An architecture for autonomic security adaptation

Andreas KLENK*, Heiko NIEDERMAYER*, Marcus MASEKOWSKY*, Georg CARLE*

Abstract

Communication is the grounding principle of nowadays complex applications where the functionalities of the overall system are much more powerful than the ones of the isolated components. The task of keeping the communication system operable is highly critical due to the configuration complexity and the need for manual administration. Autonomous configuration mechanisms offer a compelling solution for the communication problem. We present an architecture for the autonomous configuration of secure, layer independent, end-to-end connections in this paper. The Extensible Security Adaptation Framework (ESAF) separates the particularities of communication setups strictly from the communication usage by the applications. Applications are unaware of the utilized security mechanisms and the complex configuration thereof. Protocols and security primitives can be easily introduced into the system whereas others might be disabled due to vulnerabilities without the need to modify existing programs. Moreover the setup can adapt to changing environments dynamically during runtime.

Key words: Autonomous system, Computer security, System architecture, Adaptive system, Middleware.

UNE ARCHITECTURE POUR L’ADAPTATION AUTO-ORGANISANTE DE SÉCURITÉ

Résumé

La communication est l’élément de base des applications complexes d’aujourd’hui, dans lesquels des fonctionnalités du système entier ont une puissance beaucoup plus grande que celle des composants isolés. À cause de la complexité de la configuration et la nécessité d’administration manuelle, la tâche de tenir le système de communication en fonction est hautement critique. Une solution impérative pour le problème de communication est offert par des mécanismes de configuration autonome. Dans cette publication, nous présentons une architecture pour la configuration autonome des connexions de bout en bout sécurisées et indépendantes de la couche. L’Extensible Security Adaptation Framework (ESAF) sépare strictement les particularités des environnements de communication et l’usage par les applications. Les applications sont ignorantes des mécanismes de sécurité utilisés et leur configuration complexe. Des protocoles et des primitives de sécurité peuvent être facilement introduits dans le système, tandis que d’autres pourraient être désactivés à cause des vulnérabilités, sans la nécessité de...

* Computer Networks and Internet, University of Tübingen, Wilhelm-Schickard Institute – Auf der Morgenstelle 10c, 72076 Tübingen, Germany.
During the last decade the number of computers drastically increased as well as the demand for communication. This trend raises the issue how to handle and guarantee security in those systems, considering their vast complexity. Manual configuration approaches reach their limit of applicability as the number of computer and the possible network interconnections rapidly grow. Hence security must be as easy to enforce as connecting a computer to the network.

With the introduction of innovative network concepts new challenges arise as more devices will be part of the network and network components will change more frequently. Sometimes the devices must act completely autonomic with little to none further administration, for example, in ubiquitous scenarios where computers and other electronic helpers are employed once and must operate autonomously further on. In such settings manual configuration is not feasible anymore. Thus, traditional manual security management approaches reach their limit of applicability.

The driving force for change is now the user with her needs and her fascination for new and innovative products. The complexity and the unforeseeable number of possible interactions and communication interfaces requires a self-configuration capability for the security and communication functions of the devices. A solution to this problem is offered by the introduction of autonomic communication.

I. INTRODUCTION

I.1. The non-autonomic use of current technologies

Current security technologies are either integrated into the system (like IPsec) or into the application (like SSL/TLS). An example for security configuration at system level is the management of security policies or associations for IPsec. Configuration at the system level usually reflects the highest demand for security and therefore uses the protocol and cryptographic algorithm which offers the best security guarantees. The choice of the “best” security protocol reflects only badly the true security requirements at a given time. During a session only certain data need strong protection. Another example for potential lower security requirements is communication in trusted environments, say inside the company network.