

This can require additional hardware or software solutions to enable interoperability. Stuxnet attacks on an IoT network demonstrate that isolating computers from using network security is totally inadequate, even if air gapped or intermittently connected through USB drives (Fruhlinger, 2022). NIST principles for a zero-trust architecture specify how this can be done (Rose, et al., 2020) but deploying NIST’s specifications globally, with legacy devices in the mix is a real challenge.

2.4 Data Integrity Issues for Data Collection, Analysis and Sharing

Ensuring the integrity and accuracy of IoT data is essential. This is particularly challenging when attempting to assert data consistency, completeness and reliability in large networks. IoT devices generate data in different formats, making it challenging to integrate and process it into a unified data model that collects, stores and analyzes data in a scalable and flexible way.

3. SOLUTIONS FOR ESTABLISHING TRUSTED DEVICES AND DATA FOR SMART CITY INFRASTRUCTURES

Technical solutions for device deployment in the context of trusted smart city data and IoT networks can be broadly classified into three categories: hardware, software and cloud-based solutions.

- **Hardware solutions** include specialized security chips designed to be easily integrated into IoT devices.
- **Software solutions** include the development of network and device agnostic software applications and tools that simplify the process of deploying and managing IoT devices.
- **Cloud-based solutions** involve using cloud platforms and services to manage and harvest IoT data. These solutions typically provide a variety of services, including device management, data collection and analysis, and security features.

By applying standardized protocols to all three categories as well as testing devices thoroughly before deployment and developing clear documentation and training materials for device users, organizations can improve the efficiency and effectiveness of their data fabrics and IoT deployments.

3.1 Secure Systems Approach

Security protocols such as TLS often used to secure IoT devices and data in a smart city infrastructure are not able to completely secure complex networks of heterogeneous devices running on diverse platforms. A secure systems approach to IoT fabrics involves protecting availability of information, confidentiality, integrity, accountability and authorization through practices such as:

- *Authentication and Encryption*: Devices should be required to authenticate themselves before they are allowed to connect to the network. Data should be encrypted in transit and at rest to prevent unauthorized access.
- *Firmware and software updates:* Regular firmware and software updates can address vulnerabilities and improve security.
- *Security policies and procedures:* Organizations should establish security policies and procedures, and employees should be trained on how to follow them. This can help reduce the risk of human error and ensure that security best practices are followed.

Orchestrating trusted IoT networks within smart city infrastructures to mitigate issues arising from hyperconnectivity and cyber-physical integrations involves implementing robust security that not only protects the data channels, but the data packets themselves.

Technologies such as TLS can be greatly enhanced by protecting every packet of data entering or exiting an authenticated IoT system in addition to securing the data channel with canonical encryption schemes (Maher, 2022). It also involves enhancing existing technologies such as MQTT or MAC as well as tackling the challenges of comprehensive data security, data interoperability, device deployment, network connectivity, data collection and analysis.

3.2 Network Connectivity

There are several technical solutions to address the challenges of network connectivity in IoT-based smart city infrastructures, including:

- *Mesh networking*: Mesh networking is a topology where each device in the network is connected to several other devices. This helps in creating a self-healing network that is more reliable and can cover a larger area. However, meshes can be vulnerable unless they are protected with robust security hardware and software. It is in this context that trusted interoperability platforms become the kernel of well managed secure networks.
- *Broadband wired or wireless networks*: IoT devices rely on trusted interoperability platforms to integrate diverse connectivity modalities and protocols - each with its own set of benefits and vulnerabilities. It is critical to implement network and device agnostic trusted interoperability platforms for seamless device authentication and secure data sharing.

Overall, the choice of network connectivity solution depends on the specific requirements of the IoT deployment and the available resources. It is important to consider factors such as cost, coverage, bandwidth, power requirements and data security when selecting a network connectivity solution.

3.3 Data Collection, Analysis and Sharing

Smart city infrastructures depend not only on a mesh of IoT devices working within a secure VPN, but on packets of data moving to and from this VPN protected by a "digital bodyguard" that secures them no matter where they go (Kalima & Durand, 2023). Advanced data packet protection schemes are the new technologies that offer new methods of implementing a trusted multi-layered security approach that includes device authentication, enhanced data encryption, access control and regular security updates.

