

**cPacket Networks**  
2061 Landings Drive  
Mountain View, CA 94043  
[www.cPacket.com](http://www.cPacket.com)

**For more press information contact:**

Abigail Johnson/Paul Michelson  
Roeder-Johnson Corporation  
+1 (650) 802-1850  
<http://email.roeder-johnson.com>

**For more customer information contact:**

cPacket Networks  
Mountain View, CA  
+1 (650) 969-9500 FAX: +1 (650) 969-4900  
[info@cPacket.com](mailto:info@cPacket.com)

**CPACKET EXECUTIVE SAYS NETWORK SECURITY FALLS FAR SHORT;  
REQUIRES PERVASIVE, MULTI-TIERED APPROACH WITH A LOCAL FOCUS**

**New Class of Chip, New Balance Between Local and Centralized Security Processing, Key  
to Reducing Complexity, Cost & Performance Bottlenecks**

**MOUNTAIN VIEW, CA - SEPTEMBER 19, 2007** - Security in the network will remain unacceptably poor until it becomes embedded in the network at the *local* level, not just the centralized locations where it is found today," said Rony Kay, founder and CEO of cPacket Networks. Key to pervasive security, said Kay, will be low-cost, "complete packet inspection", powered by a new generation of chips that permit wire-speed monitoring and control to be established essentially "everywhere" in the network.

"Security in the network today can be likened to a model where local law enforcement vanishes from our communities and we are left with the several massive, bureaucratic Federal agencies to keep our streets, homes, and playgrounds safe," said Kay, speaking at an industry seminar here recently. "Without pervasive, local control of our own environment, our entire social infrastructure would break down."

The network infrastructure is no different, said Kay. Despite massive investments in security, the network remains highly vulnerable and extremely fragile, as evidenced by recent events. "Look at the August 16<sup>th</sup> network woes at Charles Schwab, the 18-hour site outage at NetFlix on July 23rd, and the extremely public collapse of Skype's network for two days, also on August 16," said Kay. "These extremely public events - as well as thousands that escape the notice of the media - are a sign that current approaches are insufficient. Like policing our own communities, we need a multi-tiered approach that depends heavily on *local* network security capabilities, embedded right in the infrastructure, where they can deliver broad situational awareness and effective response *before* the problem takes the network down."

The difficulty, Kay explained, is that the complexity of the network infrastructure is increasing rapidly, with more nodes, more diverse traffic and higher bandwidth requirements with each passing day. At the same time, current technological limitations have made the cost of adding security processing to networking equipment significantly higher than the cost of the network connectivity itself - by as much as an order of magnitude! The result, said Kay, is that today's security is highly centralized, inordinately expensive, and totally lacking in the agility, visibility, and immediate response capability necessary to keep up with the threats. "It's like commissioning Homeland Security to deal with a traffic jam," said Kay.

What is required, said Kay, is a new approach that embeds security in a pervasive manner throughout the entire network, in such a way that one can have the "situational awareness" necessary to respond instantly to threats or problems, and contain the damage before it spreads into the entire network. To make this possible requires a new technology - which Kay referred to as "complete packet inspection" - that has only recently become available - in the form of a breakthrough chip - based upon a novel algorithmic "fabric" invented by cPacket.

What cPacket has done, explained Kay, is to develop an economical chip that performs both header and payload inspection of every packet, every bit, at 20 gigabits per second. This new silicon technology results in a 10-to-1 improvement in packet processing speeds, at about one-tenth the costs. The resulting

-more-

100-to-1 improvement in cost-performance permits situational awareness and rapid response to be integrated pervasively into the network infrastructure, right down to the port level, without introducing the complexity, cost, or performance bottlenecks that characterize current technologies.

Kay said that the chips were designed for ease of integration into pre-existing network equipment designs while having the flexibility to be the foundation of any future security feature. "There are just three ports," said Kay, "input, output and duplicate." This permits a "bump in the wire" model that allows the 6-watt chip to be dropped, for example, into switches and line cards - even at individual ports, with minimum disruption. Control can be in-band, or out-of-band. Moreover, the chip uses a "zero programming", template-based model to invoke the unified header parsing and regular-expression searches in the payload that it is uniquely capable of. "Provisioning is as simple as filling in a form on a browser," said Kay.

According to Kay, examples of features that switch manufacturers could instantly offer their customers using cPacket's chips include reports - accessible from a browser - to enhance visualization and situational awareness; protective rate limits to contain denial of service attacks; behavior monitoring of critical ratios and key performance indicators to detect behavioral anomalies; advanced access control lists (ACLs) based on header and payload information; and smart, selective mirror ports, to facilitate troubleshooting and debugging.

The bottom line, concluded Kay, is that there is now a means for network equipment manufacturers to provide cost-effective, easy-to-use network visibility and response based upon complete packet inspection, that is both suitable and economical for pervasive deployment throughout the network, and not just in expensive, high-end products. "There's a new sheriff in town," said Kay.

Kay made his remarks at a seminar entitled "Embedded Network Security Design" hosted by the Linley Group, on September 13.

#### **About cPacket**

cPacket Networks is an emerging leader in chips and technologies that offers breakthrough, "complete" packet inspection, at a fraction of the complexity, power, or cost of preexisting approaches. It provides manufacturers of routers, switches and other network appliances a low-impact means to easily drop game-changing, wire-speed active network traffic analysis and response directly into their existing or planned designs - whether targeted at the service providers, the enterprise, or the small office. The exploding use of networks for media-centric applications makes the availability of truly pervasive deep packet inspection timely and crucial.

cPacket was founded in 2003 and is located in Mountain View, CA. For more information, visit [www.cPacket.com](http://www.cPacket.com).

Editors, note: All trademarks and registered trademarks are those of their respective companies.

Additional background information is available at [www.roeder-johnson.com](http://www.roeder-johnson.com).