Automatic Risk Evaluation of Cyber-Attack Vectors

Defining attack-vector use cases according to attacker skill level

By Liron Benbenishti, cybersecurity researcher, Radiflow LTD

This paper discusses risk evaluation of attack vectors and applying Radiflow's cyber risk evaluation model, which is now incorporated into Radiflow's iSID Industrial Threat Detection System.

WHAT IS RISK EVALUATION AND WHY WOULD YOU NEED IT?

In general, OT networks have very high availability requirements. This makes asset patching a very complicated task, whether the patching is done for operational or cybersecurity purposes.

Therefore, prioritization of patching tasks is crucial for maintaining a strong and relevant cybersecurity posture. This calls for a risk model that takes into account parameters relevant to the organization.

Radiflow's risk model includes several characteristics and algorithms. This paper will focus on the effects of the cyber-attacker's capabilities and their potential lateral movement within the ICS network.

ATTACKER SKILL LEVEL

In a recent whitepaper, we explored and analyzed the different attacker capabilities, based on published cyber-incidents as well as data acquired during various Radiflow assessments (available at https://radiflow.com/download-whitepaper-meet-your-attacker-taxonomy-analysis-of-a-scada-attacker/).

The whitepaper classified attackers' capabilities using over ten properties. In this paper, I'll use a three-level categorization of attacker skills:

- "Script-kiddies" – this category of attacker uses malicious scripts, programs and various exploitation frameworks, widely available to anyone on the dark web, to attack computer systems and networks. These attackers are capable of exploiting only IT protocols and software by weaponization publicly available exploits and delivering them to the target. For th purpose of this article I'll call them "low level".
- Professional hackers with ICS capabilities – this category of attackers is characterized by their ability to exploit entire suites of both IT and ICS/OT protocols. The limitation for these groups is that they have no resources/capabilities to research and develop, or acquire zero-day OT vulnerabilities and exploits. Still, this attacker category ("medium-level") is capable of exploiting open-specification OT protocols and developing or acquiring its own exploits for published known vulnerabilities.
- Nation-state sponsored (APT) groups – this category of attacker is capable of performing long-term extensive research to find unknown (zero-day) vulnerabilities, and is also capable of exploiting them. Their research spans both IT and OT software and protocols including proprietary ones. Among their targets are critical national infrastructures, major manufacturers and others.

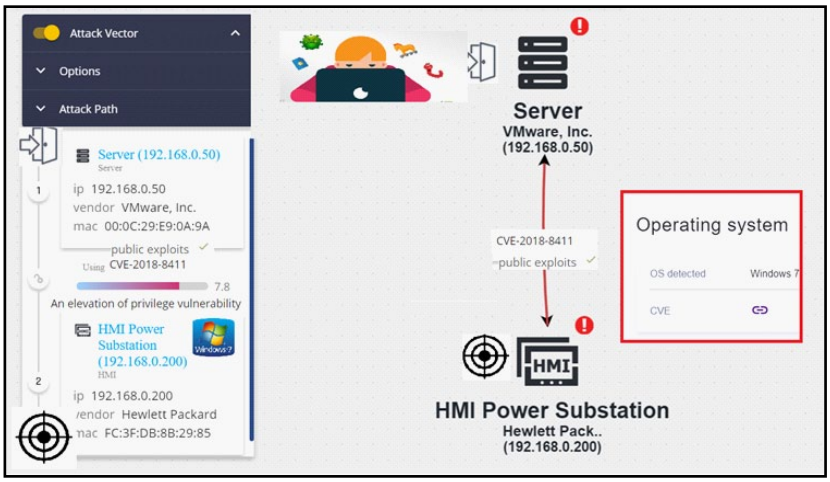
Since different attacker groups can exploit different paths in the target network, I will demonstrate how incorporating the attacker profile model in Radiflow's iSID threat monitoring and detection system allows the ICS security staff to discover the most vulnerable path for each attacker category. This will allows prioritizing the security patch management process according to the enterprise's cyber-threat level.

First, let's examine the network. In our analysis we used a typical network topology for a power utility, created by Radiflow's iSID asset management engine. Then we applied Radiflow's risk evaluation model of attack vectors, to deterimine the most likely attack path for each attacker profile.

ATTACK PATH BY ATTACKER PROFILE

Script-kiddie Attackers

Low-level attackers lack the ability to develop their own sophisticated programs or exploits. To move laterally in the network, a low-skill attacker would only be able to exploit known vulnerabilities using publicly available exploit codes.

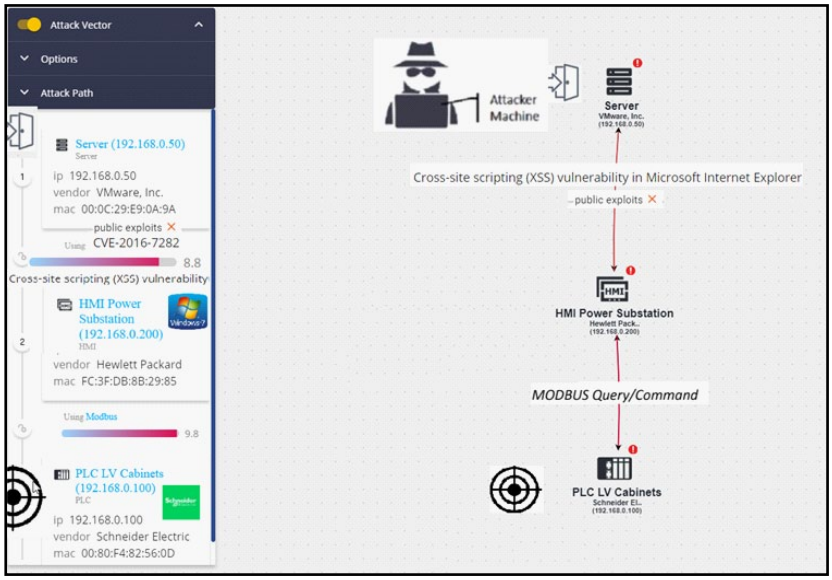


In this case, the attacker's target is a Windows-based HMI workstation, which has a known vulnerability (namely CVE-2018-8411.) This vulnerability can be exploited by executing a Metasploit framework-based public exploit. After exploiting this privilege-elevation vulnerability, the attacker can execute commands with elevated privileges.

