Challenges in Critical Infrastructure Security

Corrado Leita

Challenges in Critical Infrastructure Security

Corrado Leita

Symantec Research Labs Europe, Sophia Antipolis, France
Corrado_Leita@symantec.com

Abstract. The threat landscape is continuously evolving. Large, widespread worm infections are leaving more and more space to more stealthy attacks targeting highly valuable targets. Industrial Control Systems (ICS) are rapidly becoming a new major target of cyber-criminals: ICS are evolving, bringing powerful capabilities into the critical infrastructure environment along with new and yet undiscovered threats.

This was pointed out in multiple occasions by security experts and was confirmed by a recent survey carried out by Symantec: according to the survey (http://bit.ly/bka8UF), 53% of a total of 1580 critical infrastructure industries have admitted to being targeted by cyber attacks. The survey implies that the incidents reported by the press over the last several years are nothing but the tip of a considerably larger problem: the vast majority of these incidents has never been disclosed. Moreover, when looking at the few publicly disclosed incidents such as Stuxnet, we see a completely different level of sophistication, compared to traditional malware witnessed in the wild in previous years.

This talk will dive into the challenges and the opportunities associated to ICS security research, and on the tools at our disposal to improve our ability to protect such critical environments.