innovation forward

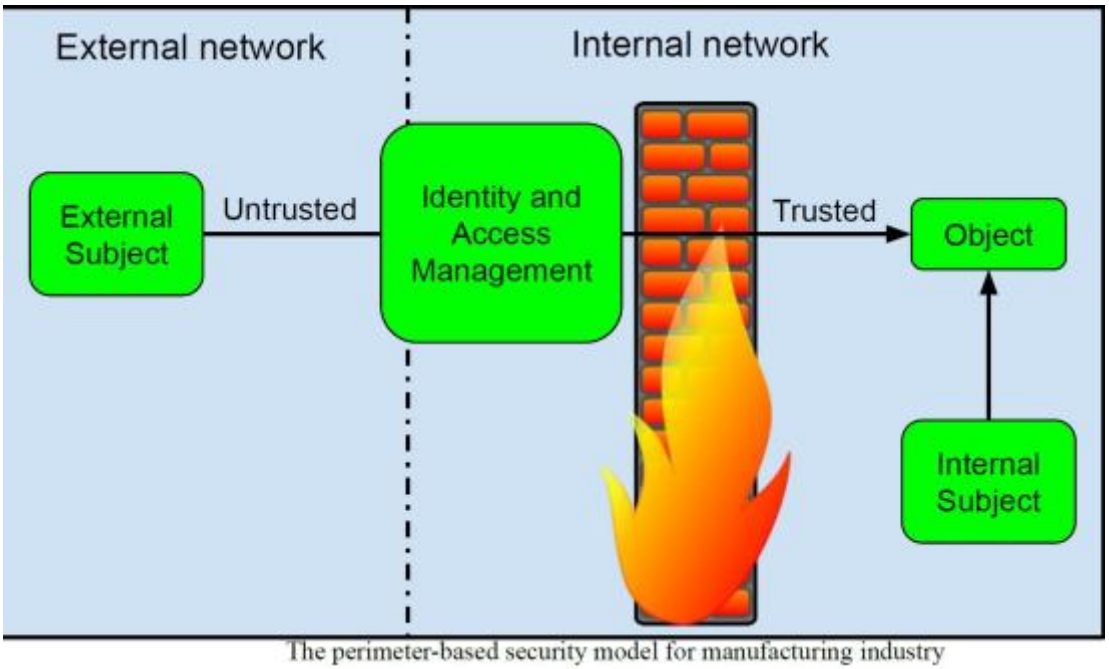
Zero Trust - towards a secure smart manufacturing architecture

10 February 2023, 12:08

Farhad Aghili

Rooted in the principle of “never trust, always verify", Zero Trust represents a strategic approach to cybersecurity that strives to maintain an organization's digital security by eliminating implicit trust and continuously validating every stage from the creation of a digital interaction until its completion.

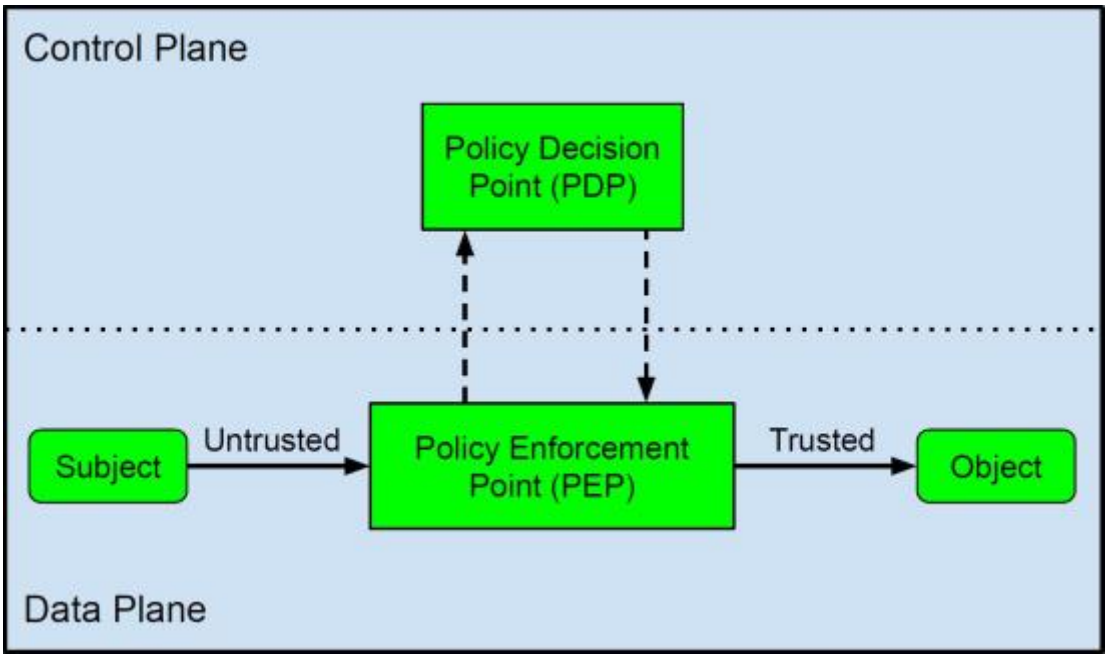
Traditional smart manufacturing industry security architectures use a **perimeter-based security model** where operators located in the internal network are considered trustworthy by default. As a result, they can access internal enterprise resources. The perimeter-based security protects external networks with a firewall, an intrusion prevention system (IPS), etc. Thus, users located on external networks must be authenticated before they can be trusted. In addition, once authenticated, a user is trusted for a long time and can access internal enterprise resources if authorized.



