Alma Mater Studiorum · Università di Bologna

COMPUTER SCIENCE AND ENGINEERING - DISI

Digital Transformation Management

SECURING CONSTRAINED NETWORKS THROUGH ZERO TRUST ARCHITECTURE

Relatore:	**Presentata da:**
Gabriele D'Angelo	**Filippo Ciliberti**

Sessione

Anno Accademico 2024 - 2025

Alla curiosità che mi guida,
alle montagne scalate,
a chi ha creduto in me,
sempre ...

Abstract

In this era of digital transformation, the rapid multiplication of interconnected devices has profoundly expanded the landscape of cyber threat. New security challenges are a daily priority on the agenda, especially in constrained networks where the traditional security architecture has proven to be insufficient per design. The rise of the Internet of Things (IoT) added an additional burden to the already weak security infrastructure. This drew attention to the need for new frameworks that aim to contain the attack surface that, after the advent of these interconnected smart technologies, expanded without control.

This dissertation explores the Zero Trust Architecture (ZTA) as a shift toward robust protection in embedded devices, resulting in a safeguard of the overall security posture and exposure in networks. Although this shift allowed the evolution of legacy security approaches and principles, it does not completely discard them. Eliminates fundamental weaknesses to the detriment of the implicit trust that the IoT has aggressively assumed.

Contents

List of Figures

Chapter 1

The new Digital Paradigm

1.1 The Origins and Evolution of Cybersecurity

In the last decades, cybersecurity has evolved drastically, shaped by the increasing digitalization of society and the constant demand for connectivity interconnection. Although cybersecurity was once exclusive for military operations and warfare, with these technological advancements and the increasing reliance on these digital systems, it has now become a fundamental pillar across all industries, positioning itself at the core of business, infrastructure and financial systems. As the Internet expanded, so did the attack surface and the complexity of cyber threats. As a result, cybersecurity defenses evolved rapidly with the advent of new defense means and the establishment of national cybersecurity agencies to mitigate worldwide cyber risk. Today, cybersecurity is a multibillion-dollar industry looking for steady growth and evolution. In fact, it grows along with the emerging technologies that expand the attack surface. One beneficial aspect is that the drive for security and protection has always been strong, often reinforced by critical turning points, like the 1998 Morris Worm which highlighted vulnerabilities and the need for robust security measures. Continual awareness ensures that the new security principles and new architectures are built on a solid foundation established to mitigate the threats of the older technologies [1].

As cybersecurity continues to evolve alongside technological advancements, one of the most significant challenges today comes from the rapid expansion of interconnected devices. An example of this is the Internet of Things (IoT), which connects billions of devices in several industries. IoT has introduced new security vulnerabilities that require the adaptation of existing cybersecurity frameworks and the development of specialized protocols to protect these systems. Before a deep dive into what IoT is and how it is structured, let's first explore the fundamental principles that form its foundation.

1.2 The growth of IoT and its protocols

The growth of IoT has not only revolutionized industries but also significantly altered the cybersecurity landscape. Ensuring secure communication between these connected devices requires dedicated protocols that balance efficiency, energy consumption, and security requirements. The number of industries that IoT revolutionized and transformed is profound and boosted the pervasive adoption of technology within individuals and businesses. Different sectors, which will be highlighted in the next chapter, found their efficiency, automations, and decision-making enhanced, resulting in an optimized development and an expectation of exponential growth.

At its core lies the facilitation of scalable communication between millions of devices. To ensure interactions between them, various protocols govern data transmission, each one based on the specific need, considering bandwidth, energy consumption, and responsiveness, which for IoT needs to be real-time. Among the various IoT communication protocols, one of the most widely used is Message Queuing Telemetry Transport (MQTT) which will be highlighted in the next chapter, to discuss its security vulnerabilities and the risks associated with its widespread adoption[2]. MQTT relies on the Transfer Control Protocol (TCP) to ensure reliable message delivery between IoT devices. TCP was originally neglected as a transport layer protocol for the IoT due to significant constraints with respect to the memory, processing, and energy of IoT devices. On the other hand, TCP was leveraged for its mainstream position [3]. As the communication channel is the backbone of the IoT, we identify the same principles and architecture of the TCP protocol suite (TCP/IP) as it is the most effective and widely adopted standard, and must be followed regardless of the type of communication.

Having established the importance and reliability of communication standards, it is equally important to be aware of their inherited security limitations of the interconnected ecosystem, made up of devices, users, and distributed networks. Protocol suite design was not originally conceived with security at the core, particularly true for the TCP/IP Suite, developed in 1980s, and its mainly focused on facilitating reliable communication between different computer systems rather than ensuring secure data transmission [4]. In fact, in the IoT realm, these limitations are even more pronounced due to problems that occur both in the network and in the transport layer, suggesting a comprehensive reevaluation of its architecture [5].

As will be discussed in the following chapter, similarities can be found within the TCP/IP suite and the IoT architecture, as well as vulnerabilities and exploits. Building on this foundation, the following chapter will examine the layered structure of IoT and its inherent security challenges. The introduction of a robust and needed security measure will be adopted to avoid the annex risks and the impact of technological development.

Chapter 2

Internet of Things

2.1 Understanding Constrained Networks and IoT

To understand what IoT is, we need to focus first on the term Constrained Node. A constrained node is a node with physical constraints not limited to available power deployment options, user interface, and energy, but also extended to computation and memory limitations. Due to these limits, the efficient use of energy and bandwidth is a primary focus, to extend the device lifespan and ensure reliable effectiveness in these environments. These small devices, or better known as smart devices, can form a network called "Constrained Network", which inherits constraints and restriction of each member involved, for example, unreliable channels, limited and unpredictable bandwidth, and highly dynamic topology [4].

The Internet of Things (IoT) represents a key component of resource-constrained nodes. "Things" are internet-connected devices that represent a bridge between the digital and the physical world, thanks to the constant source of information collected by a set of sensors. Any physical object can potentially be converted into a "thing" and generate telemetry data. This is the step that goes beyond the traditional way of computing and can be the first step towards the embedded intelligence of our environment, aligning with the idea that Mark Weiser envisioned in 1999, when he described how the best technologies are those that disappear [6].With the growing presence of Wi-Fi internet access, the evolution towards an ubiquitous network is already evident.

An IoT system provides the sensing and actuation functionalities performed by actuators that turn energy into motion via mechanical or electromechanical devices and the analysis and monitoring of activities. Today, IoT systems are becoming ubiquitous and integrated in various aspects of daily life and industrial applications. Some use cases include Smart Homes, Healthcare, Agriculture, Smart Cities, Transportation, and Logistics. Most organizations have hundreds of thousands of these devices, including badge scanners, printers, devices for teleconferencing or security cameras, as well as devices to manage Heating, Ventilation and Air Conditions (HVAC) systems. Below, an overview of the advanced services that improve the handling of the physical infrastructures surrounding humanity in this century.

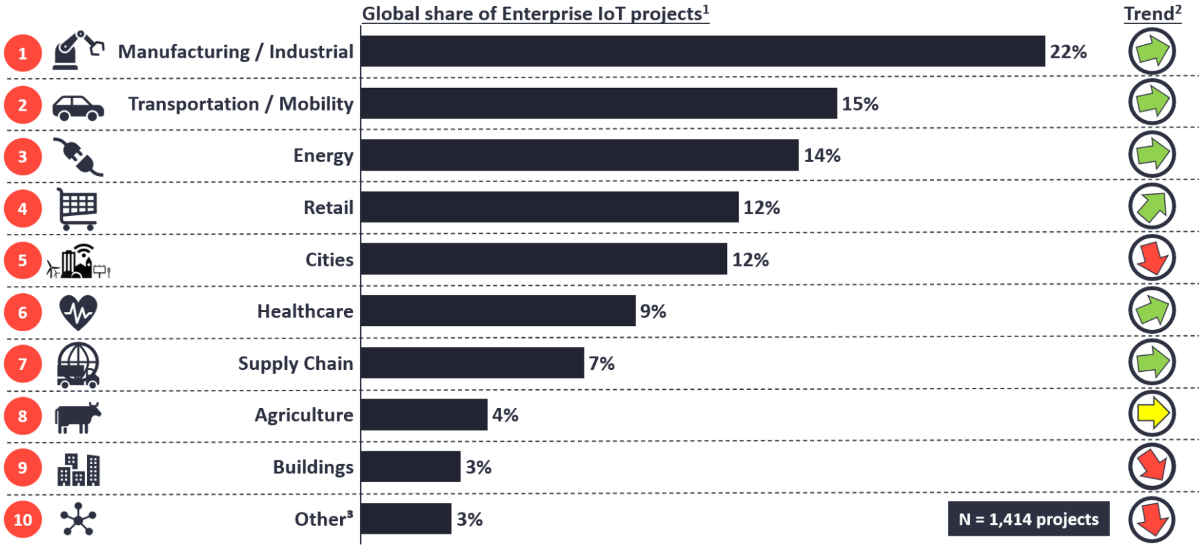


Figure 2.1: IoT Applications [7]

IoT devices often lack strict security protocols, have weak password input validation, and most importantly can reveal sensitive information [8]. At present, everything is connected to the Internet, inter-accessible, and vulnerable. The attack surface is widening more than ever and the attack vectors are multiple. Even the deployment and maintenance of IoT devices can lead to vulnerabilities, especially on a large scale. Attackers know that the resources needed to monitor such an extended ecosystem are very expensive and, when it comes to cybersecurity risk, these ecosystems are extremely dangerous.

