



POLITECNICO DI TORINO
Repository ISTITUZIONALE

Sicurezza nelle reti: utilizzo di architetture multi-core per il monitoraggio del traffico IP

Original

Sicurezza nelle reti: utilizzo di architetture multi-core per il monitoraggio del traffico IP / Mezzalama M.; Oglietti G.; Venuto E.. - ELETTRONICO. - (2013), pp. 176-185. ((Intervento presentato al convegno Frontiere Digitali: dal Digital Divide alla Smart Society tenutosi a Fisciano (ITA) nel 18-19-20 Settembre 2013.

Availability:

This version is available at: 11583/2515100 since:

Publisher:

AICA

Published

DOI:

Terms of use:

openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

Sicurezza nelle reti: utilizzo di architetture multi-core per il monitoraggio del traffico IP

Marco Mezzalama, Gianluca Oglietti¹, Enrico Venuto²

Politecnico di Torino – DAUIN

Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)

marco.mezzalama@polito.it

¹Politecnico di Torino

Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)

gianluca.oglietti@polito.it

²Politecnico di Torino

Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)

enrico.venuto@polito.it

Abstract. *The IP packet capture activity has always assumed great importance in the computer networks security. It's daily used in fact to monitor and analyze the IP traffic passing through a computer networks with the purpose to identify anomalous behaviors that could be associated with security problems. The new infrastructures for high throughput networks, also used in small or medium sized local networks, have made this activity more and more difficult showing some limits of the most recent multi-core capture systems used today. This paper has the purpose to describe the main technologies used in a generic capture system, to identify its possible limits, to diagnose its causes and to discover the possible solutions that must be adopted.*

Keywords: security, networks, multi-core, packet capture, high throughput.