J. Lopez, et al., “Protecting Industry 4.0 against Advanced Persistent Threats”, *European CIIP Newsletter*, vol. 11, pp. 27-29, 2017.
NICS Lab. Publications: https://www.nics.uma.es/publications

Protecting Industry 4.0 against Advanced Persistent Threats

Javier Lopez, Cristina Alcaraz, Jesus Rodriguez, Rodrigo Roman and Juan E. Rubio

Department of Computer Science, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain

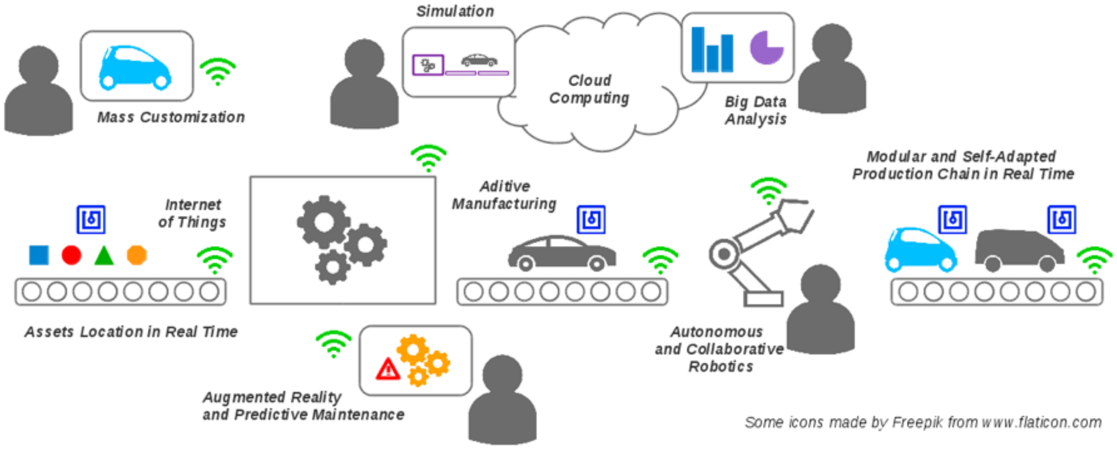
1 CIIP and the Industry (4.0)

The SADCIP project has arisen from the need to deal with increasingly intelligent and autonomous industrial and monitoring systems, capable of collaborating with each other to meet a common objective: provide efficient and real-time manufacturing and logistics from anywhere, at any time and anyhow [1]. However, any new condition that implies open communication with the Internet and the adaptation of heterogeneous (wireless) systems can, certainly, bring about numerous interoperability and security problems [2].

What types of problems? From a slight fault or anomaly within the operational applications, to massive and distributed attacks of a subtle and potentially damaging nature. Such problems can even have an aggressive effect on the welfare of other critical infrastructures. It is not the same to protect all those operational elements involved in the construction of each component that forms, for example, a bicycle, as the components that comprise a system of transport of greater reach, such as, a plane or a train. Therefore, it is self-evident that there is a relationship between the need to protect todays industry and the need to ensure protection, at all levels, of the rest of the dependent, critical infrastructures.

In addition, this characteristic underlines the criticality degree of a new paradigm related to the Internet of Things known as Industry 4.0, which in itself, can also be considered as a critical infrastructure.

Industry 4.0 (cf. Figure 1) constitutes a technological progress within the traditional industry. Here, both novel and existing systems coexist and share, in a centralized or decentralized way, resources, data and actions. As a result, novel services are enabled, and efficiency is increased. However, the nature of this context makes it difficult to trust fully on the goodness of the whole system, as multiple vulnerabilities are born mainly because of its complexity and heterogeneity. Moreover, in this particular context, one of the most dangerous threats are advanced persistent threats, or APTs. Therefore, SADCIP looks towards improving the state of the art, trying to find the necessary tools to a) monitor the technical capacities of the operational elements in the field, and b) detect relative evidence that, if applicable, should be addressed through optimal proactive response systems [3].


