Protecting CRUTIAL Things*

(Extended Abstract)

Alysson Neves Bessani Paulo Sousa Miguel Correia Nuno Ferreira Neves Paulo Verissimo

LASIGE, Faculdade de Ciências da Universidade de Lisboa – Portugal

1 Introduction

Today's critical infrastructures like the Power Grid are essentially physical processes controlled by computers connected by networks. Once these systems were highly isolated and secure against most security threats. However, in recent years they evolved in several aspects that greatly increased their exposure to cyber-attacks coming from the Internet. Firstly, the computers, networks and protocols in those control systems are no longer proprietary but standard PCs and networks (e.g., wired and wireless Ethernet), and the protocols are often encapsulated on top of TCP/IP. Secondly, these networks are usually connected to the Internet indirectly through the corporate network or to other networks using modems and data links. Therefore these infrastructures have a level of vulnerability similar to other systems connected to the Internet, but the socio-economic impact of their failure can be huge. This scenario, reinforced by several recent incidents [6], is generating a great concern about the security of these infrastructures, especially at government level.

Recently, we proposed a reference architecture to protect critical infrastructures, in the context of the CRUTIAL[1] EU-IST project [5]. The idea is to model the whole infrastructure as a WAN-of-LANs, where the typical facilities that compose it (like power transformation substations or corporate offices) are modeled as collections of LANs interconnected by a wider-area network (WAN). Given the ease of defining LANs in today' IP architectures (e.g., through Virtual switched LANs), there is virtually no restriction to the level of granularity of our architecture's LAN, which can go down to a single host. Using this architecture, we reduce the problem of critical infrastructures protection to the problem of protecting LANs from the WAN or other LANs. In consequence, our model and architecture allow us to deal both with outsider threats (protecting a facility from the Internet) and insider threats (protecting a critical host from other hosts in the same physical facility, by locating them in different LANs).

*Contact email: *pjv@di.fc.ul.pt*. This work was partially supported by the EC through project IST-2004-27513 (CRUTIAL) and NoE IST-4-026764-NOE (RESIST), and by the FCT through project POSI/EIA/60334/2004 (RITAS) and the Large-Scale Informatic Systems Laboratory (LaSIGE).

[1]Critical UTility InfrastructurAL Resilience: `http://crutial.cesiricerca.it`.

2 The CIS Protection Service

Here, we introduce a device for protecting LANs called *CRUTIAL Information Switch* (CIS). A fundamental service provided by CIS is the *Protection Service*, which ensures that the incoming and outgoing traffic in/out of the LAN satisfies the security policy of the infrastructure. Figure 1 ilustrates the use of CIS protecting several LANs of a critical infrastructure.

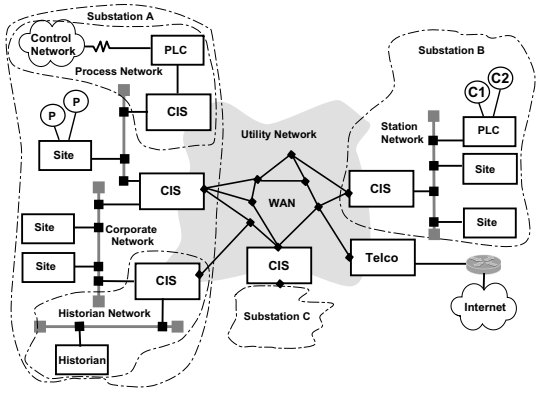

Figure 1. WAN-of-LANs connected by CIS.

A CIS can not be a simple firewall since that would put the critical infrastructure at most at the level of security of current (corporate) Internet systems, which is not acceptable since intrusions in those systems are constantly being reported. Instead, the CIS has several different characteristics. Firstly, it has similarities to a *distributed firewall* [2], since CIS can be deployed not only on the network border but inside the networks to better protect critical equipment. Secondly, the CIS uses a *rich access control model* that takes into account the involvement of different organizations and allows the access control rules to depend on context information. Thirdly, the CIS is *intrusion-tolerant*, i.e., it operates correctly even if there are intrusions in some of its components and withstands a high degree of such hostility from the environment, seeking unattended perpetual operation.

In this work we address specifically the last topic. The intrusion tolerant CIS is replicated in a set of $n \geq 2f + 1$ machines. Each *CIS replica* receives all packets to and from the LAN and verifies if this packet satisfies some pre-defined

application-level policy [2]. The difficult point here is to ensure that intrusions (modelled as Byzantine faults) in at most f of the replicas are masked, i.e., that all valid packets are accepted and all invalid packets are dropped. The CIS design presents two very interesting challenges that make it essentially different from other Byzantine fault-tolerant services. The first is that a firewall-like component has to be transparent to protocols that pass through it, so it can not modify the protocols themselves to obtain intrusion tolerance. This also means that recipient nodes will ignore any internal CIS intrusion-tolerance mechanisms, and as such they can not protect themselves from messages forwarded by faulty replicas not satisfying the security policy.