Threat actors are increasingly disrupting ecosystems by compromising IoT devices, as always driven by political, financial, or ideological interests [8].

2.2 Attack surface and attacks

As previously mentioned, similar to the TCP/IP suite, IoT systems are structured into different layers, each responsible for specific processes and functionalities. This layered approach improves clarity and simplifies understanding by assigning different scopes and roles to each layer, as shown in Fig. 2.2.

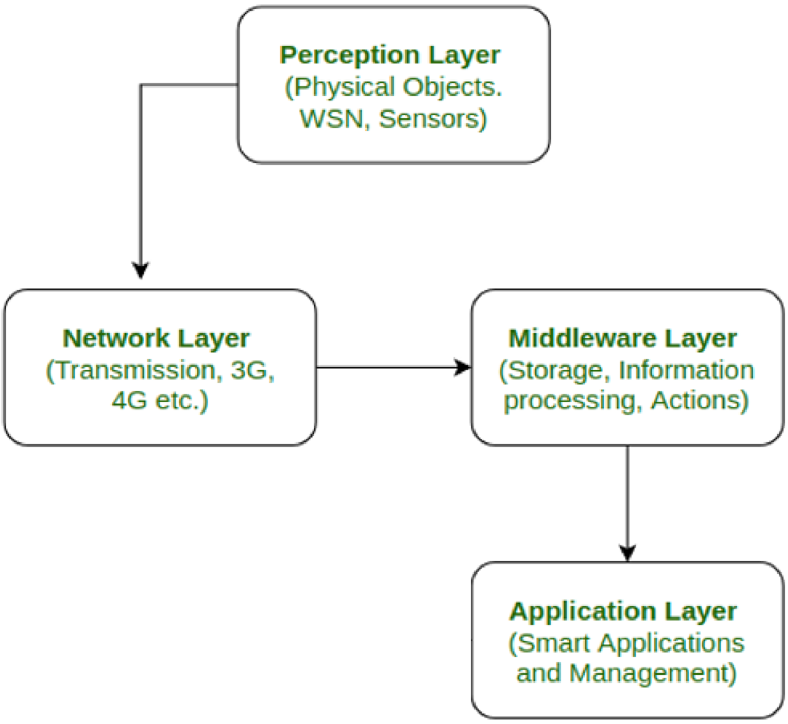


Figure 2.2: IoT architecture. The four layers of IoT and their functionalities [8]

The **perceptual layer** collects information using a variety of physical sensors, readers, or satellites with the aim of identifying the physical world. Node included in this layer are not capable of security measures such as hopping the frequency to minimize interception of communication or applying encryption algorithms to prevent unauthorized accesses, making it very tricky to protect from attacks such as data manipulation, eavesdropping, or resource exhaustion. The main challenge for the perceptual layer is to ensure confidentiality, and regardless of weak or often absent Identity Access Management (IAM), the main requirement is to enforce authentication [8]. IAM will be discussed in the next chapter as part of the core principles of the ZTA. IoT devices are usually deployed in adverse environments, therefore can easily be accessed or tampered by an adversary. The most common attacks in the perceptual layer include the following:

- **Node Capture:** it is the easiest attack to launch, as well as the first. It is generally divided into three stages: (i) physically capture the node, extract sensitive information, (ii) compromise it, (iii) redeploy the node, and perform internal attacks [10]. To extract sensitive information, attackers aim to the encrypted embedded memory in secure chips, exploiting weaknesses of the encrypted memory with microprobing attacks [11].

- **Node Replication:** once one node has been controlled, an adversary can easily generate replicas and manipulate network behaviors, such as intercepting data, inject malicious commands or disrupt operations. Anomaly-based intrusion detection systems (IDS) can effectively detect replication attacks [12].

- **Node Destruction:** refers to the physical destruction of nodes by any means, with the aim of permanently damaging the node, therefore its availability [13].

The **network layer** is the second layer, reliable for establishing and maintaining communication between the several components of the entire environment. The transmission of information is based on basic network principles and communication protocols, essential for the exchange of information between devices [13]. The attacks in network layer are very common and diverse and include:

- **Denial of Service (DoS):** it is the most common and easiest attack against IoT. It floods the target, exhausting its resource and jeopardizing availability. They can be launched at different component of the system, including physical, data link, transport and application layers. incapacitates all three fundamental pillars of cybersecurity, confidentiality, integrity, and availability [9].

- **Monitoring and Eavesdropping:** attackers can intercept with IoT communication using wireless receivers. Since 98% of all the IoT traffic is unencrypted, personal and confidential information are at severe risk [14]

- **Domain Name System (DNS) tunnelling:** each device connected to the Internet has a an unique IP address, required to identify itself and communicate with other devices over the network. The Internet Protocol (IP) follows a client-server model, meaning that a client sends a request to the server, which processes the request and "serves" the requested information back to the client. Today we access information through domain names, which are translated in IP addresses by DNS. We can think of the DNS as the Internet's phonebook that translates, or resolves, domain names into IPs. As domain names are easier to remember than IP addresses, DNS simplifies web navigation by translating human-friendly names into numerical addresses, allowing an easier human interaction when rendering or retrieving information online.

  Since most of the network communication relies on this protocol, DNS queries are allowed by firewalls by default, as blocking them would result in service disruption. This design makes DNS a valid candidate for attackers willing to sneak malicious data, such as stolen information, malware, or Command and Control (C2) techniques to maintain communication with compromised devices [13].

Known also as **middleware layer**, the third layer is called the support layer. It acts as a bridge between the application layer and the hardware components, passing through the network layer. Its primary role is to facilitate communication, data management, and interoperability across diverse IoT devices and platforms. It has been defined as computer software that facilitates communication and integration between different IoT applications and the underlying hardware or operating system (OS) [15]. Middleware solutions support cloud-based infrastructures, edge computing, and distributed networks, helping IoT systems scale while maintaining low latency. By handling tasks such as data storage, analysis, and processing, the middleware layer enables IoT systems to make informed, automated decisions based on collected data. Indeed, the most critical aspect of this layer is the security, due to the huge number of devices connected and data generated.

Middleware-based IoT application protocols play a crucial role in enabling bidirectional communication and remote control of IoT devices. Among the various IoT application protocols, Message Queuing Telemetry Protocol (MQTT) is being widely adopted due to its simple model and low bandwidth usage. It is a publish-subscribe (pub-sub) application protocol that uses TCP as its transport protocol to ensure reliable, ordered and error-free delivery of messages between clients and broker [16]. Indeed, the delivery of the packets is as follows: (i) the publisher sends a CONNECT packet to the broker, (ii) the broker responds with a CONNACK packet, confirming the establishment of the connection, (iii) the publisher sends a PUBLISH packet with the topic and the message payload to the broker, (iv) the broker forwards the packet to all the clients subscribed to that topic, (iiv) the publisher terminates the connection sending a DISCONNECT packet to the broker [17].

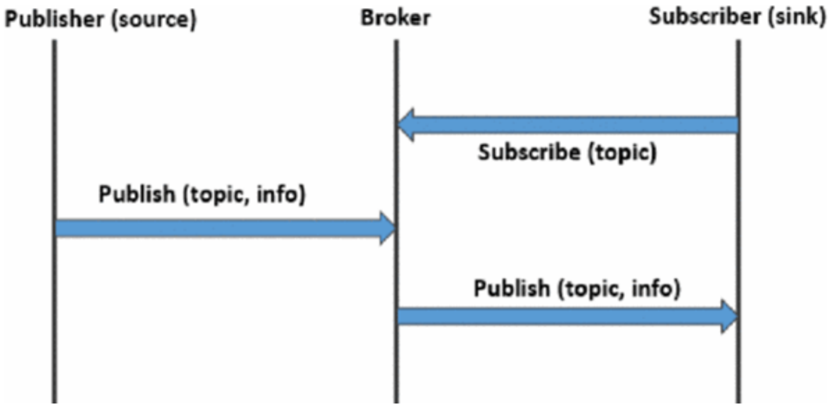
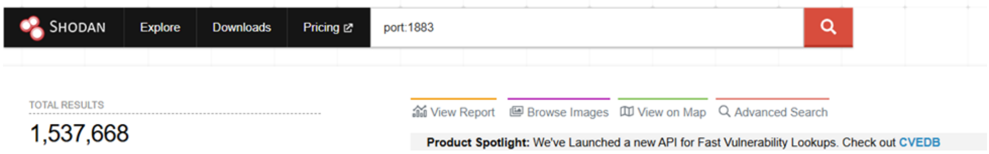


Figure 2.3: Pub-Sub process in MQTT [17]

By default, all communication is in plain text, unencrypted, making all IoT devices vulnerable. Since this default behavior poses significant security risks, the implementation of TLS throughout communication is crucial to avoid interception or tampering. These security measures are suggested by the Oasis standard (Section 5) which follows Request For Comment 5246 [RFC5246] [18], although poorly implemented. This is confirmed by analyzing on the Shodan tool the difference between the devices founded querying both the unencrypted port 1883 and the encrypted 8883.



