Introduction

Ever-increasing IP traffic and security threats are driving the need for more robust cyber security and extensive analysis of packet flows to better protect and manage network traffic. In response, a new breed of security appliances has emerged, interrogating packet content and extracting metadata, and providing far more traffic flow detail than made possible with first generation deep packet inspection (DPI) solutions that primarily check TCP/UDP port numbers and look for patterns in packet headers. With these new capabilities, network equipment can now examine flows in real time, identify protocols used, recognize data relationships and communications patterns, and improve the detection of sophisticated malware.

Fortunately, it's possible to develop these advanced security appliances with minimal software effort and no exotic hardware. Proving this point, Intel and Qosmos* are showing equipment manufacturers how to deploy the necessary DPI technology on general-purpose computing platforms. As such, Intel® architecture-based platforms are typically more economical, scalable and flexible than those based on specialized hardware, while delivering comparable performance. For instance, some Intel architecture processor platforms are capable of supporting both packet handling and DPI simultaneously at tens of gigabits per second (Gbps). This is possible because workload acceleration technologies embodied in Intel® QuickAssist Technology and Intel® Data Plane Development Kit (Intel® DPDK) dramatically speed up packet processing on Intel® processors, thereby enabling a higher level of throughput.

Cyber security vendors need to increase the effectiveness of their products, such as next-generation firewalls and solutions for NBAD, SIEM and DDoS attacks, by using DPI and network metadata. Metadata can be leveraged to see good from bad network behavior faster than current COTS products and raw data analysis that use data logs, full packet capture and deep packet inspection.

This paper discusses the security and traffic policy enforcement benefits derived from Qosmos advanced DPI technology and the Intel DPDK that runs on Intel® Xeon® processors through to Intel® Atom™ processors. Equipment manufacturers can take advantage of this combination to deliver cost-effective, next-generation security and networking solutions.
Fundamentals: What is DPI?

Firewalls can no longer rely exclusively on ports to effectively classify traffic. At a minimum, today’s firewalls should examine individual IP flows at a highly granular level using a form of network packet filtering called deep packet inspection (DPI). DPI combines a traditional stateful firewall with intrusion detection and prevention functionality performed by thoroughly inspecting packet payloads and identifying individual streams of traffic on a per-user and per-application basis.

DPI is illustrated in Figure 1, where DPI inspects the protocol and data types of the OSI model layers 1-7, as well as the packet payloads. In contrast, shallow packet inspection only checks the header portion of layers 1-3 and not packet payloads.

Network intelligence technology, depicted in Figure 2, actively parses packets, peeling away each layer of encapsulation until it reaches the data contained within. NI is a more sophisticated and “deeper” approach than the first generation DPI, which typically looks for TCP and UDP port numbers and patterns in packet headers. Using NI technology, cyber security solutions can:

- Identify applications independently of which port numbers they might use
- Detect when tunneling protocols are being used, and parse through them in order to find the information they encapsulate
- Group application data into their respective flows, and use the signaling information to group correlated flows into sessions
- Extract application content and metadata

Beyond DPI: Network Intelligence Technology

For some time, telecom equipment and solution vendors have employed DPI in their network solutions to deliver basic IP traffic visibility to their service provider customers. But with so many applications now completely reliant on the Internet as a platform, solutions to manage, secure and monetize networks now require deeper visibility and more granular detail on traffic flows than DPI was designed to provide.

Going beyond DPI, network intelligence (NI) technology further inspects IP data packets by identifying the protocols used and extracting packet content and metadata (see sidebar), thus enabling the analysis of data relationships and communications patterns. The resulting visibility into network activity provides the true picture of data usage, purpose and value, which is critical for detecting abnormal behavior and defending against potential cyber attacks. NI serves as a middleware element to capture and feed information to advanced network applications, such as for bandwidth management, traffic shaping, policy management, charging and billing, service assurance, revenue assurance, cyber security and more.
The additional information available from NI is exemplified in Figure 3, which shows the metadata from the Qosmos network intelligence solution next to output from Netflow, an industry standard for IP traffic monitoring. Netflow is fast and repeatable, but since it’s signature-based, it cannot disclose potential threats. Consequently, finding the behavioral context requires security specialists to mine and analyze full data packets and logs, sometimes done manually or with outdated tools. This process makes it difficult to perform event correlations or to differentiate normal and abnormal behavior.