The perimeter-based security model for manufacturing industry

Hence, in this approach, once an adversary gains access to the internal network (e.g., by compromising a trusted operator/identity), it becomes easy for them to access internal resources in the same way as legitimate users. Moreover, an adversary who has gained access to the internal network is able to move laterally throughout the network and compromise other critical hosts, servers, infrastructure. VMware Report 2022: Lateral movement was seen in 25% of all attacks.

Conversely, **Zero-Trust** (ZT) is based on the concept of never trusting and always verifying. In this way, ZT applies the same security checking and access control to internal and external users. ZT also limits internal lateral movement by controlling the data bridge and validating every access per session. The access control model used in ZT employs not only static policies but also dynamic policies taking into account users, accessed resources and environmental attributes such as the location where the access request originated. **Additionally, it is essential to match the risk with the level of trust assigned to a particular user or device that wants to access specific resources**. The logical view of ZT for an enterprise system is illustrated in the figure below.



Access control models

To design a ZT architecture (ZTA), **identity authentication**, **access control**, and **trust evaluation** algorithms should be well thought of. A review of the access control models that may (or may not) be appropriate for the smart manufacturing industry domain is required in ZTA. It is imperative to stress that there should be access control for both users and devices. More precisely, the ZT system needs to monitor different devices trying to access the smart manufacturing network and ensure that each device is authorized.

Specifically, the smart manufacturing industry uses either local servers or cloud systems to store information and system entities (users, devices). Entities are able to access this data with some pre-defined access control rules and perform specific actions (e.g., data analytics, ML, AI). These mechanisms use static access control models (i.e., defined once - used many times) such as Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Mandatory Access Control (MAC). As mentioned earlier, ZT is based on the premise of "never trust and always verify" and user trust must always be commensurate with risk and dynamic policy. Thus, access control models based on pre-defined access control rules are not suited for use in ZTA.

Another well-known access control model that has been widely used recently is the **Attribute-Based Access Contro**l (ABAC) which is an excellent alternative solution to RBAC. With ABAC, access is granted to a user/device if and only if it meets the model's attributes. The Basic ABAC model relies only on pre-defined static attributes such as “identity”, “role", and so on. The problems with this model are (1) that there is no real-time verification and (2) the user mobile device stores all the static attributes inside the device. Using the full potential of ABAC, more specifically, by using both static and dynamic attributes derived from user behaviour (e.g., "time" and "location"), the model can now always verify the behaviour to be granted access. In addition to what is mentioned above, the access control model used for ZT must consider the user or network's recent history into account during access requests evaluation.

Given a smart manufacturing's dynamic environment, and the fact that the ZT system requires real-time decision-making capabilities, a **risk-aware access control** model can be used to solve grant access problems based on action risk levels. Many factors can be considered in calculating risk, including contextual and environmental factors as well as the trustworthiness of the requesting user/device. Generally, the risk access control model consists of “risk factors”, “risk estimation”, and “access control module” elements. User clearance, accessed recourse sensitivity, action severity, risk history, user behavioural trust, benefits, outcomes of actions, and context features could be considered as a list of vital risk factors in the context of smart manufacturing. Risk estimation techniques for risk-based access control models could be based on fuzzy logic, machine learning, game theory, and risk assessment. However, the key problem in the context of smart manufacturing is the lack of a dataset to represent the likelihood and impact of each risk. By integrating a risk-aware access control model with an ABAC model where the risk factor is treated as an attribute, it can be used as a practical access control model to propose ZTA for the smart manufacturing industry.

On your way to secure and reliable ZTA

Over time, ZT architecture (e.g., the ZTA proposed by NIST in 2020) has been primarily applied to enterprise systems (most commercial offerings). However, ZT's deployment in operational technologies (OT) domains, such as smart manufacturing, is still in an early stage and many challenges regarding its principles, architecture, and implementation remain. Sirris experts with

deep knowledge of ZT models and smart manufacturing security architecture in a variety of areas will make your life easier. This will enable you to design a secure and reliable ZTA for your smart manufacturing industry.

Learn more on ZT models & practices:

- Our masterclass Masterclass Cybersecurity - Manufacturing | Sirris
- Our collaborative knowledge build-up / dissipation project Cybersecurity 4.0 | Strategic and case-specific cybersecurity - for Industry 4.0 in SMEs | Sirris

Sirris is currently coordinating several projects as well in this domain under the **EU ITEA** framework. If you would like to know more, contact us! New partners can still be added.

Authors

Farhad Aghili