Industrial control systems (ICS) are rapidly becoming a new major target of cyber-criminals. This was pointed out in multiple occasions by security experts [1], [2] and was confirmed by a recent survey carried out by Symantec [3]. In this survey, 53% of the 1580 critical infrastructure companies that were interviewed admitted to having been targeted by cyber attacks. On average, the surveyed companies admitted to having been attacked 10 times in the last 5 years, with each of these attacks having an average cost of 850k USD. The survey provides a basis for a quantitative estimate of the extent of the problem and 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 incidents have never been disclosed. Still, the details of the publicly disclosed incidents give us a better understanding of the underlying issues we face. For instance, a recently discovered malware variant called Stuxnet which has been analyzed at length by Symantec [4] was shown to be part of a highly sophisticated targeted attack aiming at tampering with devices involved in the control of high speed engines, and compromise the associated industrial process [5]. The infection was only uncovered accidentally when an operational anomaly was discovered — Stuxnet has probably been operating undetected since June of 2009 [6]. Stuxnet, and other related threats discovered recently [7], show that industrial control systems are evolving, bringing powerful capabilities into the critical infrastructure environment along with new and yet undiscovered threats.

The power grid infrastructure is a clear example of this evolution. As in other critical infrastructure environments, the idea of interconnecting industrial control systems with other networked computing systems came up only in the last decade, beginning as a method for lowering costs while increasing system efficiency [8]. This convergence is now moving beyond industrial control systems, and the Smart Grid is now being promoted globally as a way to solve problems with energy production, distribution and consumption, to enable energy independence and to combat climate change. Smart Meters, or more generally, the Advanced Metering Infrastructure (AMI), have been aggressively adopted by many European countries. For example ENEL, the Italian utility company, has already deployed over 30 million meters. Similar trends are being followed by other European countries such as France and Netherlands, in which a pilot deployment of 250,000 units will be enriched in the future years to cover 80% of the national installations.

1. Power grid infrastructure and IT security

The convergence between ICS environments and standard IT practices and technologies has important security implications [9], implications which have only been marginally explored by security researchers.

On the one hand, the increasing use of COTS (commercial, off-the-shelf) operating systems (Windows, Linux, etc...) has exposed these environments to attacks, incidents and intrusion techniques characteristic of traditional IT environments.

On the other hand, the employment of standard IT technologies can be seen as an opportunity to access the extensive array of standard IT security techniques (intrusion detection systems, file scanning, standard hardening techniques) and to apply it on these networks. Security techniques honed over many years of practical application can now be used to bear on security issues new to the critical infrastructures.

On the other hand, the employment of standard IT technologies can be seen as an opportunity to access the extensive array of standard IT security techniques (intrusion detection systems, file scanning, standard hardening techniques) and to apply it on these networks. Security techniques honed over many years of practical application can now be used to bear on security issues new to the critical infrastructures.

We claim the trade-off between benefits and associated challenges to be currently imbalanced: standard IT security technologies, however robust, cannot protect critical infrastructure as effectively as it is possible in standard enterprise IT environments, given the greater amount of variation in existing control systems and communication protocols as well as the prevalence of older technologies in operation concurrently with newer systems. Moreover, no concrete solutions have
been proposed so far for addressing the security concerns associated with new technologies such as AMI infrastructures, where the introduction of basic security primitives (e.g. encryption and authentication in network communications) does not tackle the serious concerns associated to their large scale deployment [10], [11], [12].

1.1. Specific challenges

In order to understand the reasons at the root of the ineffectiveness of standard IT security techniques, we need to look more in detail at the characteristics of the threat model and of the environment being protected. Many of the incidents which have been publicly disclosed in the last years have in fact underlying important facts.

The complexity of the environments is often very difficult to handle. For instance, a nuclear plant in Georgia was shutdown for 48 hours as a consequence of a software update installed on a workstation operating in its business network. Nobody was aware of the connection between the workstation in the business network and the control system on the SCADA network, and of the effects caused by this connection.

Additionally, incidents witnessed in the recent years have underlined an unprecedented level of sophistication in the threats targeting ICS environments. A prime example of this sophistication is the Stuxnet infection, which used four distinct and previously unknown zero-day exploits, and leveraged multiple stolen certificates for the injection of its rootkit: when the certificate used for the installation of the rootkit was reported stolen, and consequently revoked by the Symantec (Verisign) Certification Authority, the malware was immediately patched remotely to utilize a second stolen certificate. Stuxnet was not an isolated incident: in 2011, a threat sharing similar characteristics to Stuxnet was discovered and was shown to have been generated by the same authors, or those who have access to the Stuxnet source code [7].