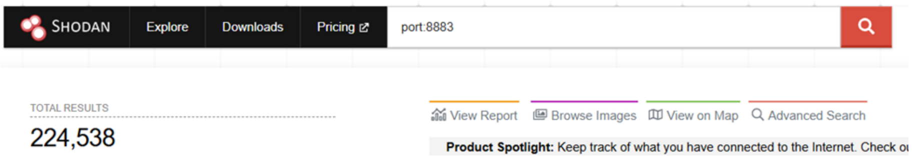
port:1883

TOTAL RESULTS

1,537,668

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

Figure 2.4: Unencrypted TCP connections: port 1883



port:8883

TOTAL RESULTS

224,538

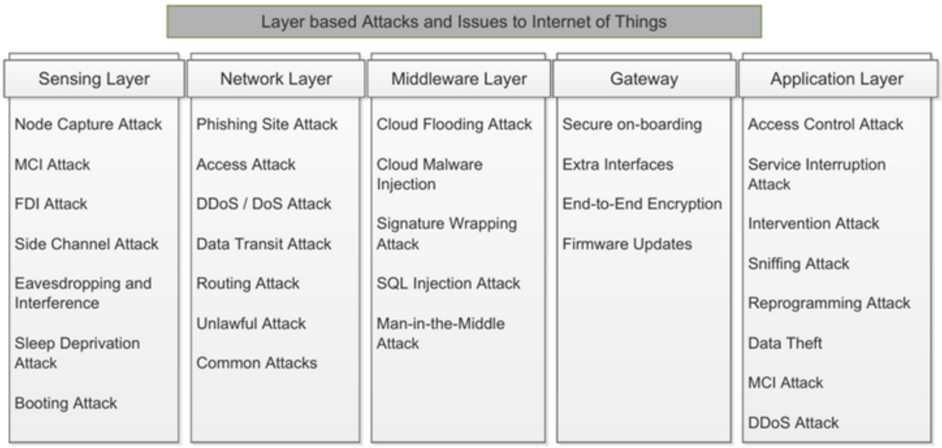
Product Spotlight: Keep track of what you have connected to the Internet. Check ou

Figure 2.5: Unencrypted TCP connections: port 8883

The above results show that out of 1,762,206, only 12.7% is relying on secure TCP connections, making attacks like Man In The Middle (MITM) and subsequent session hijacking attacks feasible. However, these attacks remain technically challenging, as they often require advanced network infiltration techniques and in some cases, bypassing additional security measures such as Virtual Private Networks (VPNs) or firewalls.

Application layer encompasses all applications that use IoT technologies or in which IoT systems have been deployed. The data that the middleware layer processes is used by this layer to deliver the appropriate services to applications depending on the type of data collected by the sensors. A few examples of applications implemented through IoT can be listed as smart home, smart farming, smart health, smart city, intelligent transportation [19]. Common attacks on the application layer include often attacks on access control, malicious code injection, service interruption and software flaws.

In the image below, we can observe different types of attack for each different layer of the IoT architecture.



Layer based Attacks and Issues to Internet of Things

Sensing Layer	Network Layer	Middleware Layer	Gateway	Application Layer
Node Capture Attack	Phishing Site Attack	Cloud Flooding Attack	Secure on-boarding	Access Control Attack
MCI Attack	Access Attack	Cloud Malware Injection	Extra Interfaces	Service Interruption Attack
FDI Attack	DDoS / DoS Attack	Signature Wrapping Attack	End-to-End Encryption	Intervention Attack
Side Channel Attack	Data Transit Attack	SQL Injection Attack	Firmware Updates	Sniffing Attack
Eavesdropping and Interference	Routing Attack	Man-in-the-Middle Attack		Reprogramming Attack
Sleep Deprivation Attack	Unlawful Attack			Data Theft
Booting Attack	Common Attacks			MCI Attack
				DDoS Attack

Figure 2.6: Layer based attacks [20]

2.3 Risk and Impact

The primary objective of the Internet of Things (IoT) is to enhance environmental intelligence. Therefore, the economic impact deriving from exploits varies between industries based on their adoption. In 2023, Zscaler, a leading provider of cloud security solutions, reported a 400% increase in IoT attacks within a period of one year. The manufacturing and retail sectors represented nearly 52% of affected IoT devices, experiencing approximately 6,000 attacks per week. Furthermore, the education sector witnessed an unprecedented surge in IoT-related threats, with an increase of 1,000% in attacks. This poses a significant and concerning risk of long-term data exfiltration, given the large repository of intellectual assets, research data, and personal information of future professionals and academic personnel [21]. According to the Federal Bureau of Investigation (FBI), American lost $13 billion due to cyberattacks in 2023, with more than 41% small businesses that experienced a cyber attack [22]. As more and more industries adopt smart solutions, the exponential increase in cyber threats will be significant, with annexed loss of reputation, business disruptions, and long-term data exfiltration.

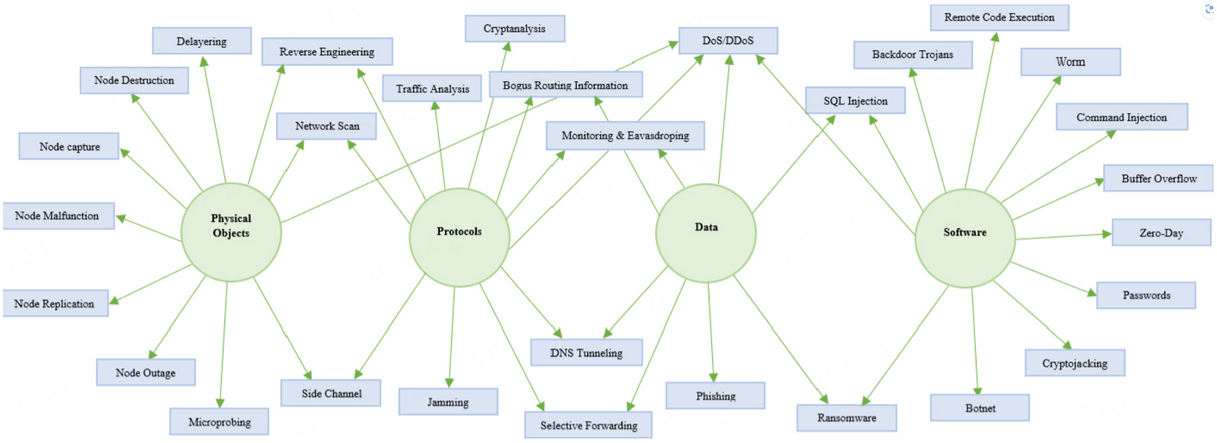


Figure 2.7: Attacks vs Assets [13]

Like traditional systems, security in IoT follows a multi-layered approach, where the control is applied at every layer of its architecture. In the following chapters, we are going to analyze how existing architectures and frameworks have developed in direction of a more robust model and how it can be applied to the context of constrained networks.

Chapter 3

Zero Trust Architecture

3.1 The evolved perception of trust

The concept of trust is an interdisciplinary definition that has been explored and analyzed for decades. Since it still lacks a universal definition, we can interpret it within the cybersecurity as a risk factor that influences system integrity. Indeed, it is the result of policies, access control decisions, and mitigation strategies that have been designed to control interactions within a network. To better frame and interpret trust, we need to build upon traditional security methods and the multilayered security approach which are, as mentioned, intrinsically related to IoT architecture. Traditionally, models absolutely trusted entities within the network perimeter. Indeed, networks were divided into (i) an internal trusted network and (ii) an external untrusted one. Usually, the perimeters were defined by, firewalls, or IDSs.

