Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 30 (2008) 424–432
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Redesigning remote system administration paradigms for enhanced security and flexibility

Marco Prandini [a,*], Marco Ramilli [b]

[a] University of Bologna, Viale Risorgimento 2, Bologna, Italy
[b] University of Bologna, Via Venezia 52, Cesena, Italy

Available online 8 March 2008

Abstract

Remote system administration is usually performed according to the standard client–server model. However, important security and flexibility limitations, arising from the usage of a predictable access port for such a critical application, prevent a satisfactory trade-off between authentication strength and service availability. We illustrate an alternative solution, based on an additional system placed in between the remote server and its administrator. Our design ensures that the new component's role does not weaken the existing security mechanisms already in place, but it can instead enhance them, and provide a very effective decoupling between a server and its visible management ports.

Keywords: System administration; Security; IRC; Intelligent agents

1. Introduction

System administrators usually perform their tasks by connecting to a service allowing to control a remote system. Such a service either provides a remote view of the locally available administration tools (e.g.: remote terminal, remote desktop), or implements a back-end for the execution of complex commands received through a corresponding front-end (e.g.: web-based administration interfaces). This approach is so "natural" for the average administrator that he/she usually does not see its significant security and efficiency limitations. With this paper, we start a research line hopefully leading to overcome two issues: first, the lack of flexibility provided by the methods commonly available to the administrator for contacting the remote server, and second the lack of expressiveness usually associated to the command and control environment present on the server.

In this work, the focus is placed on the communication-related aspects, proposing an alternative to the common client/server model. A service implementing the latter kind of model has to listen to a known network port and to authenticate the incoming connection attempts. In many cases, the service has to be reachable from unpredictable locations, with standard client software; for this reason, implementing protection mechanisms relying on network tools (such as packet filtering) or on peculiar client capabilities (such as cryptography-based authentication) is not always viable. Both brute-force attacks against the remote administration service and attempts at exploiting software/protocol vulnerabilities, then, must be considered possible. Host- and network-based intrusion detection systems can help thwarting the attacks before they succeed, but cannot guarantee security against the vastly distributed attacks that are presently possible, especially considering the value of the target (that is full control of an Internet host). The goal of this research is to devise an unconventional model of communication between the system administrator and the remote administration interface. In the proposed solution, the aforementioned vulnerability of the traditional scheme is addressed by reversing the client–server relation; an administration engine replaces the classical service, originating connections to an intermediate system instead of listening for connections.

The immediate advantage arising from this design choice is that there is nothing to attack on the remote host. On the other hand, the introduction of an additional system in the security chain must be carefully evaluated, to avoid introducing

* Corresponding author.
E-mail address: marco.prandini@unibo.it (M. Prandini).

0920-5489/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.011

unexpected attack paths, and eventually making the system less robust than it originally was. We claim that, if properly modeled and implemented, a platform based on the meeting of the server and its administrator on an intermediate system is expedient in terms of security, availability, usability and opportunity for future extension.

After an analysis of the existing related work, presented in Section 2, the paper proceeds to highlight the illustrates the peculiarities of the proposed model in Section 3, gives architectural details in Section 4, analyzes the implementation choices allowing to satisfy the security, efficiency and effectiveness constraints in Section 5, and concludes with a summary of attained results and potential for future research in Section 6.

2. Scenario modeling and related work

In this section we analyze the main remote administration paradigms currently available and their potential evolution. As illustrated in Fig. 1, the proposed classification is two-dimensional, the first aspect being the kind of intelligence that can be associated to the administration interface, and the second being the flexibility of the communication path between the system and its administrator.

The simplest forms of remote administration exploit a standard client/server model to let the administration access some server's functionalities. These can be either non-interactive, providing a means of giving orders or examining information, or interactive, providing an environment where the effect of each basic instruction imparted to the system can be immediately perceived.

Examples of systems belonging to the former category are web-based administration interfaces; a common trait of these systems is the possibility of making quite complex tasks available by means of intuitive but powerful interfaces, since the processing is done in batch on the server after all the relevant data has been collected through a front-end. The main drawbacks of this approach are the lack of interactivity, the hiding of the exact results on the system configuration, and often the difficulty of extending the functionalities beyond what is specifically provided by the designer of the interface.

Interactive interfaces, on the other hand, encompassing remote desktop and remote terminal systems [17,2], offer direct access to the native administration environment of the server. The availability of the most fine-grained tools allows a greater precision and flexibility, but, on the flip side, a deep knowledge of the inner workings of the system is required in order to perform even simple tasks, and complex tasks tend to require a high number of low-level, manually-coordinated operations.

By changing the paradigm for imparting commands from imperative to declarative, it could be possible to retain some benefits of the traditional interactive approaches, while at the same time being able to program the system in terms of desired configuration goals, leaving to its "intelligence" the task of designing the most effective plan to reach them. Proposals for the implementation of a command-line substitute of this kind, based on Jabber, have been made a few years ago [1].

Every interface based on a client–server protocol exhibits a common weakness. The server part of the system must listen on a known network port, which becomes the obvious target for attacks targeting either protocol vulnerabilities or authentication weaknesses. Moreover, it often represents a critical single point of failure, taking the system completely out of control in case of problems.

With the intent of overcoming the aforementioned limitations, we propose to introduce a third party in the system/administrator communication model. The role of said party is that of abstracting the concept of remote management port, as it will be detailed in the following section. The change in the communication model does not affect the possibility of implementing both interactive and batch-like administration systems. Moreover, since the design of the mediated channel calls for the adoption of artificial intelligence techniques, an evolution towards an integrated declarative approach can be envisaged. A not trivial, yet powerful evolution of an approach based on artificial intelligence would be substituting the need for a traditional communication channel with autonomous, possibly mobile agents.

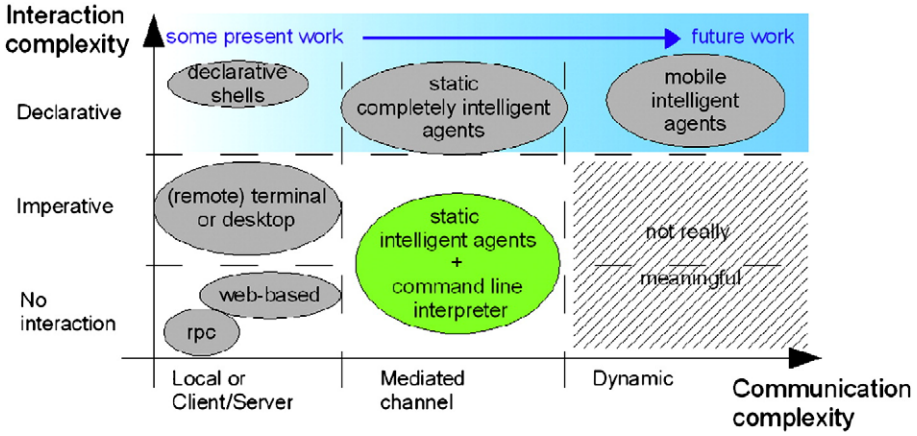

Fig. 1. Classification of system administration paradigms.