

DATA SHEET

PADE

PROTOCOL & APPLICATION DECODING ENGINE

ipoque Protocol and Application Decoding Engine (PADE) is a software library for integration in networking equipment and for standalone use. It extracts information from network application data transmissions and presents them with configurable level of detail ranging from individual events to fully aggregated and correlated session transcripts.



APPLICATION SCENARIOS

Lawful interception and mass interception network probes

Generation of layer-7 IPDRs/CDRs – or Intercept-Related Information (IRI) – and decoding of Content of Communication (CC) in lawful interception (LI) and mass interception network probes

Backend decoding systems in lawful interception solutions

Extraction of application-layer meta data and fully decoded communication content from

recorded network trace data as well as live interception data from LI probes and mediation devices for data retention and post-processing

Traffic and bandwidth management systems

Extract application-layer and content criteria for bandwidth management and quality-of-service (QoS) rules

Next-generation firewalls

Enable data leakage prevention, deep security scans and network access control based on application- and content-layer criteria

HIGHLIGHTS

Full protocol and application decoding

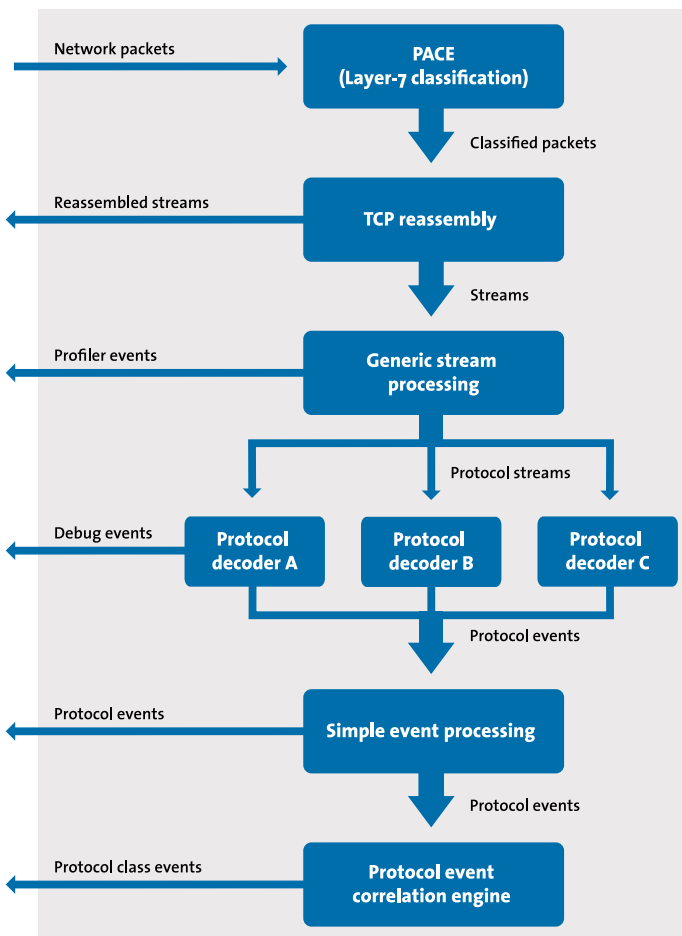
Extraction of all relevant information of the analyzed protocols

Real-time operation at multi-gigabit speeds

Comprehensive support for e-mail, messenger protocols and Web applications

IPv6 ready

Possibility for customers to add own decoders



Protocol class events

Individual protocol events of an application session are intelligently aggregated by a protocol event correlation engine into a single, more complex and well-structured protocol class event. This approach produces semantically rich information and significantly reduces the event output rate of the decoders, which makes post-processing much easier. For example, one protocol class event is triggered for each complete HTTP transaction, including all individual protocol operations, such as HTTP requests and responses, that are part of the transaction. Data transmissions originating from the same application are automatically correlated, e.g. voice and video transmissions are allocated to the corresponding messenger application. The same protocol types (e.g. e-mail, chat, search engine) generate the same event classes. For example, all chat protocols output user details, buddy lists, chats and file transfers using the same protocol class event format, no matter what application was used.

HIGHLY OPTIMIZED IMPLEMENTATION

Network Traffic Processing

- Full TCP reassembly to handle fragmented, duplicated and out-of-order packets
- Decapsulation and decoding support for tunnel traffic
- Uses ipoque's field-proven and widely deployed Protocol and Application Classification Engine (PACE), that is based on advanced deep packet inspection (DPI), behavioral and statistical protocol analysis, to feed the correct packets into each decoder module

Performance

- Developed entirely in C
- Suitable for both real-time and offline processing
- Easy scalability with built-in load balancing and symmetric multi-processing (SMP) support
- Multi-gigabit throughput on single multi-core systems
- Low, predictable and stable memory consumption

NEXT GENERATION EVENT ENGINE

PADE extracts comprehensive information from network application signaling and data transmissions. It produces clearly structured output with configurable granularity using two types of events: simple protocol events and aggregated protocol class events.

Protocol events

One event is generated for each individual protocol operation providing the maximum level of detail in real-time. For example, each HTTP request immediately triggers a protocol event.

SUPPORTED TARGET ENVIRONMENTS

- C, Java
- Linux, distribution-independent
- 32-bit & 64-bit compatible
- Little & big endian architectures
- Runs on every hardware platform that supports Linux

SUPPORTED PROTOCOLS

Standard

HTTP*
FTP
RADIUS*
DHCP*
Telnet
DNS*

Tunnel Protocols

L2TPv2

E-mail/Webmail

SMTP*
POP3*
IMAP*

Yahoo Mail

Gawab
Maktoob
Mail.com
GMX
Hotmail

Chat

Oscar (AIM and ICQ)
ICQ 6.5
ICQ 7.1
AIM 6.1
Pidgin 2.6.6
Jabber /XMPP
Google Talk

Yahoo Messenger

Yahoo 10.0
Pidgin 2.6.6
Paltalk
Paltalk 9.8101.3701
Paltalk 9.9103.4199
MSN
MSN 14.0.8089
Pidgin 2.6.6
IRC
xchat 2.8.6 Windows
xchat 2.8.8 Linux
MSN Webchat
ICQ Webchat

YAHOO Webchat

eBuddy Webchat
VoIP
SIP*
RTP
P2P
BitTorrent
eDonkey

Search Engines

Google Search
Bing Search
Yahoo Search

Social Networks

Facebook
Friendster
Hi5
LinkedIn
MySpace
Orkut
Twitter

*asymmetric support