In contrast, the Qosmos network intelligence solution parses traffic in real-time for user behavior and application usage, providing insight into what actually occurred between the source and destination. In this example, the Qosmos metadata additions to the Netflow record reveal:

1. A referring party (chicaroo.cc)
   - Why is chicaroo.cc referring users to the Qosmos site?
2. A suspicious URL (http://www.golf.com/faillogin.php) and no cookies
   - Why would anyone go directly to a failed login page without a session cookie?
3. A suspicious browser (cURL2.x) – not Internet Explorer*, Firefox* or Chrome*, etc.
   - Is a malicious script invoking the command line version of this browser?
4. The server code is giving a positive result (200) despite the record’s irregularities
   - Is someone exploiting a vulnerability?

This detailed flow information can be used to create situational awareness, enabling security specialists to quickly identify suspect traffic and categorize the risk of flows coming in, such as low, medium or high risk. For instance, a real-world deployment of network intelligence revealed that users visiting Qosmos.com spend an average of 20 minutes on the site, typically get a session cookie assigned to them from the site, and use one of the top three browsers 95 percent of the time. After studying user behavioral patterns, Qosmos determined visitors coming to the site’s main page (index.html) via the Firefox web browser and having a session cookie are low risk. On the other hand, someone using an unknown browser and going to an unheard of URL (e.g., www.qosmos.com/fjdfghdfghkdby7cvb45fg) is considered medium risk.

More about Metadata

Metadata bridges the gap between conventional tools and raw analysis by enabling the detection and differentiation of good and bad behavior patterns in network traffic flows. Through the use of network metadata, cyber security solutions can provide a wide range of new functionality, including the ability to:

- Provide full classification and decoding of network protocol layers 4-7 and describe as many protocol and application attributes as needed.
- Boost performance since metadata can be extracted from traffic in real-time without the need for data aggregation and formatting or database searches; therefore, flow inspection is more precise, faster and easier than when using data logs.
- Query traffic without the need to store full, raw data packets, thus reducing storage requirements by a ratio of 1000:1 compared to processing packet captures and/or Syslog.
- Track multiple flows with a single protocol (e.g., an FTP connection and data channels).
- Increase application and session awareness.
Table 1 lists network metadata examples. It is noteworthy that some protocols and applications have more than 50 metadata attributes—totaling thousands of attributes collectively. They can be selected, correlated, and analyzed to provide a complete understanding of the quality and purpose of network events.

<table>
<thead>
<tr>
<th>Protocol Examples</th>
<th>Typical Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP (Hypertext Transfer Protocol)</td>
<td>URL, browser, cookies, domain naming system, authentication…</td>
</tr>
<tr>
<td>TCP (Transmission Control Protocol)</td>
<td>Source port, destination port, client port, server port…</td>
</tr>
<tr>
<td>GTP (GPRS Tunneling Protocol)</td>
<td>Device, user location, quality of service (QoS) metrics, time, duration…</td>
</tr>
<tr>
<td>UDP (User Datagram Protocol)</td>
<td>Source port, destination port, client port, server port…</td>
</tr>
<tr>
<td>IP (Internet Protocol)</td>
<td>Source address, destination address, source port, destination port, data…</td>
</tr>
<tr>
<td>RTSP (Real Time Streaming Protocol)</td>
<td>Play/pause, streaming file, URL, duration…</td>
</tr>
<tr>
<td>SIP (Session Initiation Protocol)</td>
<td>Caller, entity called, codec…</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Examples</th>
<th>Typical Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (POP, SMTP)</td>
<td>Sender, receiver, login, subject, message, attachments, date &amp; time…</td>
</tr>
<tr>
<td>Webmail (Yahoo! Mail*, Gmail*, etc.)</td>
<td></td>
</tr>
<tr>
<td>IM (MSN, Yahoo, Skype, QQ, etc.)</td>
<td>User login, IP address, MAC address, mobile ID (IMSI, IMEI), called party, message, attachments, duration, date &amp; time…</td>
</tr>
<tr>
<td>Web Apps (YouTube, eBay, etc.)</td>
<td>IP address, MAC address, mobile ID, duration, date &amp; time, video on demand usage, channels viewed (as applicable)…</td>
</tr>
<tr>
<td>A/V Apps (Shoutcast, Yahoo Video*, MSN Video*, IPTV, etc.)</td>
<td>User login, login / logout date &amp; time, data transfer sessions (type, content, time), volume (per user, IP, subnet, application), app response time…</td>
</tr>
<tr>
<td>Business Apps (CRM, ERP, Citrix, Oracle, MS Exchange, SAP, etc.)</td>
<td></td>
</tr>
</tbody>
</table>

