Protocol and Application Classification Engine (PACE)

Technology Brief

- Layer-7 protocol and application detection software library
- DPI combines pattern matching, behavioral, statistical and heuristic analysis
- Proven signatures for most of today's network protocols, incl. Web, P2P, VoIP, IM, Skype, media streaming and many more
- Reliable detection of proprietary, obfuscated and encrypted protocols
- No false classification
- Flexible and portable to any architecture
- Streamlined integration process
- Regular signature updates

ipoque's Protocol and Application Classification Engine (PACE) uses a combination of deep packet inspection (DPI) technologies, including pattern matching, behavioral and statistical analysis, to reliably detect protocols even if they use advanced obfuscation and encryption techniques. It helps network equipment and software vendors to enhance their products with powerful and proven layer-7 protocol management capabilities. PACE has been optimized for performance and classification reliability. It is highly flexible and can be integrated in any existing platform such as firewalls, network security appliances and lawful interception systems.

Application Scenarios

Next-Generation Firewalls & WAN Optimization Controllers (WOC)

Reliably classify network protocols and applications, independent of TCP and UDP ports, for network access control

Traffic Analysis, Accounting and Billing Systems

Collect detailed and rich network statistics based on actual protocol and application usage for performance monitoring, network resource planning, billing and accounting

Bandwidth Management

Network bandwidth management to provide quality of service (QoS) in fixed-line and mobile networks with per-protocol and per-application bandwidth priorities, guarantees and caps

Lawful Interception

Reliably classify intercepted traffic for negative and positive filtering, protocol-based load balancing and improved post-processing

Advanced Deep Packet Inspection Engine

PACE is a software library which detects and classifies protocols and applications from a network packet stream. It uses a wide range of deep packet inspection (DPI) technologies, including pattern matching, behavioral, statistical and heuristic analysis. Based on this combination, PACE is able to reliably detect proprietary, encrypted and obfuscated protocols with a very low false negative rate and virtually no false positives.

PACE – Beyond Protocol Detection

- Sub-protocol detection allows to differentiate between various connection types initiated by the same application, such as audio, file transfer, encrypted and unencrypted
- Symmetric and asymmetric traffic detection
- Decapsulates tunneling protocols with arbitrary encapsulation depth
- Statistical traffic measurements: TCP SYN to SYN/ACK and SYN/ACK to ACK round-trip time measurement, TCP out-of-order counter
- RTP performance measurements provide jitter and packet loss information
- Metadata extraction for HTTP, SIP and SSL in real time
- RTP flows are optionally correlated with the corresponding protocol that initiated them (e.g. SIP, MSN, Yahoo)
- Low-impact signature upgrade by flow state preservation before reboot

Custom Protocol Definition

Custom Protocol Definitions allow to extend the PACE signature database with a combination of the following additional layer-4 and layer-7 criteria:

- Layer-4 protocol (i.e. TCP, UDP)
- Layer-4 ports (lists and ranges of source and destination ports)
- Layer-7 protocol
- HTTP host list or URL list for HTTP-based layer-7 protocols
- Traffic direction (i.e. inbound, outbound)

Highly Optimized Implementation

Performance

- Developed entirely in C
- High throughput for deployment in core network links operating at speeds of 10 Gbit/s and beyond
- Integrated highly optimized flow tracking for millions of concurrent connections
- Less than 2,000 CPU cycles on average per complete protocol detection
- Less than 1,000 CPU cycles on average per flow for the built-in flow tracking code
- Fastpath implementation that analyzes only as much packets per flow as necessary for a reliable protocol detection; later packets simply pass by the detection engine saving valuable CPU resources

Memory Footprint

- 392 bytes per flow
- 816 bytes per network user or subscriber
- 50 kbytes for initialization data structures

The entire memory is allocated at initialization. During packet processing, PACE does not dynamically allocate any memory.

Flexible Integration in Any Target Platform

- Runs on virtually any hardware architecture with at least 32-bit processor and C compiler
- Can be used as a dynamic or static library in user space or as a kernel module in kernel space
- 32-bit & 64-bit compatible
- Little & big endian architectures
- Runs on any Linux and Windows environments
- 100% proprietary code provides clean licensing without GPL compliance issues
- Optional GPL-compliant Linux Netfilter wrapper for user space operation
- Integrated connection/session tracking engine; existing implementations can also be used

Field-Proven & Widely Deployed

PACE is the heart of ipoque's PRX Traffic Manager and DPX Network Probe with over 200 installations in more than 50 countries across the globe. PACE has also been successfully integrated in third-party firewalls, WAN optimization controllers, lawful interception systems and 3G/4G mobile network data gateway systems.

Maintenance & Support

- Regular signature updates for reliable protocol classification
- Support for new protocols and applications can usually be provided in less than one month
- Development support for a streamlined integration process

"Implementing traffic management for P2P and IM protocols for our Netfence gateway product line was a straightforward and efficient process with ipoque's PACE solution. Outstanding performance, ease of implementation and responsive support confirmed ipoque was the best solution to fit our needs."

Dr. Klaus Gheri, CTO & Co-Founder phion AG

ipoque GmbH, Mozartstr. 3, 04107 Leipzig, Germany
Phone: +49-341-59403-0 Fax: +49-341-59403-019

www.ipoque.com
info@ipoque.com

rev.2010-05-26