With the massive increase of more sophisticated cyber threats, traditional perimeter-based defense was proved to be insufficient. As the perimeter began to dissolve, there was the need to address both internal and external menaces [23] by adopting a more robust methodology, able to tackle a wider variety of attacking techniques. Here, a multilayered approach comes into play, a security scheme that aimed to make the perimeter thicker and, as the name suggests, considers different layers of defense to mitigate different threat and vulnerabilities at each different layer of the architecture. The goal is to create diverse security controls ensuring that, even if one layer gets compromised, the others in place will keep protecting critical assets. One of the most implemented strategies is Defense in Depth (DiD), a concept that employs a multilayer protection with diverse strategies and controls, to cope with multiple risks that organizations could face and so mitigate. DiD comes from the military sector; it has been shown to be an effective way to guarantee a strong level of security and prevention against a wide range of attacks [24]. Below, a visual representation of the approach to be described:

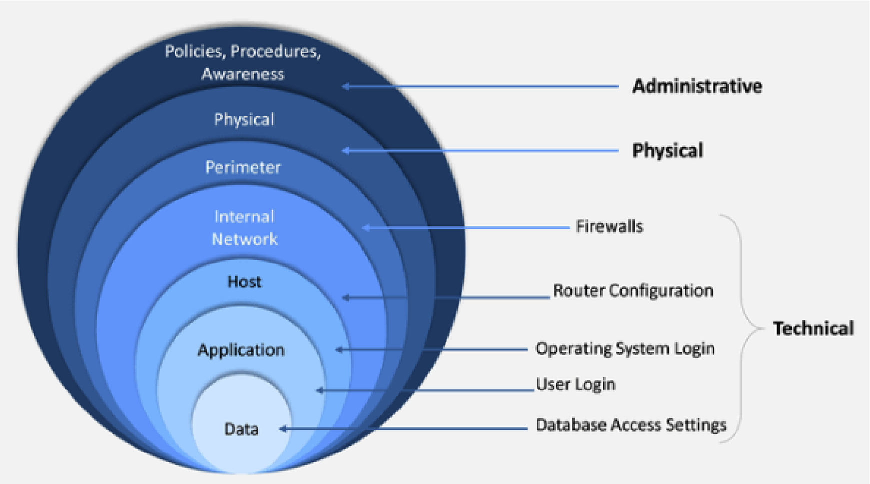


Figure 3.1: Defense in Depth [33]

It is considered one of the most flexible techniques for protection, which divides its components as follows:

- **Policies and Procedures:** the established guidelines, behaviors and access controls within a system. The foundation to implement other security measures.
- **Physical Security:** the protection against physical threaths.
- **Newtwork Security:** protection from external attacks by implementing security measures such as firewalls, or IDS.
- **Monitoring and Logging:** detection and analysis of telemetry and events across the systems.
- **Host Session and Application Security:** security of individual hosts, applications and users from unauthorized assets or threats.

- **Data Security:** ensure the protection of sensitive information.

However, the increasing complexity of emerging solutions, such as cloud and multi-cloud, together with the contemporary threat actors that become more persistent and stealthier, made perimeter-based defenses with multiple layers of security obsolete and made once again questioning about the meaning of trust. Zero Trust Architecture proved to be a modern and better approach to protect organizations and provide unified access control to data, services, applications, and infrastructure [25]. Its goals are to safeguard the overall security posture and exposure in networks, and to ensure that no asset or user is at risk. ZTA operates on a deep core principle, the Zero Trust principle: "never trust, always verify". No entity, regardless of the origin of every access and regardless of whether it was originated within or outside the network perimeter, is inherently trusted; every access is treated as if it originates from untrusted networks, with the necessity of an accurate verification process before access can be granted. The implementation of proactive measures like adaptive and other trust control mechanisms copes with the expansion, the complexity, and the dynamism of what information security became today.

ZTA emphasizes identity verification, least privilege principle and continuous monitoring, as well as Identity and Access Management (IAM), Multi-Factor Authentication (MFA), visibility, and micro-segmentation [26]. Therefore, it is a collection of concepts and ideas that aim to minimize uncertainty with the focus towards authentication, authorization, and shrinkage of trust zones within the enterprise's cybersecurity plan.

3.2 Zero Trust vs Zero Trust Architecture

Zero Trust (ZT) assumes there is no implicit trust based neither on the physical location and the network, nor on the ownership of the asset or user accounts. It focuses on protecting assets, services, workflows, accounts, but not segments of networks, as the network location is not longer seen as a discriminant to assess the security posture of the resource. A Zero Trust Architecture (ZTA) uses the principles and concepts of ZT to plan infrastructures and workflows and produce a ZT environment [27] which is the result of comprehensive security monitoring, together with dynamic risk-based access control and security automation, focusing on protecting critical assets in real-time. ZT assumes breaches by default, defending as if an adversary already infiltrated the environment and maintaining a commitment towards explicit verification, continuosly authenticating and authorizing every request [23]. Having established the importance of ZT in ZTA to transform security paradigms, let us analyze all the core principles that nowadays help us reduce the potential impact of breaches by restricting access privileges and continuously verifying trustworthiness at every interaction.

3.3 Core Principles Zero Trust Architecture

Beyond the principle of never assuming trust but always verifying, ZTA is built on different core principles [23] that determine the implementation and its operation, including:

- **Least Privilege Access:** a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks [28].

- **Micro-Segmentation:** implemented to create security zones and isolate sensitive data, to reduce the attack surface and prevent lateral movement of threats. Specifically, it secures infrastructures by allowing only specific traffic and, by default, denying everything else [29].

- **Identity-Centric Security:** IAM ensures secure access across organizations; its integration into ZTA demonstrated an enhancement of security in the critical phase of the continuous identity verification procedure. To be effective in ZTA, it has to leverage real-time adaptive policies, to evaluate legitimacy of accesses. It often integrates with Multi Factor Authentication (MFA) and Role Based Access Control (RBAC) which supports the IAM system and help in granting access. While the first takes place when attempting to log into computer resources, the latter aims to restrict access only to authorized users that fall into specific roles, according to their responsibilities. The IAM system is composed of the following:

  - **Configuration Phase:** system administrators need to set up access rights, define roles and permission, to be part of a policy that controls who can access specific resources.

- **Operational Phase:** it is the process in which authentication is referenced against the established configurations and the user is allowed to perform its intention.

These two phases are crucial to handle permission and can be visualized in the Fig.3.2.

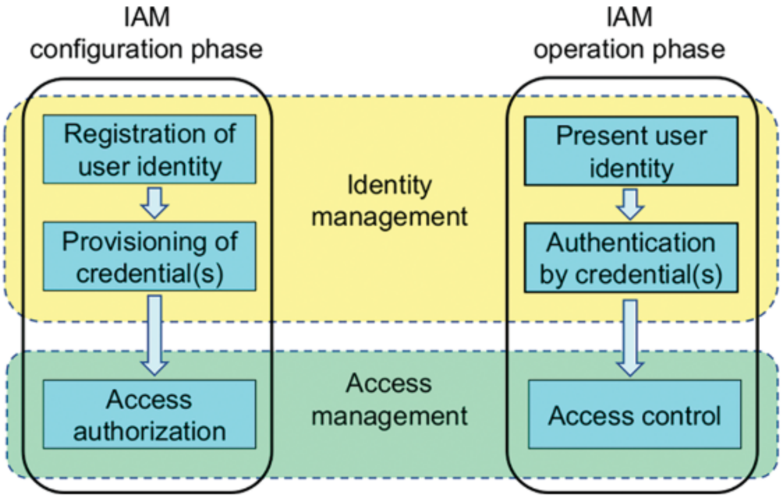


Figure 3.2: IAM phases [30]

- **Continuous Diagnostic and Mitigation (CDM):** protects against adversaries, using a risk-based and cost-effective solution, to deliver better visibility and awareness across networks. With real-time and automated reporting capabilities, CDM allows to monitor and manage the threat of any vulnerability, to identify who and what is on the network and how data is being protected. CDM allowed to move away from hardened perimeter security mindset, smoothing the transition to a non-implicit access environment, and so ZTA [31].
- **Visibility and Analytics:** while visibility enhances the detection of anomalous behaviors, analytics provides statuses on health, perfomance and behavior, by analyzing telemetry or logs. These two pillar allow the dynamism of policies and ease

the real-time decision making process by facilitating the analysis of events and activities and by ensuring that detection and response will be faster and meaningful. Together with automation and governance, it is the foundation for ZTA.

3.4 Zero Trust Maturity

ZTA is a gradual and ongoing journey. As described, it is also based on multilayers and requires a structured adoption process. Indeed, as depicted in the figure below, achieving such a robust security model depends on securing Identities, Devices, Networks, Applications and Data. All these columns advance through different maturity levels, that as can be seen on the left part of the picture, range from traditional perimeter-based state to an optimal state of continuous monitoring and mitigation. As previously mentioned, the foundations of this models are Visibility and Analytics, Automation and Orchestration and Governance which guide towards the accomplishment of a Zero Trust Maturity. Within the ZTA framework, maturity is reached when basic security measures advance and improve drastically, until an advanced or optimal state of automation, analytics, and dynamic enforcement of policies. It reflects the ability of responding to cyber threats with efficiency and precision, to proactively drive intelligent security strategies and maintain business continuity and integrity [32].