For this attacker level, our recommendation was to prioritize applying security patches for the Windows station, as the most appropriate form of mitigation.

Professional Hackers

The next use-case is assumes a medium-level attacker. This attacker's entry point, to eventually reach the HMI, is an IT server. Using their ability to develop their own tools, the mid-level attacker can create a program to exploit a known vulnerability (without using publicly available code).



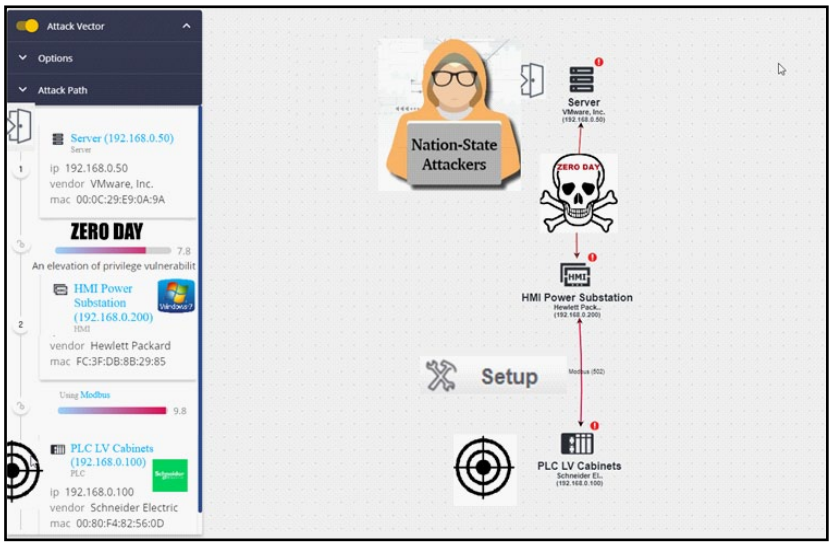
This exploit allows the remote attacker to perform cross-site scripting (XSS) attacks by injecting an arbitrary web script into Microsoft Explorer browser to steal cookies, session ID, usernames or other sensitive information, that were delivered from the PLC to web-based HMI.

Equipped with this information, the attacker can now move laterally inside the OT network using his advanced OT-protocol exploitation skills.
The attacker can gain access to the PLC by exploiting the Modbus protocol, a communication protocol known to be highly exploitable.

Once the attacker accesses the PLC, they can perform several actions within the cyber kill chain: from reconnaissance to gain data about the target (using diagnostic Modbus commands), to sending specially-crafted modbus packets that can cause loss of PLC availability. Once the attack objective is achieved the attacker will clear any logs and tracking information, to cover their tracks.

In this manner, a mid-level attacker can gain control over critical processes such as Low Voltage cabinets in a powerplant. However, having only medium-level skills, this threat actor cannot exploit control plane protocols and therefore cannot upload malicious firmware and unauthorized commands to the PLC.

Nation-state sponsored (APT) groups



Nation-state sponsored (APT) groups posses the advanced skills that allow them to exploit proprietary protocols and develop their own code to exploit zero-day vulnerabilities.

In this example, the the attacker's entry point is the IT server, and the end point is the HMI station. This attacker will use knowledge gained while performing long-term extensive research into unknown (zero-day) vulnerabilities, and perhaps utilize their capabilities to create their own tools to exploit these vulnerabilities.

In ICS/OT networks, a high skill level to exploit proprietary protocols (with no public specification) between an HMI and a PLC, to launch targeted attacks on the controller (e.g. attacking a production facility by injecting malicious controller firmware which is almost identical to the original, except for additional attacker programmed functionality.)

In addition to changing the firmware, the attacker is able to commit configuration commands on the PLC by exploiting a proprietary protocol. These actions might affect the controllers' logical decision-making and cause direct harm to production line operations.

CONCLUSION:

In this paper we discussed Radiflow's model for risk evaluation of attack vectors, which greatly simplifies that task of asset patching prioritization. We demonstrated the influence of the cyber attacker's capabilities on their potential lateral movement in the ICS network, using three use cases, each for a different attacker profile: low, medium and high-skill.

Low-skill attackers can move laterally inside the IT network and reach the HMI station by exploiting vulnerabilities with publicly available exploits.

Mid-level attackers are capable of moving laterally inside the OT network gain access to their targeted PLC by exploiting OT protocol.

High-skill attackers are able to move laterally inside in the OT network and are capable of committing operational actions on the PLC by exploiting proprietary protocol. These attackers have the highest possibility to cause the biggest impact on business processes.

These scenarios clearly demonstrate the need for adopting a evaluation model that takes into account different attack paths by different players, in order to prioritize mitigation measures (e.g. patching controllers) and optimizing the organiation's cybersecurity resources.

ABOUT RADIFLOW

Radiflow is a leading provider of cyber security solutions for critical industrial automation networks, non-intrusive IDS (Intrusion Detection System) and in-line security gateways.

Radiflow's leadership team consists of cyber experts from elite Israel Defense Forces (IDF) cyber defense and warfare units, as well as industrial automation professionals from global automation vendors and operators. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

radiflow
Secure Your Assets
www.radiflow.com | info@radiflow.com