Introduction

Industrial control systems (ICS) are rapidly becoming a new major target of cyber-criminals. This is shown by statistics worldwide: for instance, a recent survey (http://bit.ly/bka8UF) showed that 53\% of a total of 1580 critical infrastructure industries have admitted to being targeted by cyber attacks. While details about most of these incidents are not disclosed for a variety of reasons, the few episodes whose details have been publicly available emphasize that important breaches in the security of these environments exist. For instance, a recently discovered malware variant called Stuxnet which has been analyzed at length by Symantec[1] 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. The infection was only uncovered accidentally when an operational anomaly was discovered - Stuxnet has probably been operating undetected since June of 2009. It is clear that industrial control systems are evolving, bringing powerful capabilities into the critical infrastructure environment along with new and yet undiscovered threats.

The evolution of these systems has not been coupled with significant advances in their protection. The deployment of COTS technologies has meant that the extensive array of standard IT security techniques (intrusion detection systems, file scanning, standard hardening techniques, etc.) can now be utilized on these networks, bringing security techniques honed over many years of practical application to bear on security issues new to the critical infrastructure environment.

Challenges

Unfortunately, standard IT security technologies, however robust, cannot protect critical infrastructure as effectively as it is possible in standard enterprise IT environments, for a variety of reasons.

1. **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. Because of this heterogeneity in hardware, software and network topology, the security assessment of these environments is particularly challenging.
2. **Many communication protocols are vendor-specific:** while standards exist for many communications protocols, vendors have added specific extensions to provide additional functionalities. The lack of publicly available information negatively impacts standard security mechanisms,

[1] See http://www.symantec.com/connect/blogs/w32stuxnet-dossier

including most Intrusion Detection Systems, which generally rely on signatures for the detection of threats.

3. **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. 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.

Objectives

Threat analysis

Despite the convergence with IT technologies, standard security mechanisms do not suit in many cases the characteristics of Critical Infrastructure environments. This allowed threats such as Stuxnet to infiltrate a highly sensitive network and operate undetected for many months. Look back at the vast amount of information available on the incident, and try to get a detailed understanding of its characteristics.

State of the art

Look at the state art in intrusion detection systems and host-/network-based protection. Which mechanisms would have helped to block a similar threat? Try to reason on the threat characteristics, but also on the environment characteristics: a generic IPS may detect and block a threat, but its false positives may have catastrophic effects on the environment operation!

Gap analysis

Building upon your analysis of the state of the art, try to underline some major research gaps and requirements for the development of future systems for the protection of critical infrastructure environments from this type of threats.

References

A few links to get you started:

- http://bit.ly/bka8UF
- http://go.symantec.com/stuxnet
- http://www.symantec.com/connect/blogs/trojanhydraq-incident
- http://www.symantec.com/connect/blogs/w32stuxnet-variants
- http://www.symantec.com/connect/blogs/stuxnet-breakthrough
- Dacier, Marc, “On the resilience of the dependability framework to the intrusion of new security threats “, Chapter book In "Dependable and Historic Computing (essays dedicated to Brian Randell on the Occasion of his 75th Birthday)", Eds. Jones, Cliff B; Lloyd, John L; LNCS Vol 6875, Springer Verlag, ISBN:9783642245404 , pp238-250