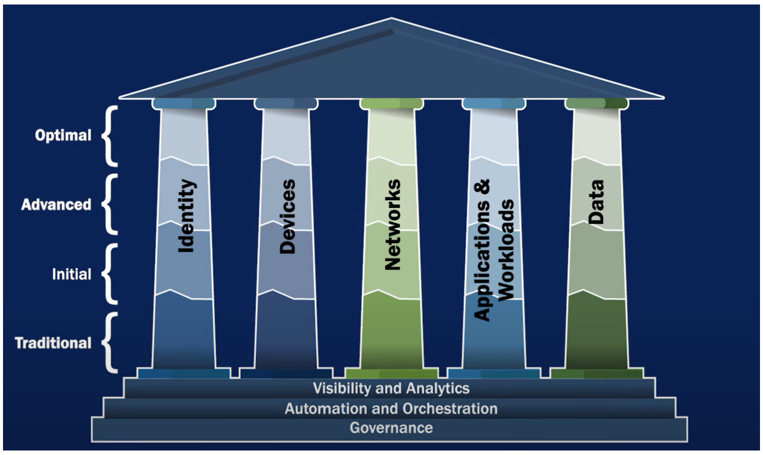


Figure 3.3: ZTA pillars [31]

3.5 Benefits and Challenges of ZTA

To enhance the security strength and succeed in this journey, several aspects must be considered. Below, a representation of the process of implementing Zero Trust Architecture within an organization. In addition to the aforementioned phases, the cultural challenge becomes an important actor.

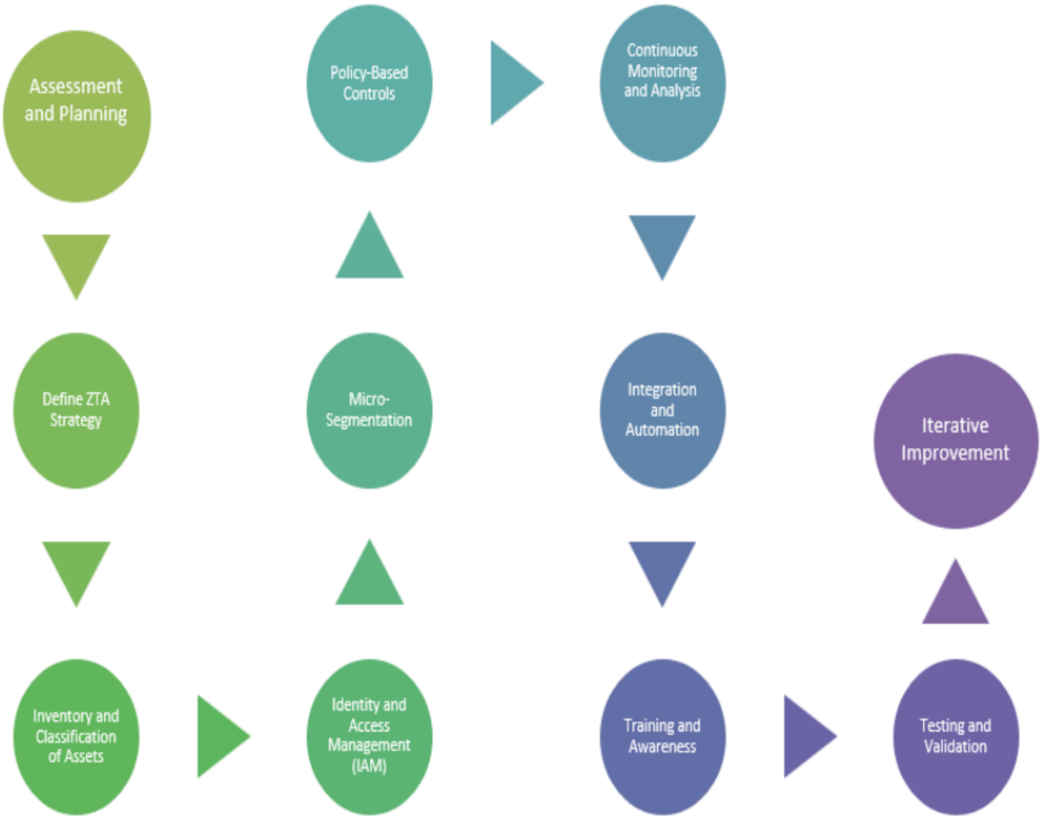


Figure 3.4: Process of ZTA [23]

This drastic change fosters awareness and accountability. On top of that, there is the need of assessing the compatibility of new solutions within the existing infrastructure, which often leads to migrations and transitions from legacy equipment in conjunction with legacy security models to newer solutions. If this evolution goes through successfully, the benefits that derives from it would be massive. The attack surface would significantly shrink, and insider threats diminish. Thanks to the pro-activeness in mitigating risks, together with the micro-segmentation, and least privilege access principles, companies would become compliant with standards and regulations. The efficiency that derives from ZTA adoption would be "up to speed" as well as up to date. The costs incurred in securing organizations would stabilize and reduce after reaching maturity; undeniably, it would allow improved and advanced data and threat protection with strong remote access security.

3.5.1 Applications and Considerations of ZTA

This architecture has been implemented worldwide by several players in all sectors. Today, being secure is a prerogative and the need to keep up with the latest and better security principles is a must. Cisco is an example of this adoption; it developed and implemented a holistic and transparent ZT model, focusing on continuous verification and strict access control methodologies, with the use of Single Sing On (SSO) which enables multi-application authentication, avoiding interference with user experience. Their motto, indeed, is "frustrate attackers, not users"; their implementation is divided into four key functions: (i) establish trust, by authenticating each user, device, and service entity, (ii) enforce trust-based access, (iii) continuously verify trust, looking for unusual behavior and predetermined red flags, and (iv) if there is a potential compromise, quickly respond to changes in trust. The biggest challenge for companies is how to implement this approach into a diverse and multi-information technology environment, to overcome the well-known "Security vs. Productivity" trade-off. Here, players like Cisco come into play, helping organizations implementing a scalable and adaptable model, that integrates within diverse ecosystems [34].

As we will discuss in the next chapter, the IoT is a crucial area where the adoption of ZTA is gaining momentum and we will analyze its implementation in constraied networks. The ZT principles need to extend within this realm, as they play a decisive role in preventing unauthorized access and identifying compromised devices that represent a risk for sensitive data.

Chapter 4

Applying ZTA to Constrained Networks

In the previous chapters, we understood why ZTA has gained interest in the last years and what the challenges it solves. In this section, we are going to evaluate what is ZTA in the context of IoT and what are its main challenges.

4.1 Initial considerations

Since traditional security models, based on a fixed perimeter, are not able to cope with the IoT dynamism and with the establishment of a secure boundary, Zero Trust Architecture (ZTA) is becoming more and more important. The application of ZT is a challenge due to the natural complexity and the steady evolution of IT environments. Especially within IoT, security policies need to be adaptable and capable of adjusting to changes in real-time; indeed, smart devices transition between networks, and dynamically change their status due to network interference, mobility, power optimization strategies, and a variety of different communication protocols.

IoT devices are limited in terms of resources, making it challenging for zero-trust models to continue authenticating and monitoring. Interoperability is also tricky; IoT devices come from different manufacturers, use different communication protocols, and have their own default security measures. Traditional security methods, which assume a static and controlled environment, cannot keep up with this level of dynamism. [35]

4.2 Emerging Technologies in IoT

The fast-changing landscape in the IoT era requires a new security strategy. As companies build more connected ecosystems, integrating devices from different vendors and engaging in various collaborations, the importance of a security model like Zero Trust becomes clear. Zero Trust's flexible approach ensures that security measures adapt to the fast pace of changes, protecting sensitive data and critical assets in an ever-growing IoT environment. Old security models cannot follow this speed, often making IoT devices open to new threats. Zero Trust, with its flexible and smart approach, become indispensable, giving central importance to proactivity and robustness against evolving threats in this ever-changing environment. In the IoT world, technology moves and evolves fast. The quick adoption of new technologies, like, for example, Machine Learning (ML) or Artificial Intelligence (AI), introduce both new opportunities and security risks. For instance, anomalous behavior or malicious activities in network traffic can be easily detected, vast amounts of data can be analyzed to discover threats and automatic policy configurations can enhance complex rules establishment by minimizing time and effort [36]. As the IoT expands, to enhance scalability, analytics and data processing, this ecosystem started to converge from local data processing to a scalable cloud-based systems. This represented a shift towards external cloud infrastructure with annexed challenges such as expanded attack surface, and privacy risk from the handling of data from third parties [37].