There are several approaches to address the challenges of data collection, analysis and sharing in IoT-based smart city infrastructures, including:

- *Edge Computing:* A distributed computing model that brings computation and data storage closer to the location where it is needed. In the context of smart city infrastructure, edge computing can help to reduce network traffic and latency by processing data locally on the devices, rather than sending it to a centralized server for processing. This can lead to faster response times, lower bandwidth requirements and more efficient use of resources. However, it is here where it is important to consider that IoT devices need to be properly authenticated to guarantee that their edge computing function is fully trusted.
- *Data Privacy and Security:* Ensuring the privacy and security of data collected from IoT devices and sensors is crucial in smart city infrastructure. Solutions such as encryption, authentication and access control can be used to protect the data from unauthorized access and to ensure the privacy of the citizens.
- *Data Visualization:* The use of graphical representations to make smart city data easier to understand and interpret. Visualizing and presenting complex data in an intuitive, trusted and accessible way enables city managers and other stakeholders to make informed decisions. Trusted interoperability platforms are the key to efficient data visualization across disparate data consumers.

4. CONCLUSION

A trusted interoperability infrastructure ensures that legacy and modern IoT devices can communicate and work together seamlessly. Interoperability can be achieved by using common communication protocols, such as enhanced MQTT or MAC that not only protect the data channels but also the data packets traversing through any networks or devices (Kalima & Durand, 2023). Furthermore, encryption and authentication mechanisms with digital signatures can be used to secure data transmissions and ensure the integrity of data and devices.

A holistic approach to these challenges comprises establishing integrated, trusted infrastructures, through synchronized collaborations among stakeholders and through well planned IoT fabric deployments. For efficient collaboration experiences across all data and device stakeholders, consider integrating a flexible interoperability trust stack that implements state of the art technologies that go beyond standard solutions, such as TLS or MAC where the trust and protection is agnostic to the network and device technologies and where data is protected beyond a session or endpoint, in zero-trust environments. Technologies such as XPN can enhance MQTT, MAC and TLS frameworks, thereby achieving a robust smart city zero-trust environment.

Addressing these key points through flexible interoperability trust stacks delivers environments where legacy and modern IoT devices can be integrated into trusted interoperability infrastructures for smart cities, enabling improved efficiency, enhanced safety and security, better citizen services, improved environmental sustainability and economic growth.

REFERENCES

Ammara, Umme, Rasheed, Khansa, Mansoor, Athar & Al-Fuqaha, Ala (2022, June) "Smart Cities from the Perspective of Systems." Researchgate.net. *https://www.researchgate.net/publication/361260619_Smart_Cities_from_the_Perspective_of_Systems*

Bauer, Martin, Sanchez, Luis & Song, JaeSeung (2021, June). "IoT-Enabled Smart Cities: Evolution and Outlook." National Library of Medicine. *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8271664/*

Fruhlinger, Josh (2022, August). "Stuxnet explained: The first known cyberweapon." csoonline.com *https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html*

Gold, Jon (2019, July). "Report: Smart-city IoT isn't smart enough yet." Network World. *https://www.networkworld.com/article/3411561/report-smart-city-iot-isnt-smart-enough-yet.html*

Hamilton, Michael & D'Souza, Cedric B. (2022, February) "Technology of IoT Systems." UL Solutions. *https://collateral-library-production.s3.amazonaws.com/uploads/asset_file/attachment/44554/CS249800_-_Whitepaper_-_Technology_of_IoT_Systems_Final_Digital.pdf*

Kalima, Chris & Durand, Julian (2023, February). "How is XPN different from a VPN." Intertrust Technologies. *https://www.intertrust.com/platform/xpn-faq/#faq-item-6*

Maher, Dave (2022, June). "SPTIoTCoE fireside Chat." Intertrust Technologies. *https://www.youtube.com/watch?v=apwUjGm_okk*

Rose, Scott W., Borchert, Oliver, Mitchell, Stuart & Connelly, Sean (2020, August) "Zero Trust Architecture." Nist.gov. *https://www.nist.gov/publications/zero-trust-architecture*

Thomas, Ian, Kikuchi, Shinji, Baccelli, Emmanuel, Schleiser, Kaspar, Doerr, Joerg & Morgenstern, Andreas (2018, October). "Design and implementation of a platform for hyperconnected cyber physical systems." Sciencedirect.com. *https://www.sciencedirect.com/science/article/abs/pii/S2542660518300581*

Weinberg, Adam (2021, October). "Common IIoT & IoT Protocols and Their Security Flaws." First Point Magazine. *https://www.firstpoint-mg.com/blog/common-iiot-iot-protocolsand-their-security-flaws/*

Zetter, Kim (2022, April). "Israel May Have Destroyed Iranian Centrifuges Simply by Cutting Power." theintercept.com. https://theintercept.com/2021/04/13/iran-nuclear-natanz-israel/