These examples highlight specific challenges of protecting critical infrastructure environments, challenges which can be traced back to how critical infrastructure environments differ from typical enterprise environments.

Critical infrastructure environments are very heterogeneous. They include a mix of traditional desktop computers, large mainframes, and field devices. These devices are profoundly different in terms of computational power, communication protocols and even in their ability to be managed and provisioned (i.e. install new software or upgrades). The manner in which these devices are interconnected can vary significantly from company to company (even in the same business branch, such as energy) and automated management controls are frequently non-existent. Because of this heterogeneity in hardware, software and network topology, the security assessment of these environments is particularly challenging. Preliminary studies performed on some of these devices have shown that the security of those systems has been neglected and that a motivated attacker could easily penetrate those systems.

Many communication protocols are vendor-specific. While standards exist for many communications protocols [13], vendors have added specific extensions to provide additional functionalities. The lack of publicly available information on these extensions and their interactions negatively impacts standard security mechanisms, including most Intrusion Detection Systems, which generally rely on signatures for the detection of threats, as well as standard vulnerability discovery tools which require knowledge of the protocol specifications in order to properly assess the robustness of protocol implementations.

Critical infrastructure environments are very valuable targets. Because of their strategic importance, critical infrastructure environments are likely to be targeted by highly motivated and resourceful attackers. The motivation and resources available to individuals interested in compromising these systems can be considerably greater than those attacking more typical IT environments. Many security practices that aim at preventing intrusion by raising their cost (e.g. requiring valid signatures to load kernel drivers) may be ineffective when dealing with these highly resourceful attackers.

2. The CRISALIS project

The CRISALIS project (Critical Infrastructure Security Analysis), is a Research Project funded by the European Commission in the context of the FP7 research framework that aims at revisiting the convergence between standard IT systems and industrial control systems typically used in the context of the power grid from a security standpoint. The project will involve in a three-year effort a set of key actors in European academic research (EURECOM, Chalmers University, University of Twente), in the manufacture of devices (Siemens), in the development of security solutions (Symantec) as well as in the deployment and maintenance of national infrastructures (ENEL, the Italian energy provider, and Alliander, key actor in the deployment of Smart Meters in the Netherlands).

The CRISALIS project is a Research Project funded by the European Commission in the context of the FP7 research framework that aims at revisiting the convergence between standard IT systems and industrial control systems typically used in the context of the power grid from a security standpoint. The project will involve in a three-year effort a set of key actors in European academic research (EURECOM, Chalmers University, University of Twente), in the manufacture of devices (Siemens), in the development of security solutions (Symantec) as well as in the deployment and maintenance of national infrastructures (ENEL, the Italian energy provider, and Alliander, key actor in the deployment of Smart Meters in the Netherlands).
The project is articulated over a set of coherent and pragmatic guidelines:

- Focus the attention on real-world, targeted attacks carried out by resourceful attackers against critical infrastructures.
- Address two specific, yet interlinked, environments, namely the SCADA systems employed in power generation and distribution as well as the AMI infrastructure employed in the distribution of electricity to consumers.
- Develop practical solutions and tools, and test these tools on real systems.

The project research effort spans over three main themes: (i) securing the systems, by means of novel automated analysis of CI environments and discovery of new threat vectors; (ii) detecting the intrusions, by developing new technologies aiming at coping with the heterogeneity of protocols, interactions and devices typical of these systems; (iii) analyzing successful intrusions, by devising techniques to facilitate the “post-mortem” analysis of the environments and of specific devices. These three research themes are meant to complement each other in order to address their respective limitations. Not all the security problems can be easily discovered and fixed, therefore the need to improve our capability of detecting anomalous interactions in these environments. Similarly, not all the intrusions can be detected with certainty, therefore the need to develop tools to inspect specific devices and detect tampering. Key to the uniqueness of the project is a specific focus on two main challenges that characterize these environments:

**System complexity.** An important transversal research theme consists in the development of tools and techniques for the automated discovery of the structure and the interactions in these environments. This will include protocol learning techniques to address the proliferation of vendor-specific protocol dialects in these networks, as well as new device fingerprinting approaches able to deal with the diversity in the involved devices.

**Validation.** In order to guarantee the practicality and the general applicability of the developed tools and techniques, the CRISALIS project will setup a set of real-world environments for their validation and evaluation thanks to the involvement of critical infrastructure maintainers such as ENEL and Alliander.

The project, set to start on the 1st of March 2012, will ultimately contribute to addressing the current imbalance between challenges and opportunities associated to the convergence of IT technologies with Industrial Control Systems. If accepted, the presentation will present more in depth the research content, the planned methodology and early results of the project.

**References**