4.3 Cloud-based ZT system

When it comes to cloud-based zero-trusted systems, different are the approaches suggested to implement ZT for cloud-based systems.

The earliest ZT implementations are transport-level access control. This approach prevents unauthorized traffic from entering sessions, and checks the first packet coming from a user to confirm identity before a session is established.

While useful in analyzing early packets, this method has key limitations:

- **Resource Intensiveness:** extra computational overhead;
- **Session Hijacking Risks:** TCP reliance highlights vulnerabilities [38].

Another approach considers scenarios where both data and control planes may be compromised, in the so-called survivable Zero Trust framework. It is comprised of three main components:

- **Trust Engine:** verifies access requests and enforces granular security policies,
- **Fault-Tolerant Controller:** maintains network operations despite failures or intrusions;
- **Survivable Data Plane:** provides a secure communication channel, even under adverse conditions [39].

Current research focuses on micro-segmentation which divides a network into smaller, isolated segments, each governed by distinct policies. Most of the time it is combined with encryption and strict access control to enhance security posture in the cloud.

ML or AI are also exploited to detect threats and respond in real-time, underlining the necessity of adaptive measures in modern networks.

In cloud-based systems, combining various approaches might be beneficial for security but introduces computational overhead, potential delays in communication, and increased costs related to the enforcement of policies. Although these approaches we saw would be favorable and valuable, this added complexity must be taken into account. As network segmentation and encryption are used more and more, challenges arise especially within constrained networks; the trade-off between strong security and efficiency still applies and persists [38].

This problem might be solved by Software Defined Networks (SDN) which is a flexible and easy to manage architecture that delivers centralized control, automation and policy enforcement [40]. SDN would be helpful in implementing adaptable ZTAs, especially useful for what concerns IoT merged within cloud services. SDN would ease the enforcement of access policies and ZT principles in micro-segmented environment, and thanks to AI-driven mechanisms, to dynamically adapt to emerging threats within all the optimized network micro-segments [38].

4.4 IoT-based ZT

As previously mentioned, IoT converges together the physical and the digital world. This transformative technology creates a smart ecosystem where everything communicates autonomously and triggers actions. Considering the unique IoT characteristics to ensure the successful implementation of ZTA in IoT systems, we need to rethink access control architectures, policy models, and mechanisms to continuously validate every device, user or service that needs to access resources and to automate security decisions.

4.4.1 Foundational Approaches in ZT for IoT

In this subsection, we are going to explore the key approaches to implement ZT in IoT environments, which address its unique challenges thanks to various strategies that can be explored, and eventually adopted.

When a huge amount of heterogeneous constrained nodes are connected over the internet, a proposed framework called the Enterprise Internet of Things (E-IoT), integrates two major components:

- **Lightweight Cryptography-Based Secure Transmission:** ensure data integrity and confidentiality minimizing the burden on constrained devices resources;

- **Machine Learning-Based Intrusion Detection:** identifies malicious activities thanks to real-time analysis. [38].

Another proposed approach is the hierarchical management ZT for IoT, which assigns different roles to three key components:

- **Policy Manager:** defines high-level security rules;

- **Attribute Authority:** manage security attributes for devices.

- **Policy Enforcement Point:** real-time authorization based on the assigned attributes [38].

The hierarchical design limits unauthorized access and help reduce tampering of data, but it might introduce additional overhead in large-scale IoT deployment [38].

As IoT extends across several domains, each of which demands for consistent security, with these proposed approaches challenges persist and, besides the computational overhead that induces performance issue and latency, important is to determine which approach should be adopted and why. Since the complexity of policy management has to be minimized and the trade-off between security and operability has to remain beneficial, we can rely on different frameworks proposed.

4.5 Advancing ZT Framework towards IoT

To provide a structured approach to the authorization policy model in ZT systems, with a focus on the requirements of access control within the IoT, different frameworks have been devised. These frameworks derive from the fundamental principles of ZT NIST special publication [27] that represent the basic idea or goal of ZT but it is not possible to be implemented in every system. The NIST publication served as the primary reference and guideline for the development of new frameworks specific for IoT.

4.5.1 ZT-ARF: Zero Trust Authorization Requirements Framework

The Zero Trust Authorization Requirements Framework (ZT-ARF) is a structured framework to define how authorization policies work. The framework divides authorization needs into seven main parts that help designers to shape policies that fit specific situations, risks, and demands. ZT-ARF focuses on operational authorization policies, considering actor characteristics as mandatory. These characteristics include identity, clearance, roles, trust level, and location. In systems where actors (devices, applications, or automated services) request access, their characteristics are also considered part of the actor's profile. The more components are included in an authorization representation of the profile, the closer it aligns with the objectives of ZT.

The elements that ZT-ARF highlights are decisive for decisions in ZT setups. They can be observed Fig 4.1. and described below.

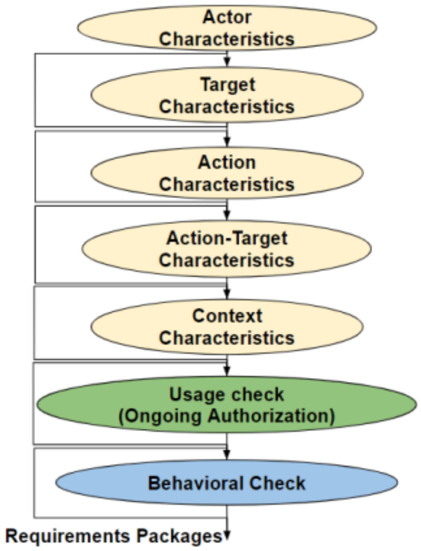


Figure 4.1: ZT-ARF [41]

- **Actor Characteristics:** entities that initiate the access request. They represent the actor's properties such as ID, clearance, roles, trust level and location; these properties are considered part of the actor's characteristics;

- **Target Characteristics:** resources needed to to access the request. Targets are associated with characteristics, and might include information such as, files or directories of an operating system, rows or columns within a database management system;

- **Action Characteristics:** programs that, once invoked, perform specific actions on behalf of the actor;

- **Action-Target Characteristics:** actions are associated with targets, which needs to capture characteristics, for example the lever of danger of an action;

- **Context Characteristics:** combine environment information, in example the operating system version, with telemetry and status of threats. Telemetry and threats information include information on the different assets or the network infrastructure;

- **Usage Check:** dynamic authorization in ZT systems. If any access requirement or characteristics change during the access, the authorization system revokes the granted access and modifies the no longer satisfied security policy accordingly;

- **Behavioral Check:** how different components part of the system behave.

In the first five characteristics, we can distinguish between two types: (i) static, and (ii) dynamic, depending if these characteristics are going to change or not over time [41].

4.5.2 ZT Authorization in IoT

In this subsection we are going to analyze the authorization requirements for IoT and understand which component of the ZT-ARF could be considered in designing ZT access control models for IoT. For what concerns authorization models in IoT systems, when designing access control models, it is necessary to consider the following requirements:

- **Dynamic Authorization:** grant or revoke access dynamically, based on the contextual characteristics;

- **Fine-grained Authorization:** enables selecting control over subsets of the same action, mitigating the risk from unsafe operations. An example is the home security system in which a user might be allowed to view camera videos, but not allowed to download the recordings;

- **Suitable for constrained smart devices:** the model should not require extensive computation overhead;

- **Scalability:** to integrate a large number of devices;

- **Privacy-Preserving:** the access control model should safeguard privacy, allowing users to decide to share data only if required [42].

In IoT, different actors communicate within some specific scope, in example smart home ecosystems, or healthcare monitoring systems. As the scope is composed of synchronous and interconnected interactions, there is the need to take into account contextual awareness of policies and the ability to manage the entire life-cycle of the multiple and often concurrent and continuous authorizing sessions. Usage control, as explained in the following subsection, can solve this issue.

