Spoofing Protection

Introduction

In late 2014, a steel mill in Germany suffered massive damage as the result of a cyber attack that required advanced hacking skills, applied industrial control knowledge and endurance. No one has claimed responsibility for the attack and the lack of attribution and clear objective emphasize that not only are the threats very real, but anyone can become a target without apparent reason. This incident is only one of many examples of successful cyber attacks of industrial automation and control systems, and together with Stuxnet manifests the reality of cyber threats.

Unless you have experienced a serious security incident first hand, it is easy to believe such attacks only happens to someone else, but not having experienced such an incident however, does not mean you haven't been compromised. In fact, according to a report from KPMG from 2014, it is more likely than not that information is being exfiltrated by malware without your knowledge from your office networks. 14 companies were studied, and data was actively stolen from 10 of them without their knowledge.

The report is yet another strong indication traditional, best-practice defense like anti-virus, perimeter firewalls and network intrusion detection systems based on signatures are easily avoided. It also indicates insufficient organizational readiness as no action was taken even when malicious code was detected.

Westermo present a series of five basic applications assets owners can apply in their own networks to improve the security posture in a sustainable way.

Spoofing Protection

Spoofing in the context of networking is when an attacker manage to masquerade their devices to look like they are already existing and legitimate devices on the network. The most common attack using spoofing is man-in-the-middle, where the attacker manage to intercept communication between two or more devices without them knowing. This is possible because of some intrinsic weaknesses in the IP stack specifications.

One way to mitigate some of these attacks on a WeOS device is to enable port authentication 802.1x over RADIUS.

Protection

Enabling port authentication using 802.1x over RADIUS adds an important layer of defense as it require all devices that physically connect to a WeOS device to authenticate themselves using

credentials defined in a RADIUS server, usually in the same perimeter security zone.

Without the credentials, the connected device is not granted access to the network defined for the port it connects to which means all spoofing attacks are effectively mitigated.

Detection

Logging failed authentication attempts to an intrusion detection system is a good indication of either misconfiguration or potential attack. Either way, it is valuable information that should be acted upon.

