WIKIPEDIA

Deep packet inspection

Deep packet inspection (**DPI**) is a type of data processing that inspects in detail the data being sent over a computer network, and may take actions such as alerting, blocking, re-routing, or logging it accordingly. Deep packet inspection is often used to baseline application behavior, analyze network usage, troubleshoot network performance, ensure that data is in the correct format, check for malicious code, eavesdropping, and internet censorship,[1] among other purposes. There are multiple headers for IP packets; network equipment only needs to use the first of these (the IP header) for normal operation, but use of the second header (such as TCP or UDP) is normally considered to be shallow packet inspection (usually called stateful packet inspection) despite this definition.[2]

There are multiple ways to acquire packets for deep packet inspection. Using port mirroring (sometimes called Span Port) is a very common way, as well physically inserting a network tap which duplicates and sends the data stream to an analyzer tool for inspection.

Deep Packet Inspection (and filtering) enables advanced network management, user service, and security functions as well as internet data mining, eavesdropping, and internet censorship. Although DPI has been used for Internet management for many years, some advocates of net neutrality fear that the technique may be used anticompetitively or to reduce the openness of the Internet.[3]

DPI is used in a wide range of applications, at the so-called "enterprise" level (corporations and larger institutions), in telecommunications service providers, and in governments.[4]

Contents

Background

DPI technology boasts a long and technologically advanced history, starting in the 1990s, before the technology entered what is seen today as common, mainstream deployments. The technology traces its roots back over 30 years, when many of the pioneers contributed their inventions for use among industry participants, such as through common standards and early innovation, such as the following:

- RMON
- Sniffer
- Wireshark

Essential DPI functionality includes analysis of packet headers and protocol fields. For example, Wireshark offers essential DPI functionality through its numerous dissectors that display field names and content and, in some cases, offer interpretation of field values.

Some security solutions that offer DPI combine the functionality of an intrusion detection system (IDS) and an Intrusion prevention system (IPS) with a traditional stateful firewall.[5] This combination makes it possible to detect certain attacks that neither the IDS/IPS nor the stateful firewall can catch on their own. Stateful firewalls, while able to see the beginning and end of a packet flow, cannot catch events on their own that would be out of bounds for a particular application. While IDSs are able to detect intrusions, they have very little capability in blocking such an attack. DPIs are used to prevent attacks from viruses and worms at wire speeds. More specifically, DPI can be effective against buffer overflow attacks, denial-of-service attacks (DoS), sophisticated intrusions, and a small percentage of worms that fit within a single packet.[6]

DPI-enabled devices have the ability to look at Layer 2 and beyond Layer 3 of the OSI model. In some cases, DPI can be invoked to look through Layer 2-7 of the OSI model. This includes headers and data protocol structures as well as the payload of the message. DPI functionality is invoked when a device looks or takes other action based on information beyond Layer 3 of the OSI model. DPI can identify and classify traffic based on a signature database that includes information extracted from the data part of a packet, allowing finer control than classification based only on header information. End points can utilize encryption and obfuscation techniques to evade DPI actions in many cases.

A classified packet may be redirected, marked/tagged (see quality of service), blocked, rate limited, and of course, reported to a reporting agent in the network. In this way, HTTP errors of different classifications may be identified and forwarded for analysis. Many DPI devices can identify packet flows (rather than packet-by-packet analysis), allowing control actions based on accumulated flow information.[7]

At the enterprise level

Initially security at the enterprise level was just a perimeter discipline, with a dominant philosophy of keeping unauthorized users out, and shielding authorized users from the outside world. The most frequently used tool for accomplishing this has been a stateful firewall. It can permit fine-grained control of access from the outside world to pre-defined destinations on the internal network, as well as permitting access back to other hosts only if a request to the outside world has been made previously.[8]

Vulnerabilities exist at network layers, however, that are not visible to a stateful firewall. Also, an increase in the use of laptops in enterprise makes it more difficult to prevent threats such as viruses, worms, and spyware from penetrating the corporate network, as many users will connect the laptop to less-secure networks such as home broadband connections or wireless networks in public locations. Firewalls also do not distinguish between permitted and forbidden uses of legitimately-accessed applications. DPI enables IT administrators and security officials to set policies and enforce them at all layers, including the application and user layer to help combat those threats.[9][10]

Deep Packet Inspection is able to detect a few kinds of buffer overflow attacks.