Challenges for Cyber Security Solution Developers

Easier said than done, next generation solutions must deliver high-performance packet processing and DPI, while ensuring both types of workloads interact with each other efficiently. Given the complexity, some security solution vendors may find it cost-effective to integrate a third-party DPI solution over developing one in house.

Challenge #1: Maximizing packet processing performance without sacrificing portability

In typical networked security applications, over 90 percent of the computing workload is sophisticated packet processing and forwarding. Consequently, developers must focus on packet processing performance, and unfortunately, they may be unable to use standard networking stacks because operating system overhead can significantly limit their performance. As a result, it may be necessary to re-engineer networking stacks in a way that allows them to be portable across industry-leading processor architectures, and their on-chip accelerators and offload engines.

Challenge #2: Handling the complexity of deep packet inspection without sacrificing throughput

An essential component of a DPI solution is the decoding technology, which must parse data from hundreds of protocols and applications, as well as from new applications (e.g., video, social networking, P2P) being launched everyday. Further complicating matters, most applications are not standardized and require reverse engineering. It’s also necessary to deal with complex mechanisms associated with applications that deliberately hide and encrypt data and support several protocols, some of which may be revised regularly. To cope with exploding traffic throughput, solutions may need to support multiple 10 Gbps traffic streams, with 40 gigabit Ethernet on the horizon.

Challenge #3: Optimizing the interaction between packet processing and DPI

In order to maximize system throughput, developers should pre-filter packets, so only the relevant ones are subjected to full DPI processing, and avoid packet manipulation overhead via packet cloning, zero-copy architecture and other mechanisms. Optimizations must also work when multiple application instances are running concurrently.
Qosmos* ixEngine

Cyber security developers can greatly reduce their development time by integrating the Qosmos* ixEngine, a software development kit (SDK) composed of software libraries and tools that are easily integrated into new or existing solutions. The SDK contains a decoding engine, protocol libraries, advance DPI and metadata extraction features that deliver complete visibility into network traffic in real-time.

Using ixEngine*, developers can take advantage of protocol and application classification and the delivery of communication metadata, which enables application-level insight to be incorporated into security solutions. Designed with developers in mind, ixEngine accelerates the product development cycle by offering the capabilities listed in Figure 4. Ready-to-use software libraries reduce the effort and lower the risks associated with developing and maintaining a highly complex technology internally.

The following describes the features of the Qosmos ixEngine in more detail.

Decoding engine

- Identification of protocol and applications contained in IP Flows using stateful inspection and heuristic analysis. Qosmos’ protocol plug-in suite includes over 1,000 protocol and application plug-ins to classify flows and extract metadata (4,500 metadata available to date).
- Extraction of metadata from protocols (e.g., volume, delay, jitter etc.) and applications (e.g., name of file streamed on a website)

Protocol updates

- Continuous watch of protocols and applications, and update of ixEngine when new versions appear that impact classification and metadata extraction

Protocol services

- Instant access and continuous updates to 1000+ protocols and 4500+ communications
- On-demand development of new protocol plug-ins
- Protocol change reports for notification of changes in protocols

Protocol Plug-in SDK

- Ready-to-use DPI development tools and libraries
- Allows users to develop custom protocol plug-ins for their ixEngine

Supported operating system

- Linux* Standard Base 3.x

Running DPI on a General-Purpose Computing Platform

Until recently, cyber security vendors had no choice but to run DPI software on hardware platforms based on special packet processors in order to attain the necessary performance. Some of the downsides of using these purpose-built platforms include their relatively high cost, scalability and support challenges, and inconsistency with the Cloud’s general-purpose platform approach.

