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

Marco Mezzalama, Gianluca Oglietti[1], Enrico Venuto[2]
Politecnico di Torino – DAUIN
Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)
marco.mezzalama@polito.it
[1]Politecnico di Torino
Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)
gianluca.oglietti@polito.it
[2]Politecnico 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.