DPI may be used by enterprise for Data Leak Prevention (DLP). When an e-mail user tries to send a protected file, the user may be given information on how to get the proper clearance to send the file.[11]

At network/Internet service providers

In addition to using DPI to secure their internal networks, Internet service providers also apply it on the public networks provided to customers. Common uses of DPI by ISPs are lawful intercept, policy definition and enforcement, targeted advertising, quality of service, offering tiered services, and copyright enforcement.

Lawful interception

Service providers are required by almost all governments worldwide to enable lawful intercept capabilities. Decades ago in a legacy telephone environment, this was met by creating a traffic access point (TAP) using an intercepting proxy server that connects to the government's surveillance equipment. The acquisition component of this functionality may be provided in many ways, including DPI, DPI-enabled products that are "LI or CALEA-compliant" can be used – when directed by a court order – to access a user's datastream.[12]

Policy definition and enforcement

Service providers obligated by the service-level agreement with their customers to provide a certain level of service and at the same time, enforce an acceptable use policy, may make use of DPI to implement certain policies that cover copyright infringements, illegal materials, and unfair use of bandwidth. In some countries the ISPs are required to perform filtering, depending on the country's laws. DPI allows service providers to "readily know the packets of information you are receiving online—from e-mail, to websites, to sharing of music, video and software downloads".[13] Policies can be defined that allow or disallow connection to or from an IP address, certain protocols, or even heuristics that identify a certain application or behavior.

Targeted advertising

Because ISPs route the traffic of all of their customers, they are able to monitor web-browsing habits in a very detailed way allowing them to gain information about their customers' interests, which can be used by companies specializing in targeted advertising. At least 100,000 United States customers are tracked this way, and as many as 10% of U.S. customers have been tracked in this way.[14] Technology providers include NebuAd, Front Porch, and Phorm. U.S. ISPs monitoring their customers include Knology[15] and Wide Open West. In addition, the United Kingdom ISP British Telecom has admitted testing solutions from Phorm without their customers' knowledge or consent.[14]

Quality of service

DPI can be used against net neutrality.

Applications such as peer-to-peer (P2P) traffic present increasing problems for broadband service providers. Typically, P2P traffic is used by applications that do file sharing. These may be any kind of files (i.e. documents, music, videos, or applications). Due to the frequently large size of media files being transferred, P2P drives increasing traffic loads, requiring additional network capacity. Service providers say a minority of users generate large quantities of P2P traffic and degrade performance for the majority of broadband subscribers using applications such as e-mail or Web browsing which use less bandwidth.[16] Poor network performance increases customer dissatisfaction and leads to a decline in service revenues.

DPI allows the operators to oversell their available bandwidth while ensuring equitable bandwidth distribution to all users by preventing network congestion. Additionally, a higher priority can be allocated to a VoIP or video conferencing call which requires low latency versus web browsing which does not.[17] This is the approach that service providers use to dynamically allocate bandwidth according to traffic that is passing through their networks.

Tiered services

Mobile and broadband service providers use DPI as a means to implement tiered service plans, to differentiate "walled garden" services from "value added", "all-you-can-eat" and "one-size-fits-all" data services.[18] By being able to charge for a "walled garden", per application, per service, or "all-you-can-eat" rather than a "one-size-fits-all" package, the operator can tailor his offering to the individual subscriber and increase their average revenue per user (ARPU). A policy is created per user or user group, and the DPI system in turn enforces that policy, allowing the user access to different services and applications.

Copyright enforcement

ISPs are sometimes requested by copyright owners or required by courts or official policy to help enforce copyrights. In 2006, one of Denmark's largest ISPs, Tele2, was given a court injunction and told it must block its customers from accessing The Pirate Bay, a launching point for BitTorrent.[19]

Instead of prosecuting file sharers one at a time,[20] the International Federation of the Phonographic Industry (IFPI) and the big four record labels EMI, Sony BMG, Universal Music, and Warner Music have sued ISPs such as Eircom for not doing enough about protecting their copyrights.[21] The IFPI wants ISPs to filter traffic to remove illicitly uploaded and downloaded copyrighted material from their network, despite European directive 2000/31/EC clearly stating that ISPs may not be put under a general obligation to monitor the information they transmit, and directive 2002/58/EC granting European citizens a right to privacy of communications.