Today, it’s possible to achieve impressive DPI performance with the family of general-purpose Intel processors, ranging from Intel Xeon processors through to Intel Atom processors. For the high-end, Qosmos measured exceptional performance — more than 100 thousand packets per second — of its DPI and network intelligence software running on the next-generation Intel communications platform, codename Crystal Forest. The game changer for Qosmos was integrating the performance-optimized libraries from the Intel Data Plane Development Kit (Intel DPDK), which significantly increased packet processing performance.

Figure 4. Qosmos* ixEngine Capabilities
When cyber security vendors design in Qosmos software and Intel architecture processors (Figure 5), they benefit from a cost-effective solution, a pervasive processor architecture with large caches, an easy-to-use development environment and a dependable roadmap delivering continuously increasing performance. For decades, the Intel processor roadmap has confirmed Moore's Law, the result of continuous investment in technology and manufacturing. On roughly an annual basis, Intel launches higher performance computing platforms used by equipment manufacturers to develop more capable products. Now, cyber security vendors can take advantage of Intel's roadmap, as well as new advancements supported by the Crystal Forest platform and the Intel DPDK. Moreover, Qosmos software seamlessly scales across the entire family of Intel architecture processors: Intel Xeon processors, Intel® Core™ processors and Intel Atom processors.

Intel's Workload Consolidation Strategy

Today's network elements are rather complicated, particularly since many employ an assortment of processors to perform different workloads, such as application, control plane, data plane and signal processing. For instance, a rack typically contains various bladed network elements that use different processor architectures, as illustrated in Figure 6. Maintaining these network elements requires expertise across different hardware platforms, operating systems and unique vendor technologies. However, this need not be the case.

A path forward is Intel's 4:1 workload consolidation strategy, depicted in Figure 7, which enables security equipment manufacturers to consolidate various hardware platforms into one. This is achievable using Intel's next generation platform, Crystal Forest.

The platform can be easily configured for low-end elements, such as secured branch routers, as well as high-end equipment, including enterprise security appliances with unified threat management (UTM). Developers will have the flexibility to deliver three different workloads on a single architecture, assigning cores to perform application, control plane and data plane processing as they see fit.

Figure 5. Overview of Intel and Qosmos® Technologies

Figure 6. Networking and Telecommunications Infrastructure Has Various Network Elements That Use Different Architectures

Figure 7. Intel's 4:1 Workload Consolidation Strategy
The Crystal Forest platform can also accelerate complementary workloads, such as cryptographic and data compression, using Intel QuickAssist Technology. The workload acceleration capabilities, supported by a set of software and hardware modules, are accessed via a unified set of industry-standard application programming interfaces (APIs), which provides consistent conventions and semantics across multiple accelerator implementations and future-proofs software investments. The platform also delivers exceptional packet processing performance by running performance-optimized libraries from the Intel DPDK.

**Higher Packet Processing Performance**

Intel architecture has a proven track record of delivering high performance and innovation over its long history of meeting market requirements in the various embedded communication markets. By integrating a memory controller and increasing memory bandwidth, the first generation Intel® Core™ i7 processor family (codename Nehalem) achieved breakthrough performance when executing control and data plane workloads concurrently. This was possible, in large part to the Intel DPDK, which greatly improved packet processing on Intel architecture.

The Intel DPDK, consisting of a set of libraries designed for high speed data packet networking, is based on simple embedded system concepts and allows users to build outstanding small packet (64 byte) high performance applications. It offers a simple software programming model that scales from Intel Atom processors to the latest Intel Xeon processor.