4.5.3 Usage Control (UCON)

To extend traditional access control and, as mentioned earlier, to uniform the control mechanism and so regulate access and use of resources throughout the whole life-cycle of IoT devices, the Usage Control (UCON) framework allows for a continuous enforcement of policies. UCON was introduced to cope with the failure of reacting to contextual situation changes from existing IAM technologies or access control models, such as Attribute-Based Access Control (ABAC) [43]. The latter is also known as policy-based access control for IAM and grants access based on attributes or policies [44]. UCON+ is an improvement of UCON framework that continuously monitors and controls before granting or revoking authorization, taking into account decision factors such as trust or threat levels. UCON+ encompasses three different phases (i) Pre-Authorization Phase, (ii) Ongoing authorization Phase, and (iii) Post Access Phase, providing a robust mechanism throughout the entire life-cycle of authorization, enhancing security and dynamic adaptability [45]. UCON+ is composed of:

- **Attributes:** property of a resource that influences authorization decision (i.e. CPU load);
- **Phases:** the above mentioned stages of authorization;
- **Rules:** conditions based on attributes, that need to be re-evaluated at each attribute value change;
- **Decisions:** outcome based on rules i.e. Permit or Deny
- **Instructions:** final action enforced. [43]

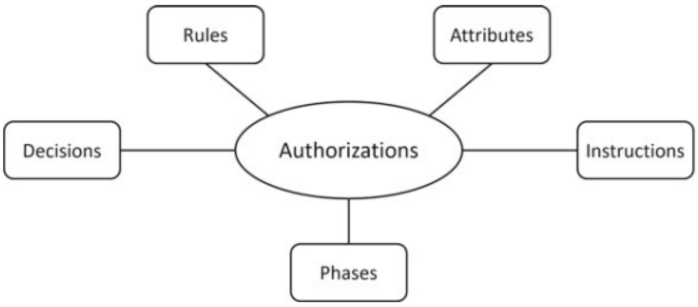


Figure 4.2: UCON components [43]

UCON+ model has been adapted for the IoT because of its benefits in operating in dynamic and distributed contexts. In the IoT context, UCON+ integrates:

- **Authorization (A):** determine if a Subject (S) which is the property of a resource that influences authorization decision (i.e. CPU load), is permitted to access an Object (O);

- **oBligation (B):** actions needed to be performed i.e. updating its firmware before accessing a certain resource;

- **Condition (C):** environmental or system requirements that have to be satisfied to grant access i.e. Network aware access control, based on processing power, memory or bandwidth [46].

UCON+ ensures that decisions to grant or revoke authorizing are continuously taken and updated based on real-time information, in order to enhance overall security, adaptability and policy enforcement within IoT ecosystems.

4.6 ZTA-IoT: Zero Trust Architecture for IoT

So far, we discussed and explored how ZT frameworks, such as ZT-ARF and UCON+ adapted to contribute in securing IoT environments and enables dynamic and context-aware authorization policies. However, the implementation of ZT within IoT, requires a more structured approach, to consider specific challenges of constrained networks, real-time adaptability, and interoperability. This section introduces the concept of Zero Trust Architecture for IoT (ZTA-IoT), a security model that primarily focuses on integrating ZT principles into cloud-enabled IoT systems.

This proposed architecture makes clear the fundamental distinction between the data plane and control plane as can be seen in Fig. 4.3. While the right side of the Fig. represent the control plan and so the policy decision layer, the left side represents the data plane, depicted as what would be the IoT architecture but adapted for a cloud-enabled IoT system.

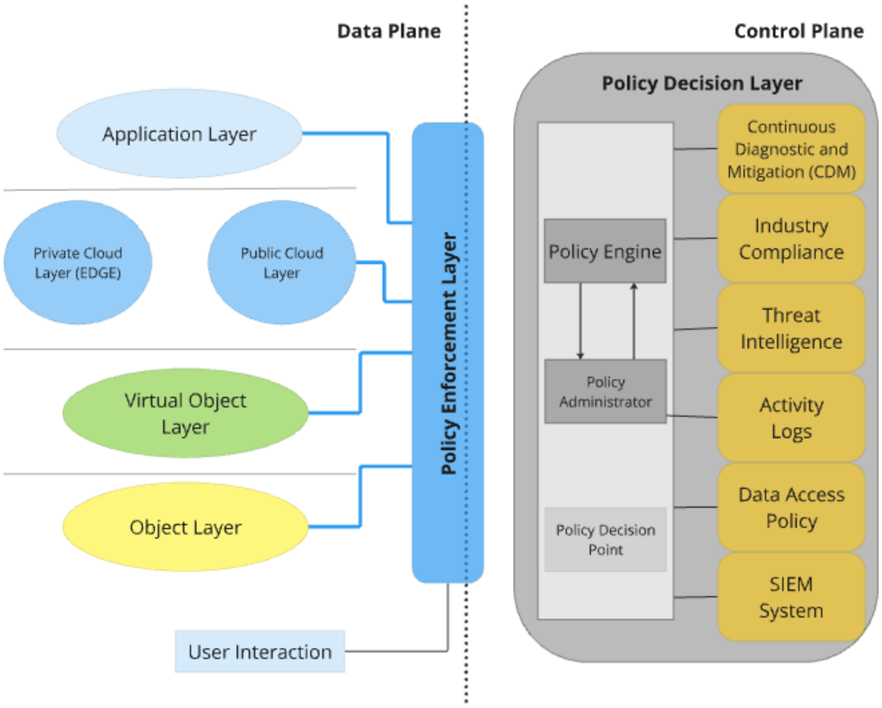


Figure 4.3: ZT architecture for IoT systems (ZTA-IoT) [42]

As can be observed, the ZTA-IoT architecture comprises four layers, namely (i) Object Layer, (ii) Virtual-Object Layer, (iii) Cloud Layer and (iv) Application Layer. All of these layers can interact with each other to exchange data and commands to accomplish specific tasks. As per ZT principles none of the components within the four layers is not inherently trusted. For communication to happen and so, to accomplish actions desired by the user, they must pass through ZT control plane components. Each communication must go through the policy enforcement layer and the policy decision layer; the former ensures that only accesses authorized by the latter are allowed. The outlines of the figure above are broken down in the following subsections.

4.6.1 Policy Enforcement Layer

The Policy Enforcement Layer enables all the interactions between IoT entities, across each layer. It is the manager of data and control planes and incorporates different Policy Enforcement Points (PEPs). PEPs communicate with the Policy Administrator to forward requests for decisions and receive policy updates. Each PEP is a mediator between sender and receiver and it is composed of:

- **Actor:** any kind of agent;
- **Target:** for example, a dedicated micro-service that enforces access controls in front of the resource.

4.6.2 Policy Decision Layer

This layer is made of the Policy Decision Point (PDP) which is composed of (i) the Policy Engine (PE), and (ii) Policy Administrator (PA). To support decisions, PDP uses multiple data sources that, as can be seen in the orange cells in the right part of the Fig. 4.3, are as follows:

- **Continuous Diagnostics and Mitigation (CDM) System:** real-time updates on the state of IoT nodes, including vulnerabilities. This system is able to recognize and enforce policies;
- **Industry Compliance System:** as the name suggests, it ensures adherence to industry standards;
- **Threat Intelligence:** insights regarding vulnerabilities and attacks;
- **Activity Logs:** information derived from telemetry that discloses insights regarding the system's security posture;

- **Data Access Policy:** attributes and authorization rules important for access control decisions;
- **Public Key Infrastructure (PKI):** manages certificates and cryptographic keys for IoT devices;
- **ID Management System:** manages identity records, including user/thing name, roles and attributes;
- **Security Information and Event Management (SIEM) System:** helps detect, monitor abnormal behaviors and analyze potential security threats.

While the PE is responsible for granting or denying access to a resource target by using the multiple data sources mentioned above, the PA establishes and terminates communication paths between an actor and a resource target by instructing relevant PEPs.

4.6.3 Object Layer

This layer includes sensors, actuators, and devices that can operate individually or as clusters. The goal is to gather and transmit data to upper architecture layers. They often have built-in applications (i.e. pressure monitoring) that can communicate with different objects to retrieve or update data, which will be subsequently sent to the cloud for further analysis.

4.6.4 Virtual Object Layer

This layer deals with digital replicas of the IoT objects. When the physical devices are connected to its virtual counterparts, it provides a current persistent status that can be updated according to the physical object availability. Virtual Objects (VOs) address various IoT challenges such as scalability, heterogeneity, security, privacy, and identification, as well as enabling seamless communication regardless of object differences and location. VOs can be associated with physical objects in various ways (one-to-one, many-to-one, or one-to-many) and facilitates the interactions between IoT objects and applications. Often, interfaces are present in this layer to allow users to easily communicate with objects and visualize the analyzed information. VOs can be created at the edge or in a central cloud.

4.6.5 Cloud Layer

This layer includes large aggregated public cloud platforms and local private edge cloud, in the Fig. 4.3 respectively referred as the Public Cloud Services Layer and Private Cloud Layer (Edge). This layer enables data storage, computation, and processing for large data collected from IoT objects, independently of the location. The data stored at this layer can be used intelligently for smart monitoring and actuation, and it can also be represented and visualized in meaningful ways for the users. Multiple cloud platforms can also communicate to share information at a broad level and pursue common goals. The cloud services running at this layer can access information and data from virtual objects.