The Motion Picture Association of America (MPAA) which enforces movie copyrights, has taken the position with the Federal Communications Commission (FCC) that network neutrality could hurt anti-piracy techniques such as deep packet inspection and other forms of filtering.[22]

Statistics

DPI allows ISPs to gather statistical information about use patterns by user group. For instance, it might be of interest whether users with a 2Mbit connection use the network in a dissimilar manner to users with a 5Mbit connection. Access to trend data also helps network planning.

By governments

In addition to using DPI for the security of their own networks, governments in North America, Europe, and Asia use DPI for various purposes such as surveillance and censorship. Many of these programs are classified.[23]

United States

FCC adopts Internet CALEA requirements: The FCC, pursuant to its mandate from the U.S. Congress, and in line with the policies of most countries worldwide, has required that all telecommunication providers, including Internet services, be capable of supporting the execution of a court order to provide real-time communication forensics of specified users. In 2006, the FCC adopted new Title 47, Subpart Z, rules requiring Internet Access Providers to meet these requirements. DPI was one of the platforms essential to meeting this requirement and has been deployed for this purpose throughout the U.S.

The National Security Agency (NSA), with cooperation from AT&T Inc., has used Deep Packet Inspection to make internet traffic surveillance, sorting, and forwarding more intelligent. The DPI is used to find which packets are carrying e-mail or a Voice over Internet Protocol (VoIP) telephone call.[24] Traffic associated with AT&T's Common Backbone was "split" between two fibers, dividing the signal so that 50 percent of the signal strength went to each output fiber. One of the output fibers was diverted to a secure room; the other carried communications on to AT&T's switching equipment. The secure room contained Narus traffic analyzers and logic servers; Narus states that such devices are capable of real-time data collection (recording data for consideration) and capture at 10 gigabits per second. Certain traffic was selected and sent over a dedicated line to a "central location" for analysis. According to an affidavit by expert witness J. Scott Marcus, a former senior advisor for Internet Technology at the US Federal Communications Commission, the diverted traffic "represented all, or substantially all, of AT&T’s peering traffic in the San Francisco Bay area", and thus, "the designers of the ... configuration made no attempt, in terms of location or position of the fiber split, to exclude data sources comprised primarily of domestic data".[25] Narus's Semantic Traffic Analyzer software, which runs on IBM or Dell Linux servers using DPI, sorts through IP traffic at 10Gbit/s to pick out specific messages based on a targeted e-mail address, IP address or, in the case of VoIP, telephone number.[26] President George W. Bush and Attorney General Alberto R. Gonzales have asserted that they believe the president has the authority to order secret intercepts of telephone and e-mail exchanges between people inside the United States and their contacts abroad without obtaining a FISA warrant.[27]

The Defense Information Systems Agency has developed a sensor platform that uses Deep Packet Inspection.[28]

China

The Chinese government uses Deep Packet Inspection to monitor and censor network traffic and content that it claims is harmful to Chinese citizens or state interests. This material includes pornography, information on religion, and political dissent.[29] Chinese network ISPs use DPI to see if there is any sensitive keyword going through their network. If so, the connection will be cut. People within China often find themselves blocked while accessing Web sites containing content related to Taiwanese and Tibetan independence, Falun Gong, the Dalai Lama, the Tiananmen Square protests and massacre of 1989, political parties that oppose that of the ruling Communist party, or a variety of anti-Communist movements[30] as those materials were signed as DPI sensitive keywords already. China previously blocked all VoIP traffic in and out of their country[31] but many available VOIP applications now function in China. Voice traffic in Skype is unaffected, although text messages are subject to filtering, and messages containing sensitive material, such as curse-words, are simply not delivered, with no notification provided to either participant in the conversation. China also blocks visual media sites such as YouTube.com and various photography and blogging sites.[32]

High-ranking websites blocked in mainland China using Deep Packet Inspection

Alexa rank	Website	Domain	URL	Category	Primary language
6	Wikipedia	wikipedia.org	www.wikipedia.org	Censorship-free encyclopedia	English
1	Google	google.com	www.google.com	Worldwide Internet search engine	English
1	Google Encrypted	google.com	encrypted.google.com	Search	English
2	Facebook	facebook.com	www.facebook.com	Social network	English
3	YouTube	youtube.com	www.youtube.com	Video	English
557	JW.ORG	jw.org	www.jw.org	Spiritual, Christianity	Multilingual
24693	OpenVPN	openvpn.net	www.openvpn.net	Avoidance of political internet censorship	English
33553	Strong VPN	strongvpn.com	www.strongvpn.com	Avoidance of political internet censorship	English
78873	Falun Dafa	falundafa.org	www.falundafa.org	Spiritual	English
1413995	VPN Coupons	vpncoupons.com	www.vpncoupons.com	Avoidance of political internet censorship	English
2761652	ElephantVPN	elephantvpn.com	www.elephantvpn.com	Avoidance of political internet censorship	English

