Journal of High Speed Networks 15 (2006) 207–208
IOS Press

Guest Editorial

Managing security policies: Modeling, verification and configuration

The importance of security in present-day communication networks is undisputed. The security of a network depends not only on the encryption algorithm and security protocols that it supports, but even more so on the policies that are used to guide and control the operations of the deployed algorithms and protocols. As a result, security policies within networks have received significant attention from the research community recently.

The paradigm of policy based management allows administrators to define higher level objectives, which through a series of refinements are translated to the configuration of network devices. However, such a refinement, if not done properly, amplifies the impact of errors and security exposures. Formal mechanisms and frameworks which permit the analysis of policies for correctness, consistency, and inherent risk are needed. Improved techniques for refining and transforming policies from higher level objectives to the network configuration are needed. Correct specification and configuration of security policies are essential for effective security enforcement. Dynamicity in the network can cause policies to be in conflict, and mechanisms that automatically generate correct policy specifications are required. Furthermore, policy based paradigms should not have an adverse impact on the performance of network security devices.

Current distributed systems are built using a variety of heterogeneous components. Each of these components usually supports its own version of security policies for access and authorization. The complexity of managing security policies across many different heterogeneous components is one of the strongest impediments to successful application of policy based security management. Managing heterogeneity is one of the key factors influencing successful enforcement of security policies in a real-life environment.

This special issue includes 8 rigorously reviewed papers that present original contributions in the area of management and analysis of security policies for networks. This special issue covers a wide range of issues representing security policy analysis and refinement, improving performance of security policies, and managing security policies across heterogeneous components. Three of the papers present different approaches for security policy analysis and refinement, one discusses performance improvement in security policy enforcement, and two discuss different approaches for dealing with heterogeneity.

Hamed and Al-Shaer address the issues of efficient enforcement of security policies. Policy enforcement devices like firewalls require evaluating and enforcing security policies on every packet arrival in real-time. They describe and evaluate a technique for dynamically reordering security filters in a firewall so that the performance of the policy enforcement is maximized.

Sandhu, Zhang, Ranganathan and Covington propose a security framework to enforce access control policies using the functions of trusted computing. The architecture is based on an abstract layer of trusted hardware and a trust monitor that verifies the integrity and properties of running applications and enforces various policies on behalf of object owners. The proposed architecture was extended to support general access control models such as lattice-based, role-based, and usage-based access control policies.

Laborde, Barrere and Benzekri address the issue of translating from higher level policies to network device configurations in a general manner. Starting from network security objectives, they provide a formal framework for deriving network security device configuration through three abstraction levels, while providing and analyzing the information model or each of the abstraction levels.

Aziz, Foley, Herbert and Swart address the issue of analyzing role-based access control policies for risks. They provide a formalism that can assess the risk for RBAC policies, and present a sequence of operators that can be use to find policies with less risk but semantics equivalent to that of original policies.

Yang, Martel, Fu and Wu address the issue of specifying IP security and VPN policies correctly. The authors present an approach for analyzing security policies, and demonstrate its applicability to inter-domain negotiation of IP-sec and VPN policies.

Ganek, Anthony Nadalin, Nataraj Nagaratnam and Dinesh Verma looks at the lifecycle of policies, and proposes an approach for security and authorization that is modeled using policies and rule attached to business process and models. It describes the operational and deployment aspects for autonomic behavior of policy-driven systems.

Heterogeneity is address in the papers by Foley et al. and Alves-Foss et al. **Foley, Mulcahy, Quillinan, Connor and Morrison** describe how they have addressed this problem in the context of Secure WebCom, a distributed computing architecture that can be used to securely distribute application components for execution over a network. They describe their approach for defining role based access control policies on the different components that are needed to implement the secure webcom architecture.

Alves-Foss and Wahsheh focus on systems developed using the MILS (Multiple Independent Levels of Security), an architecture being developed by a coalition of defense industries, academics and government agencies for development of high assurance embedded systems required in fields such as avionics and defense. Their paper describes how meta-policies can be used to handle heterogeneous enclaves of policies of systems developed using the MILS architecture. The approach proposed can be extended to other types of environments.

The papers selected in this special issue address many of the critical issues and technical challenges for managing security policies in distributed systems. Although many problems still remain, we believe that these eleven papers in this special issue reflect the state-of-the-art in this area and significantly advance the understanding of the research community.

We would like to thank all the authors and reviewers who made this special issue possible. Finally, we would like to express our gratitude to Professor Deepinder Sidhu, the Editor-in-Chief of Journal of High Speed Networking, for giving us this opportunity and accepting this topic.

Ehab Al-Shaer
Multimedia Networking Lab
School of Computer Science, Telecommunications & Information Systems
DePaul University
Chicago, IL 60604, USA
Tel: +1 312 362 5137
Fax: +1 312 362 6116
E-mail: ehab@cs.depaul.edu

Dinesh C. Verma
Autonomic Systems & Networks
IBM TJ Watson Research Center
PO Box 704
Yorktown Heights, NY 10598, USA
Tel: +1 914 784 7466
Fax: +1 914 784 7455
E-mail: dverma@us.ibm.com

Clifford Neuman
Information Sciences Institute
University of Southern California
Los Angeles, USA
E-mail: bcn@isi.edu

Hong Li
Senior Researcher
Intel IT Research
CA, USA
E-mail: hong.c.li@intel.com

Anthony Chung
School of Computer Science
DePaul University
Chicago, USA
E-mail: chung@cs.depaul.edu