4.6.6 Application Layer

Application Layer delivers services and system functionalities to the end users. It offers an interface where users can easily interact with objects and visualize the analyzed information. Physical objects communicate with virtual objects, which in turn push these data to the cloud where applications can access it. [42]

4.7 ZT Implementation - Key Takeaways

Zero Trust has become essential for IoT environments. Traditional perimeter-based strategies fail to address the unique challenges of IoT of limited computing resources and real-time operational needs. To be effective, ZT in IoT must incorporate strategies such as lightweight cryptography, micro-segmentation, or AI threat detection. Most importantly, continuous policy enforcement mechanisms have to be optimized for IoT environment; we analyzed how UCON+ framework helps to adapt to changes in context or attributes, by taking authorization decisions. Likewise, the Zero Trust Authorization Requirements Framework (ZT-ARF) clarifies how critical characteristics define access control. ZT-ARF ensures adaptive and context aware authorization, enablig real-time policy adjustments with annex resilience against evolving threats.

Finally, with the proposed Zero Trust Architecture for IoT (ZTA-IoT) we highlighted the need to distinguish between data and control planes. By placing policy enforcement and policy decision points at the heart of IoT communication, ZTA-IoT ensures continuous visibility and control over every layer, from the physical devices to the cloud and back. These components collectively enable IoT ecosystems to securely accommodate device diversity and increasing data volume, ensuring that every request is verified before access is granted.

Chapter 5

Conclusions

With this dissertation we examined the Zero Trust Architecture (ZTA), how it evolved from traditional security approaches, and how can be applicable for Internet of Things (IoT) ecosystem. The whole picture of ZTA emerged through the analysis of fundamental principles and existing frameworks, with the aim of setting the foundations to secure dynamic topologies, made up of constrained devices, with their unique characteristics and vulnerabilities.

5.1 Key Findings

After we describe the constrained networks, their widespread connectivity, and their lack of security, we highlighted how traditional trust models are inadequate for such evolving and dynamic environments. The need for a more flexible and trust-based strategy arose. We analyzed how the perception of trust evolved over time, shifting from assuming it inherently and unconditionally to continuously verifying each interaction. Zero Trust principles redefined the security boundaries, and represents the shift towards a dynamic and context-aware approach. Thanks to the least privilege access, micro-segmentation, and continuous authentication principles, communication can be examined before access is granted. Building on these principles, we analyzed different frameworks, such as ZT-ARF that established the parameters for adaptive authorization decisions and UCON+ which emerged as a valuable tool for continuous verification.

These frameworks led to ZTA-IoT, which integrates various principles explored within this dissertation into a holistic approach with the goal of implementing a context-based policy and ensuring that any kind of constrained node can be protected.

Zero Trust Architecture in constrained networks represents not only a robust model that sets the basis for an innovative future but also implements a security-first culture, towards a challenging yet necessary journey. By applying these principles and frameworks, the risks posed by a constantly expanding attack surface can be mitigated while still unleashing the transformative potential of IoT.

Bibliography

[1] T. Zaid, S. Garai - Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers

[2]] J. Katariya - A Comprehensive Guide to IoT Protocols and Standards - Moon Technolabs - February 2025

[3] C. Gomez, A. Arcia-Moret, J.Crowcroft - TCP in the Internet of Things: From Ostracism to Prominence - February 2018

[4] Tarik Eltaeib - TCP/IP PROTOCOL LAYERING - Farmingdale State College - January 2015

[5] W. Shang, Y. Yu, L. Zhang, R. Droms - Challenges in IoT Networking via TCP/IP Architecture - 10/02/2016

[6] M. Weiser - The Computer for the 21st Century - July 1999

[7] K. L Lueth - Top 10 IoT Applications in 2020 - IOT ANALYTICS

[8] S. Inamdar, S. Roy - Internet of Things: Architecture, security and Applications - International Journal of Advanced Engineering and Management - 2017

[9] E. Dzaderovic, A. Sokol, A. A. Almisreb, S. M. Norzeli - DoS and DDoS vulnerability of IoT: A review - June 2019

[10] J. Wang, C. Liu, L. Zhou, L. Tian, X. Yu - Early Detection Of Node Capture Attack in the Internet of Things - December 2021

[11] S. Skorobogatov - How microprobing can attack encrypted memory - University of Cambridge, Computer Laboratory

[12] B. Mbarek, M. Soula, T. Pitner, A. Meddeb - An Effective Replica Node Detection Scheme in Internet of Things Network - International Wireless Communication and Mobile Computing (IWCMC) - 2023

[13] M. Msgna - Anatomy of attacks on IoT Systems: review of attacks, impacts and countermeasures - December 2022

[14] Unit 42 IoT Threat Report - 2020

[15] P. Fremante, P. Scott - A security survey of middleware for the Internet of Things - January 2015

[16] S. N. Firdous, Z. Baig, C. Valli, A. Ibrahim - Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol - June 2017

[17] HiveMQ Team - MQTT Packets: A Comprehensive Guide - July 2024

[18] OASIS Standard - MQTT Version 3.1.1 - October 2014

[19] T. Mazhar, D. B. Talpur, T. Al Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, H. Hamam - Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence - April 2023

[20] N. A. Khan, A. Awang, S. A. B. A. Karim - Security in Internet of Things: A Review - Yayasan Universiti Teknologi PETRONAS (UTP) - January 2022

[21] Zscaler - Underscoring Need for Better Zero Trust Security to Protect Critical Infrastructures - October 2023

[22] FBI - Internet Crime Complaint Center - 2023

[23] G. Nagar, A. Manoharan - ZERO TRUST ARCHITECTURE: REDEFINING SECURITY PARADIGMS IN THE DIGITAL AGE - International Research Journal of Modernization in Engineering Technology and Science - March 2022

[24] R. Alsaqour, A. Majrashi, M. Alreedi, K. Alomar, M. Abdelhaq - Defense in Depth: Multilayer of Security - International Journal of Communication Networks and Information Security (IJCNIS) - August 2021

[25] NSA - Embracing a Zero Trust Security Model - February 2021

[26] T. Muhammad, M. T. Munir, M. Z. Munir, M. W. Zafar - Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future - International Journal of Computer Science and Technology (IJCST) - 2017

[27] S. Rose, O. Borchert, S. Mitchell, S. Connelly - NIST Special Publication 800-207 - Zero Trust Architecture - 2020

[28] NIST glossary

[29] CISCO - What Is Micro-Segmentation?

[30] C.Singh, R. Thakkar, J. Warraich - IAM Identity Access Management-Importance in Maintaining Security Systems within Organizations - 2023

[31] America's Cyber Defense Agency - National Coordinator For Critical Infrastructure Security and Resilience

[32] NSA - Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar - May 2024

[33] DETECTX — Cloud Security Expert - rockstarL - Cyber Kill Chain - February 2020

[34] Cisco - Zero Trust solutions - How Cisco enables zero trust security - 2025

[35] H. Kang, G. Liu, Q. Wang, L. Meng, J. Liu - Theory and Application of Zero Trust Security: A Brief Survey - November 2023

[36] C. Liu, R. Tan, Y. Wu, Y. Feng, Z. Jin, F. Zhang, Y. Liu, Q. Liu. - Dissecting zero trust: research landscape and its implementation in IoT - 2024

[37] N. Singh, R. Buyya, H. Kim - Securing Cloud-Based Internet of Things: Challenges and Mitigations - December 2024

[38] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, Y. H. Ahmed - Verify and trust: A multidimensional survey of zero-trust security in the age of IoT - 2024

[39] L. Ferretti, F. Magnanini, M. Andreolini, M. Colajanni - Survivable zero trust for cloud computing environments - November 2021

[40] Cisco - Software-Defined Networking

[41] S. Ameer, S. Bhatt, M. Gupta, R. Sandhu - BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems - 2022

[42] S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, M. Gupta ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Mode

[43] A. Hariri, A. Ibrahim, B. Alangot, S. Bandopadhyay, A. La Marra, A. Rosetti, H. Joumaa, T. Dimitrakos - UCON+: Comprehensive Model, Architecture and Implementation for Usage Control and Continuous Authorization - 2023

[44] Wikipedia - Attribute-based access control

[45] U.Ghazia, M. A. Shibli, R. Masood, M. Bilal - Usage Control Model Specification in XACML Policy Language - Policy Engine of UCON

[46] A. K. Malik, N. Emmanuel, S. Zafar, H. A. Khattak, B. Raza, S. Khan, A. H. Al-Bayatti, M. O. Alassafi, A. S. Alfakeeh, and M. A. Alqarni - From Conventional to State-of-the-Art IoT Access Control Models - 2020

Ringraziamenti

Alla fine del mio percorso universitario, un'avventura di crescita e scoperta, fatta di cambiamenti e realizzazioni.

Ai miei genitori, per avermi trasmesso determinazione e perseveranza.

Ai miei fratelli, fonte inesauribile di ispirazione ed esempio.

Ai miei zii e cugini, che sanno sempre incoraggiare e alleggerire il peso delle difficoltá.

Alla mia fidanzata, per il supporto incondizionato e per la grande gioia portata.

Ai miei amici, preziosi compagni di viaggio, per aver reso tutto memorabile.

Vi ringrazio di cuore.