**Figure 8.** Breakthrough Data Plane Performance with Intel® Data Plane Development Kit (Intel® DPDK) L3 Packet Forwarding

The Intel DPDK, consisting of a set of libraries designed for high speed data packet networking, is based on simple embedded system concepts and allows users to build outstanding small packet (64 byte) high performance applications. It offers a simple software programming model that scales from Intel Atom processors to the latest Intel Xeon processor.
processors, providing flexible system configurations to meet any customer requirements for performance and scalable I/O. While the Intel DPDK may be used in various environments, the Linux* SMP userspace environment is the most common among engineers due to the ease of development and testing of customer applications, along with maintaining leading edge data packet performance that easily outperforms native Linux*, as shown in Figure 8. The L3 forwarding for the 2.40GHz Intel® Xeon® processor E5645 (Westmere-EP ) on a native Linux stack is about 1 Mpps per core, compared to 6 Mpps (64 byte packets) per core using the Intel DPDK.

With the addition of integrated PCI Express* controllers, more cores and architecture enhancements, the 2nd Generation Intel® Core™ Processor Family (Intel microarchitecture codenamed Sandy Bridge ) provides even greater scalability and flexibility to embedded communication market segments. The Intel DPDK demonstrates the impressive small packet performance achievable using the latest Intel architecture in Figures 8 and 9.

The Intel DPDK provides Intel architecture-optimized libraries that allow developers to focus on their application. The Intel DPDK provides non-GPL source code libraries to support exceptional data plane performance and ease software development, while minimizing development time. This allows the developers to make additions and modifications to the Intel DPDK, as required, to meet their individual system needs.

Workload Consolidation Benefits

Workload consolidation paved the way for efficiency improvements for cyber security vendors in several areas, such as platform resource utilization, application development, services deployment and economies of scale. But in order to get the greatest benefit from consolidation, it’s necessary to switch from hardware-focused network elements (leveraging highly-specialized components) to software-based network elements running on general-purpose hardware. Once this transition is made, the benefits can be far reaching for both security vendors and their customers, including:

Security vendor benefits:

- **Platform development:** Use a common platform that makes it easier to deploy different security products and is easier to control.
- **Engineering resources:** Reduce development effort with one platform architecture to know, one code base to write and one development team to manage.
- **Product cost:** Take advantage of more manufacturing options, such as using commercial off-the-shelf (COTS) solutions that are refreshed yearly.
- **Market opportunities:** In addition to offering stand-alone products, give customers and solution integrators the ability to add security solutions to existing Intel architecture-based servers using virtualization.
- **In-field support:** Minimize system support cost with just one type of hardware platform to learn, deploy and maintain.

Intel® Xeon® Processor E5-2600 (B0 stepping) with 20MB L3 cache and with Intel® Hyper-threading Technology (Intel® HT Technology) disabled.

It should be noted in the case of IPv4 Layer 3 forwarding, the system throughput is I/O limited, constrained by the current PCI Express Generation 2 network interface cards (NICs); the processor computing capacity was not fully utilized. Figure 10 shows the packet performance for various packet sizes and port usage cases for a single eight core, 2.0 GHz
Packet Processing and Advanced DPI on a Single Computing Platform

Cyber security vendors can now employ a turnkey development environment from Qosmos that combines exceptional packet processing, DPI and metadata to create content aware flow classification at throughputs on the order of tens of Gbps. All of this can be done on an Intel architecture-based platform with the help of the Intel DPDK that significantly speeds up packet processing performance. This solution enables equipment suppliers and solution vendors to satisfy the security requirements of enterprises, service providers and cloud solutions across tomorrow’s communications infrastructure.

2 Performance results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

Copyright © 2012 Intel Corporation. All rights reserved. Intel the Intel logo, Intel Core, Xeon and Intel Atom are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.
To learn more about Intel solutions for communications, please visit www.intel.com/go/comms
Printed in USA  MS/VC/0412  Order No. 327184-001US