These two challenges are solved through the use of wormholes [4]: we assume that each replica of the CIS has a trusted component that cannot be corrupted. These *local wormholes* are connected through an isolated network. Moreover, each CIS replica is deployed in a different operating system (e.g., Linux, FreeBSD, Windows XP), and the operating systems are configured to use different passwords and different internal firewalls (e.g., iptables, ipf, Windows firewall). Figure 2 depicts the intrusion-tolerant CIS architecture. Every message approved by a replica is issued to the wormhole to be signed. The local wormholes vote between themselves and, if the message is approved by at least $f + 1$ replicas, it is signed using a secret key installed in the trusted component. Once the message is signed, one of the replicas (the leader) is responsible for forwarding the approved message to its destination. Failure detection, leader election and proactive recovery are other services provided by the wormhole. The traffic replication devices in Figure 2 are responsible for broadcasting the WAN and LAN traffic to all replicas. The LAN replication device is specially useful to detect if malicious replicas send non-approved messages to the LAN. When a quorum of replicas suspect some replica, it is (reactively) recovered.

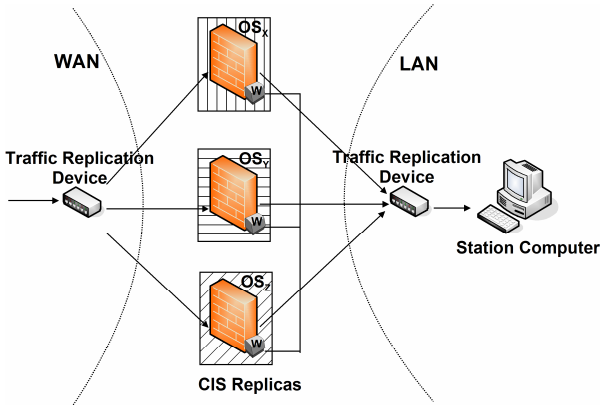

Figure 2. Intrusion-tolerant CIS architecture.

[2]The CIS design presented here assumes that policies are stateless. In [3] we explain how statefull policies could be supported.

3 Prototype and Evaluation

The intrusion-tolerant CIS can be implemented and deployed in several ways, depending on the criticality of the LAN being protected. If the LAN protected by the CIS provides a very critical service, the implementation must be based on the use of different physical replicas for each CIS replica, allowing tolerance to physical and software faults. However, since price is always a major concern, namely for power grid operators, a much more cost effective solution can be attained by resorting to virtualization. The various replicas are deployed in the same host, using virtual machines (VM) to isolate the different runtime environments, preventing intrusions from propagating.

We have implemented a VM-based CIS prototype using the XEN virtual machine monitor [1] and the Linux operating system. Preliminary experiments were conducted on this prototype, in order to evaluate its behavior in face of attacks. The results exhibited an overall good performance in terms of latency, throughput and packet loss rate. Moreover, they helped us to realize that replication based on VMs must be used judiciously, since it implies less resources for each individual replica.

4 Conclusions

This paper presented the CIS protection service, implemented by highly resilient distributed devices, aimed at protecting critical information infrastructures. The CIS has three distinguishing features: it is intrusion-tolerant, it seeks unattended perpetual operation and it supports a rich access control model that takes into account application semantics.

A detailed description of the CIS design, prototype, and evaluation is available in [3].

References

[1] P. Barham, B. Dragovic, K. Fraiser, S. Hand, T. Harris, A. Ho, R. Neugebaurer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *Proc. of the 19th ACM Symp. on Operating Systems Principles - SOSP'03*, Oct. 2003.

[2] S. M. Bellovin. Distributed firewalls. *;login:*, Nov. 1999.

[3] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves, and P. Verissimo. Intrusion-tolerant protection for critical infrastructures. DI/FCUL TR 07–8, Univ. of Lisbon, April 2007.

[4] P. Verissimo. Travelling through wormholes: a new look at distributed systems models. *SIGACT News*, 37(1), 2006, http://www.navigators.di.fc.ul.pt/docs/abstracts/ver06travel.html.

[5] P. Verissimo, N. F. Neves, and M. Correia. CRUTIAL: The blueprint of a reference critical information infrastructure architecture. In *Proc. of CRITIS'06 1st Int. Workshop on Critical Information Infrastructures Security*, Aug. 2006.

[6] C. Wilson. Terrorist capabilities for cyber-attack. In M. Dunn and V. Mauer, editors, *Int. CIIP Handbook 2006*, volume II, pages 69–88. CSS, ETH Zurich, 2006.