Iran

The Iranian government purchased a system, reportedly for deep packet inspection, in 2008 from Nokia Siemens Networks (NSN) (a joint venture Siemens AG, the German conglomerate, and Nokia Corp., the Finnish cell telephone company), now NSN is Nokia Solutions and Networks, according to a report in the *Wall Street Journal* in June, 2009, quoting NSN spokesperson Ben Roome.[33] According to unnamed experts cited in the article, the system "enables authorities to not only block communication but to monitor it to gather information about individuals, as well as alter it for disinformation purposes".

The system was purchased by the Telecommunication Infrastructure Co., part of the Iranian government's telecom monopoly. According to the *Journal*, NSN "provided equipment to Iran last year under the internationally recognized concept of 'lawful intercept,' said Mr. Roome. That relates to intercepting data for the purposes of combating terrorism, child pornography, drug trafficking, and other criminal activities carried out online, a capability that most if not all telecom companies have, he said.... The monitoring center that Nokia Siemens Networks sold to Iran was described in a company brochure as allowing 'the monitoring and interception of all types of voice and data communication on all networks.' The joint venture exited the business that included the monitoring equipment, what it called 'intelligence solution,' at the end of March, by selling it to Perusa[34] Partners Fund 1 LP, a Munich-based investment firm, Mr. Roome said. He said the company determined it was no longer part of its core business.

The NSN system followed on purchases by Iran from Secure Computing Corp. earlier in the decade.[35]

Questions have been raised about the reporting reliability of the *Journal* report by David Isenberg, an independent Washington, D.C.-based analyst and Cato Institute Adjunct Scholar, specifically saying that Mr. Roome is denying the quotes attributed to him and that he, Isenberg, also had similar complaints with one of the same *Journal* reporters in an earlier story.[36] NSN has issued the following denial: NSN "has not provided any deep packet inspection, web censorship or Internet filtering capability to Iran".[37] A concurrent article in *The New York Times* stated the NSN sale had been covered in a "spate of news reports in April [2009], including *The Washington Times*," and reviewed censorship of the Internet and other media in the country, but did not mention DPI.[38]

According to Walid Al-Saqaf, the developer of the internet censorship circumventor Alkasir, Iran was using deep packet inspection in February 2012, bringing internet speeds in the entire country to a near standstill. This briefly eliminated access to tools such as Tor and Alkasir.[39]

Russian Federation

DPI is not yet mandated in Russia. Federal Law No.139 enforces blocking websites on the Russian Internet blacklist using IP filtering, but does not force ISPs into analyzing the data part of packets. Yet some ISPs still use different DPI solutions to implement blacklisting. For 2019, the governmental agency Roskomnadzor is planning a nationwide rollout of DPI after the pilot project in one of the country's regions, at an estimated cost of 20 billion roubles (US$300M).[40]

Some human rights activists consider Deep Packet inspection contrary to Article 23 of the Constitution of the Russian Federation, though a legal process to prove or refute that has never taken place.[41]

Singapore

The city state reportedly employs deep packet inspection of Internet traffic.[42]

Syria

The state reportedly employs deep packet inspection of Internet traffic, to analyze and block forbidden transit.

Malaysia

The incumbent Malaysian government, headed by Barisan Nasional, was said to be using DPI against a political opponent during the run-up to the 13th general elections held on 5 May 2013.

The purpose of DPI, in this instance, was to block and/or hinder access to selected websites, e.g. Facebook accounts, blogs and news portals. [43] [44]

Egypt

Since 2015, Egypt reportedly started to join the list which was constantly being denied by the Egyptian National Telecom Regulatory Authority (NTRA) officials. However, it came to news when the country decided to block the encrypted messaging app Signal as announced by the application's developer.[45]

In April 2017, all VOIP applications including FaceTime, Facebook Messenger, Viber, Whatsapp calls and Skype have been all blocked in the country.[46]