Simulation
Mass Customization
Cloud Computing
Big Data Analysis
Modular and Self-Adapted Production Chain in Real Time
Internet of Things
Aditive Manufacturing
Assets Location in Real Time
Autonomous and Collaborative Robotics
Augmented Reality and Predictive Maintenance

Some icons made by Freepik from www.flaticon.com

Figure 1: Scheme of an enhanced Industry 4.0 factory

2 The threat of APTs

Nowadays, Industrial Control and Automation Systems have been affected by an increased number of inside and outside threats, mainly due to the interconnection of industrial environments with modern ICT technologies. Beyond traditional IT threats (e.g., malware, spyware, botnets), one major issue is the existence of Advanced Persistent Threats (APTs). They consist of a new class of emerging and sophisticated attacks that are executed by well-resourced adversaries over a long time period. By combining multiple attack vectors that include the exploitation of zero-day vulnerabilities, together with stealthy and evasive techniques [2], many APTs go undetected over time. Although APTs were used against military organizations in the first term, they are now targeting a wide range of companies, hence drawing the attention from researchers focused in the industrial security sector [4].

Stuxnet was the first attack of this kind, reported in 2009, which sabotaged the Iranian Nuclear Program by causing physical damage to the infrastructure and therefore slowing down the whole process for four years. Ever since, the number of reported vulnerabilities concerning the Stuxnet was the first attack of this kind, reported in 2009, which sabotaged the Iranian Nuclear Program by causing physical damage to the infrastructure and therefore slowing down the whole process for four years. Ever since, the number of reported vulnerabilities concerning the Industrial Control Systems has increased dramatically, as the research community has incremented its interest and new attacks have been disclosed: in total, 1309 vulnerabilities have been reported by ICS-CERT between 2010 and 2015 (see Figure 2 showing this growth [5]).

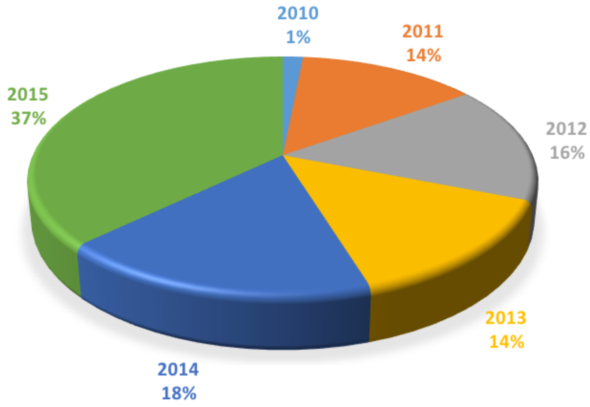


Figure 2: Reported vulnerabilities from ICS-CERT

As Stuxnet, every APT follows multiple steps, beginning with an initial intrusion commonly using social engineering (e.g., by means of fraudulent e-mails containing trojans). A successful intrusion results in the installation of a backdoor from which the attackers connect to the target network. Then, several exploits and malware are used to compromise as many computers in the victim network as possible (which is known as lateral movements), to ultimately modify the productive process or exfiltrate information back to the attacker domain. During the whole process, the threat actors make use of multiple tools to avoid detection and encrypt the external communication through publicly available services such as the Tor Anonymity Network.

Consequently, an additional effort is needed to mitigate the risks posed by these threats, which implies the effective detection of APTs through traditional countermeasures (e.g., intrusion detection systems, firewalls, antivirus) along with novel security services in continuous evolution within the company, involving all the organization with effective security awareness training and gaining knowledge from old use cases. Numerous surveys show the evolution of awareness about this field in the industry. Specifically, we can highlight the ISACA Advanced Persistent Threat Awareness Study [6], carried on in July 2015, that provides a view of the APT perception from security professionals belonging to many industries, mostly technology services, financial, military, telecommunications and manufacturing companies. Among all the statistics, it is worth commenting an increment of 4 percentage points in security training and an increase in security budget in the 53% of the entities surveyed compared to 2014. Concerning the technical measures to protect against APT attacks, a very high percentage of those enterprises (95 percent) report that they are using antivirus and traditional network perimeter technologies (e.g., firewalls), while they increasingly leverage a variety of preventive, detective and investigative controls to help reduce the likelihood of a successful APT breach. This includes mechanisms like critical controls for mobile devices, remote access technologies (RATs) or sandboxing.

3 Industry 4.0 and APTs

The industry as a whole is aware of the problems posed by persistent attacks, and there are already various mechanisms that aim to facilitate their detection. Yet the solutions that are used in traditional industrial control and automation systems are not directly applicable to Industry 4.0 contexts. The integration of Industry 4.0 principles, such as interoperability, decentralization, service oriented management, and interactivity, will fundamentally change all aspects of the industry: from the collaboration among supply chain partners, to the interactions between operators and machinery at the factory floor [7]. Yet it will also exacerbate the risks associated to APTs.

