International Working Group
on Data Protection
in Telecommunications

675.41.10 7 September 2010

Working Paper on the Use of Deep Packet Inspection for Marketing Purposes

48th meeting, 6-7 September 2010, Berlin, Germany

Deep Packet Inspection (DPI) is a technology that automates the inspection[1], in real or near-real time, of the header and content portions of data packets being transmitted on networks.

An Internet packet or datagram is generally composed of a 'datagram header' and a 'datagram data area'. The datagram header is the portion of the packet that contains information such as source and destination IP address and other details necessary to get the packet where it needs to go as it traverses the network. The datagram data area is referred to as the 'payload' because it is the content that the datagram header (the 'envelope') generally delivers. The packet header refers to any information a carrier requires to convey its telecommunications message, and the message itself is referred to as the content or payload of that telecommunications message.

While DPI cannot be considered a new technology, having been used for years in intrusion detection and prevention systems as well as in firewall systems, additional uses – enabled by increased computing power and more efficient algorithms – for traffic management, control over the dissemination of illegal or unwanted content – including copyrighted material – and even for delivering targeted advertisements to Internet users have been discussed and started to be introduced more recently.

The application of this technology can put the privacy of Internet users at risk. In particular, certain uses of DPI technologies by Internet access providers can result in severe infringements of privacy of Internet users. Access providers are the "gateway to the virtual world"; they are technically able to monitor the content of the entire communication of an Internet user. It is therefore essential that Internet access providers respect telecommunications secrecy, as laid down in the legal frameworks of many jurisdictions. In addition, Internet access providers in many cases not only offer Internet access, but also voice telephony services, as well as access to media, such as cable television. Providers of such "triple play"-services can – technically speaking – gain an even more detailed profile of the communications behaviour of their customers. Furthermore, with the advent of new and innovative services like telemedicine, more and more personal data of a particularly sensitive nature (such as health data) may be transmitted through facilities offered by Internet access providers.

The Working Group has strong reservations about the application of DPI for any purposes other than maintaining the security of information systems and networks within an organisation[2], or as otherwise allowed or required by applicable legislation.

[1] In computing, a firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a predefined rule will be allowed by the firewall, others will be rejected. Packet filters, or normal packet inspection, operates at the network layer (layer-3) and looks only at the header part of a packet, such as source and destination IP address. Deep Packet Inspection (DPI) is a firewall technology that operates at the application level (layer-7) of the OSI model. DPI enables the inspection, of the content of data packets being transmitted, such as HTTP communication and VOIP payload.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Specifically, the Working Group is concerned that any additional applications of DPI by Internet access providers and other ISPs will result in the further erosion of telecommunications secrecy. It will also damage the trust relation between these providers and their customers.

The application of DPI by Internet access providers can amount to the information society equivalent to wiretapping telephone conversations. The Group reinforces its position already laid down in earlier publications that, as a matter of principle, Network and Service Providers (including Internet access providers) must not intercept or interfere with any content of communications except where explicitly allowed or required by applicable legislation[3] (informational separation of powers). Nowadays this is also discussed under the heading of "network neutrality".

Recommendations

In the light of the above, the Working Group calls upon Internet access providers to specifically refrain from using DPI technology for targeted/behavioural advertising.

In addition, the Working Group calls for more widespread application of secure end-to-end encryption mechanisms. The (optional) provision of such technologies should be mandated by law where this is not already the case, at least for content providers offering services that involve the processing of sensitive data (e.g. online banking, uses involving credit card information, health data, etc.) as well as providers of communications services (like e-mail, chat, VoIP, etc.)[4].

[2] Cf. Working Paper on Intrusion Detection systems (IDS) (Berlin, 02./03.09.2003); http://www.datenschutz-berlin.de/attachments/203/ids_en.pdf?1177660658

[3] Cf. Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[4] Cf. Report and Guidance on Data Protection and Privacy on the Internet (Budapest-Berlin Memorandum) (Berlin, 19.11.1996), Item 7 on page 2; http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389