Critical Information Infrastructure Protection: Urgent vs. Important

Miguel Correia
INESC-ID, Instituto Superior Técnico – Lisboa, Portugal
miguel.p.correia@ist.utl.pt

Critical infrastructures like the power grid play a fundamental role in our society. The computerization of these infrastructures and the associated risk of cyber-attacks become evident in the past decade. Today, there is a clear understanding that these critical information infrastructures (CII) are a likely target for cyberwarfare attacks.

This state of affairs has led governments, companies and other organizations to understand that *urgent* action is needed to protect these infrastructures. Several standards and guidelines for critical infrastructure protection (CIIP) have appeared. The emphasis has been on trying to put CIIP at the same level of protection of Internet-connected information technology (IT) assets, e.g., at the level of the main cloud computing offerings or home banking services. Examples of technologies being pushed are firewalls, intrusion detectors, network access control, and vulnerability scanners.

Organizations as well as individuals tend to make a dangerous mistake: to confuse important with urgent. For CIIP it is indeed *urgent* to implement the mechanisms just mentioned, but that is not enough. The objective of CIIP is to reduce the risk to an adequate level, which is not doable using the same mechanisms as for IT for the simple reason that the impact of CII failure is much higher.

This talk will introduce two approaches that go beyond the urgent and deal with the important.

The objective of the first approach is to protect the firewalls that defend the CIIs from attacks against themselves (against the firewalls) [1]. Firewalls are supposed to be security bastions, but sometimes they can be attacked. The idea is to use self-healing and replication mechanisms to build high-availability / high-security firewalls.

The second approach aims to ensure the timeliness of critical commands given over wide-area networks when there are router/link failures and denial of service attacks [2]. The point is to use overlay networks and multi-homing to provide path diversity for messages sent.

Despite the benefits of both approaches, they would not be effective against attacks like Stuxnet, which manage to “fly over” the “air gap”, so often promoted as a measure for CIIP. The final part of the talk will discuss research directions to tackle this kind of attacks.

References:

[1] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves, P. Verissimo. The CRUTIAL Way of Critical Infrastructure Protection. IEEE Security & Privacy, vol.6, n.6, Nov/Dec. 2008.

[2] W. S. Dantas, A. N. Bessani, m. Correia. Not Quickly, Just in Time: Improving the Timeliness and Reliability of Control Traffic in Utility Networks. In Proceedings of the Workshop on Hot Topics in System Dependability (HotDep), Jun 2009.

This work was supported by national funds through FCT – Fundação para a Ciência e a Tecnologia, under project PEst-OE/EEI/LA0021/2011.

Short bio

Miguel Correia is an Associate Professor at Instituto Superior Técnico (IST) of the Universidade Técnica de Lisboa (UTL), in Lisboa, Portugal. He is a researcher at INESC-ID, in the Distributed Systems Group. He has a PhD in Computer Science from the University of Lisboa Faculty of Sciences. He has been involved in several international and national research projects related to intrusion tolerance and security, including the TCLOUDS, MAFTIA and CRUTIAL EC-IST projects, and the ReSIST NoE. He has more than 60 publications in international journals, conferences and workshops. His main research interests are: security, intrusion tolerance, distributed systems, distributed algorithms, computernetworks, cloud computing, and critical infrastructure protection.