On the short term, industrial protocols like IO-Link and OPC UA will facilitate the interaction between existing and novel services. These and other technologies, like the Internet of Things, recognition services, and location services, will allow all individuals from operators to administrators and executives to access any relevant information anywhere at any time, helping them to make better decisions. Yet this interconnected ecosystem not only increases the attack surface, but also expands the influence that an APT can have in all actors once it has infiltrated into the system.

The deployment of open integrated factories and the integration of intelligent, dynamic processes are some of the medium and long-terms goals of the Industry 4.0, respectively. Such goals will enable the creation of flexible workflows and production processes, the deployment of intelligent assistants using novel HMI interfaces (e.g. wearables, augmented reality), and the advent of novel services such as the digital twins (maintenance and management through simulation), amongst other benefits. Yet this flexibility and intelligence comes at a cost: APTs will be able to influence over the behavior of factory processes in subtler ways.

Moreover, we also have to consider how the Industry 4.0 and the Internet will be closely linked. Beyond the use of IoT devices, and the convergence of IT/OT infrastructures, there are novel approaches, such as cloud manufacturing, that will allow traditional manufacturing components to become virtualized and deployed in the cloud. These novel approaches will be surely become a target of APTs.

4 SADCIP Project Goals

Given the effect that APTs will have over present and future Industry 4.0 deployments, it is essential to understand the potential risks and to develop an integrated solution that can effectively detect and react against APTs. Therefore, the specific goals of the SADCIP (Advanced System for the Detection of Persistent Cyberattacks in Industry 4.0) Project [8], which is funded by the Spanish Ministry of Economy, Industry and Competitiveness, are as follows:

- Analyze and investigate the characteristics of the most relevant cyber-attacks for Industry 4.0 environments.

- Develop security guidelines for Industry 4.0 environments, which not only serve to design safer infrastructures, but also to deploy defense mechanisms in a more optimal way.

- Create the basic components of a modular, flexible and easily adaptable intrusion detection architecture for Industry 4.0 scenarios, capable of cooperatively monitoring the existence of cyber-attacks that affect its fundamental elements (IoT, cloud / fog).
- Design and develop various transversal services that support the various elements of the detection system, including security services such as trust management systems, fog-based control services, etc.
- Develop relevant analyzers for industry 4.0 environments, including scanners capable of detecting the lateral and data exfiltration attempts associated with APTs movements. These analyzers will be platform agnostic, allowing their integration with other systems beyond the SADCIP architecture,

The proposed architecture and analyzers are being developed in conjunction with the project coordinator, S2Grupo: a Spanish cybersecurity firm specialized in the development and integration of security solutions against APTs. In order to validate the results, these components will be integrated and validated in a testbed, where multiple attacks will be launched. Moreover, this testbed will also serve as a demonstrator of the resulting product.

References

[1] J. Wan, H. Cai, and K. Zhou, "Industrie 4.0: enabling technologies," in *Intelligent Computing and Internet of Things (ICIT), 2014 International Conference on*. IEEE, 2015, pp. 135–140.

[2] L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber stealth attacks in critical information infrastructures," *IEEE Systems Journal*, 2016.

[3] C. Alcaraz, L. Cazorla, and J. Lopez, "Cyber-physical systems for wide-area situational awareness," in *Cyber-Physical Systems: Foundations, Principles and Applications*. Boston: Academic Press, 2017 2017, no. Intelligent Data-Centric Systems, ch. 20, pp. 305 – 317.

[4] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *IFIP International Conference on Communications and Multimedia Security*. Springer, 2014, pp. 63–72.

[5] ICS-CERT, "Year in review 2015," https://ics-cert.us-cert.gov, last retrieved in February 2017.

[6] ISACA, "Advanced persistent threat awareness study results," http://www.isaca.org, last retrieved in February 2017.

[7] J. Smit, S. Kreutzer, C. Moeller, and M. Carlberg, "industry 4.0," *European Parliament, Directorate General for Internal Policies*, feb 2016.

[8] S. UMA, "Sadcip project," https://www.nics.uma.es/projects/sadcip, last retrieved in February 2017.