Typical application

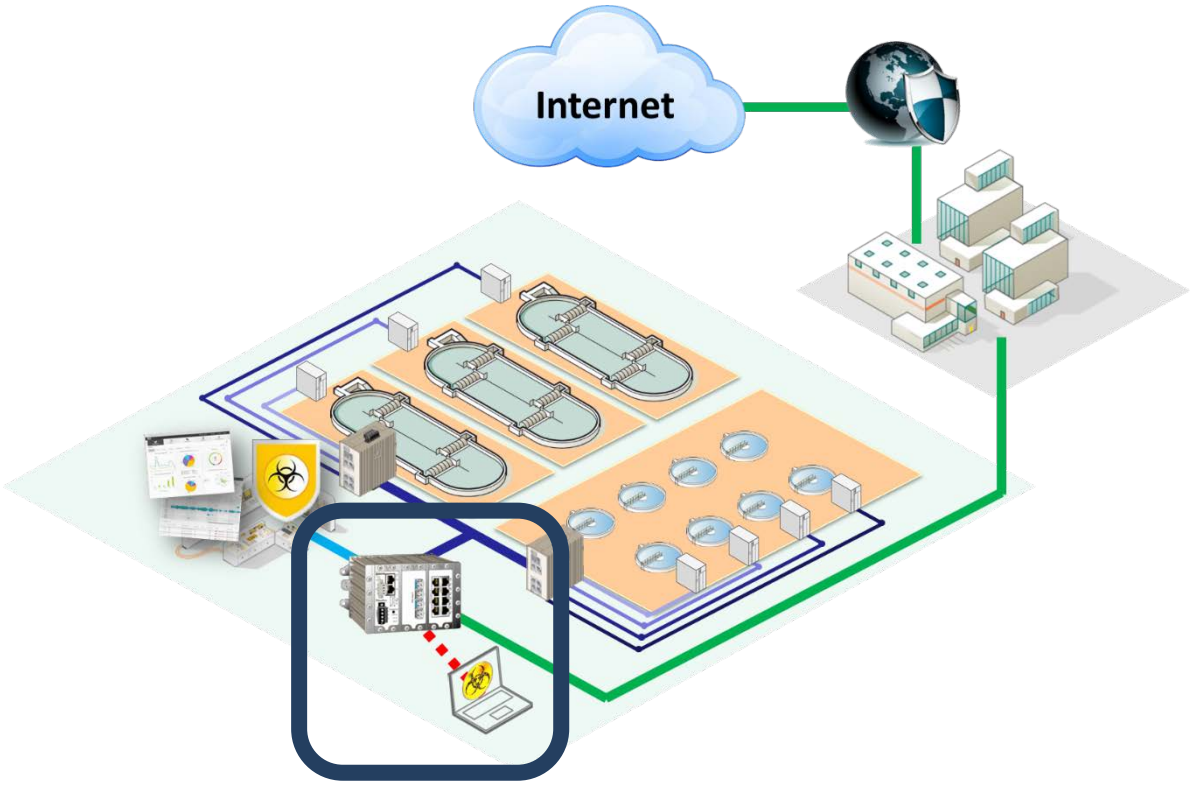

Figure 1 - Port authentication for the perimeter security zone

Modern industrial control systems usually have an authentication server, such as Active Directory that supports RADIUS, which can be used for authenticating devices as well. For systems that do not have a centralized authentication server, it is possible to install FreeRADIUS or similar open source RADIUS server for device authentication.

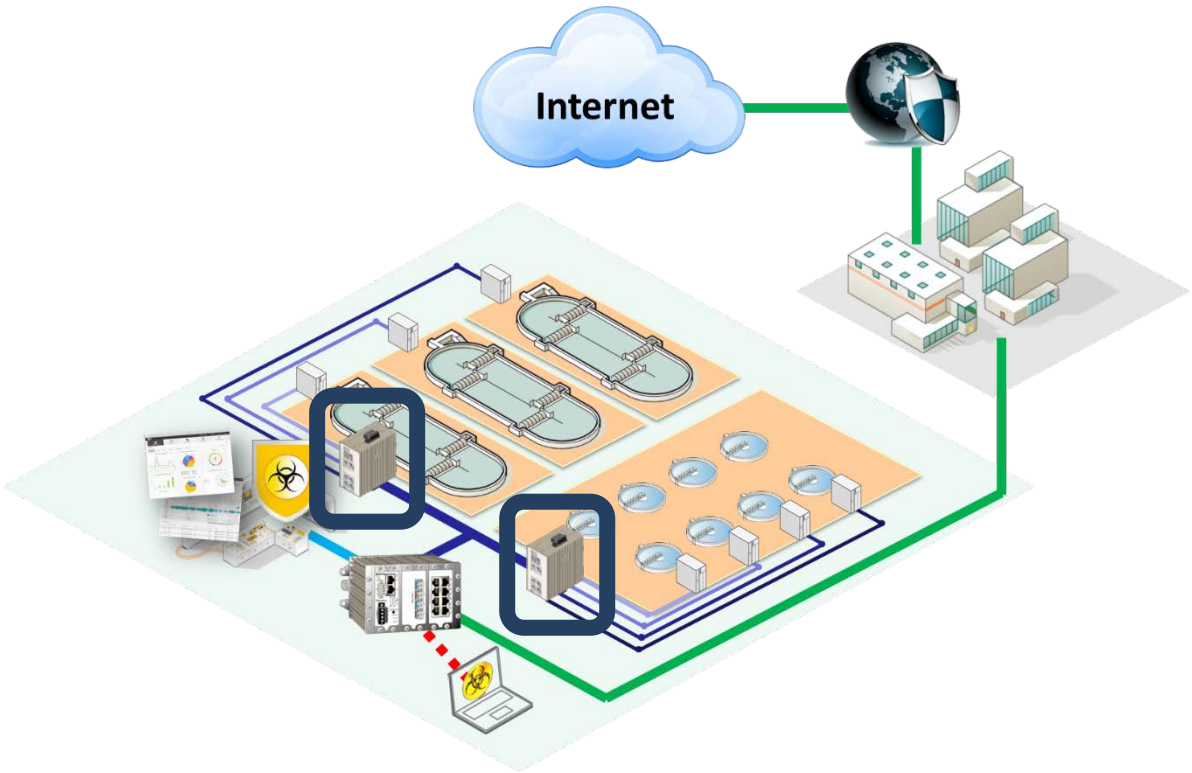

Figure 2 - Port authentication for control network security zones

Many industrial control systems have WeOS devices in secluded places where an attacker would be able to connect a rouge monitoring/tampering device. Implementing port authentication there would prevent such rouge devices and would alert an operator of the attempt if properly integrated with an intrusion detection system.