Vietnam

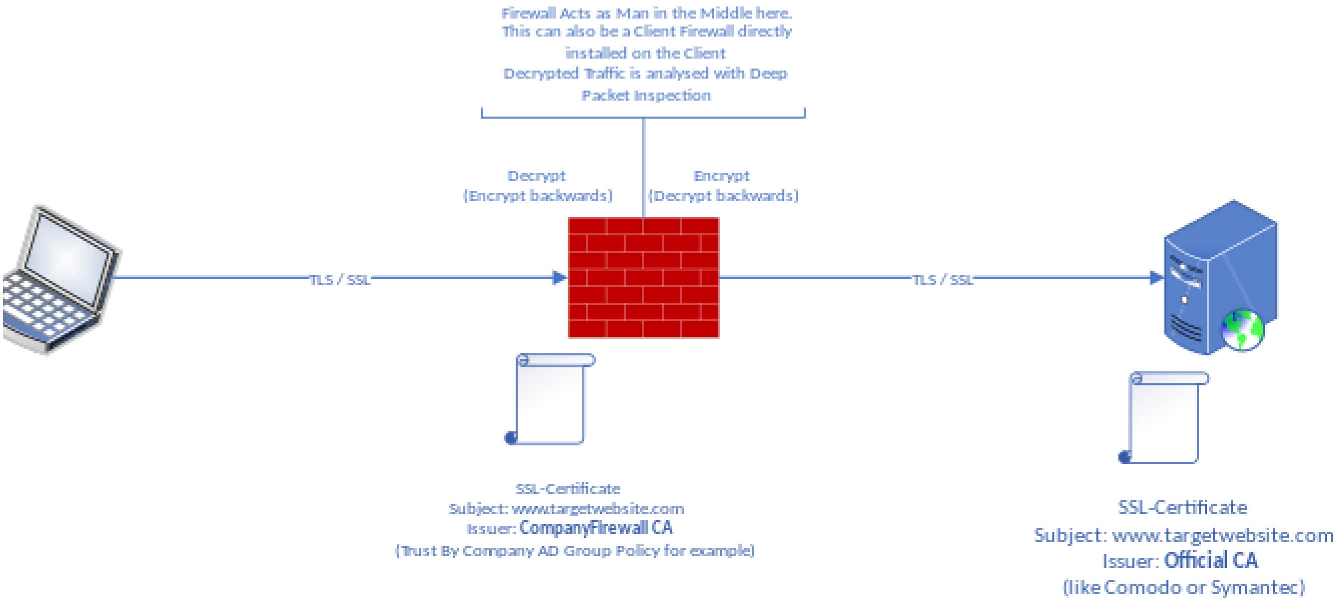
Vietnam launched its network security center and required ISPs to upgrade their hardware systems to use deep packet inspection to block Internet traffic.[47][48]

Net neutrality

People and organizations concerned about privacy or network neutrality find inspection of the content layers of the Internet protocol to be offensive,[12] saying for example, "the 'Net was built on open access and non-discrimination of packets!"[49] Critics of network neutrality rules, meanwhile, call them "a solution in search of a problem" and say that net neutrality rules would reduce incentives to upgrade networks and launch next-generation network services.[50]

Deep packet inspection is considered by many to undermine the infrastructure of the internet.[51]

Encryption and tunneling subverting DPI


Firewall Acts as Man in the Middle here.
This can also be a Client Firewall directly installed on the Client
Decrypted Traffic is analysed with Deep Packet Inspection
Decrypt
(Encrypt backwards)
Encrypt
(Decrypt backwards)
TLS / SSL
TLS / SSL
SSL-Certificate
Subject: www.targetwebsite.com
Issuer: CompanyFirewall CA
(Trust By Company AD Group Policy for example)
SSL-Certificate
Subject: www.targetwebsite.com
Issuer: Official CA
(like Comodo or Symantec)

L / TLS Deep Inspection

With increased use of HTTPS and privacy tunneling using VPNs, the effectiveness of DPI is coming into question.[52] In response, many web application firewalls now offer *HTTPS inspection*, where they decrypt HTTPS traffic to analyse it.[53] The WAF can either terminate the encryption, so the connection between WAF and client browser uses plain HTTP, or re-encrypt the data using its own HTTPS certificate, which must be distributed to clients beforehand.[54] The techniques used in HTTPS / SSL Inspection (also known as HTTPS / SSL Interception) are the same used by man-in-the-middle (MiTM) attacks[55]

It works like this:

1. Client wants to connect to https://www.targetwebsite.com
2. Traffic goes through Firewall or Security Product
3. Firewall works as transparent Proxy
4. Firewall Creates SSL Certificate signed by its own "CompanyFirewall CA"
5. Firewall presents this "CompanyFirewall CA" Signed Certificate to Client (not the targetwebsite.com Certificate)
6. At the same time the Firewall on its own connects to https://www.targetwebsite.com
7. targetwebsite.com Presents its Officially Signed Certificate (Signed by a Trusted CA)
8. Firewall checks Certificate Trust chain on its own
9. Firewall now works as Man-in-the-middle.
10. Traffic from Client will be decrypted (with Key Exchange Information from Client), analysed (for harmful traffic, policy violation or viruses), encrypted (with Key Exchange Information from targetwebsite.com) and sent to targetwebsite.com
11. Traffic from targetwebsite.com will also be decrypted (with Key Exchange Information from targetwebsite.com), analysed (like above), encrypted (with Key Exchange Information from Client) and sent to Client.
12. The Firewall Product can read all information exchanged between SSL-Client and SSL-Server (targetwebsite.com)

This can be done with any TLS-Terminated connection (not only HTTPS) as long as the firewall product can modify the TrustStore of the SSL-Client

Infrastructure security

Traditionally the mantra which has served ISP well has been to only operate at layer 4 and below of the OSI model. This is because simply deciding where packets go and routing them is comparably very easy to handle securely. This traditional model still allows ISPs to accomplish required tasks safely such as restricting bandwidth depending on the amount of bandwidth that is used (layer 4 and below) rather than per protocol or application type (layer 7). There is a very strong and often ignored argument that ISP action above layer 4 of the OSI model provides what are known in the security community as 'stepping stones' or platforms to conduct man in the middle attacks from. This problem is exacerbated by ISP's often choosing cheaper hardware with poor security track records for the very difficult and arguably impossible to secure task of Deep Packet Inspection.

OpenBSD's packet filter specifically avoids DPI for the very reason that it cannot be done securely with confidence.

This means that DPI dependent security services such as TalkTalk's former HomeSafe implementation are actually trading the security of a few (protectable and often already protectable in many more effective ways) at a cost of decreased security for all where users also have a far less possibility of mitigating the risk. The HomeSafe service in particular is opt in for blocking but its DPI cannot be opted out of, even for business users.[56]

Software

nDPI (http://www.ntop.org/products/ndpi/) (a fork from OpenDPI[57] which is EoL by the developers of ntop)[58][59] is the open source version for non-obfuscated protocols. PACE, another such engine, includes obfuscated and encrypted protocols, which are the types associated with Skype or encrypted BitTorrent.[60] As OpenDPI is no longer maintained, an OpenDPI-fork named nDPI[61] has been created, actively maintained and extended with new protocols including Skype, Webex, Citrix and many others.

L7-Filter is a classifier for Linux's Netfilter that identifies packets based on application layer data.[62] It can classify packets such as Kazaa, HTTP, Jabber, Citrix, Bittorrent, FTP, Gnucleus, eDonkey2000, and others. It classifies streaming, mailing, P2P, VOIP, protocols, and gaming applications. The software has been retired and replaced by the open source Netify DPI Engine.[63]

Hippie (Hi-Performance Protocol Identification Engine) is an open source project which was developed as Linux kernel module.[64] It was developed by Josh Ballard. It supports both DPI as well as firewall functionality.[65]

SPID (Statistical Protocol IDentification) project is based on statistical analysis of network flows to identify application traffic.[66] The SPID algorithm can detect the application layer protocol (layer 7) by signatures (a sequence of bytes at a particular offset in the handshake), by analyzing flow information (packet sizes, etc.) and payload statistics (how frequently the byte value occurs in order to measure entropy) from pcap files. It is just a proof of concept application and currently supports approximately 15 application/protocols such as eDonkey Obfuscation traffic, Skype UDP and TCP, BitTorrent, IMAP, IRC, MSN, and others.

Tstat (TCP STatistic and Analysis Tool) provides insight into traffic patterns and gives details and statistics for numerous applications and protocols.[67]

Libprotoident introduces Lightweight Packet Inspection (LPI), which examines only the first four bytes of payload in each direction. That allows to minimize privacy concerns, while decreasing the disk space needed to store the packet traces necessary for the classification. Libprotoident supports over 200 different protocols and the classification is based on a combined approach using payload pattern matching, payload size, port numbers, and IP matching.[68]

A French company called Amesys, designed and sold an intrusive and massive internet monitoring system *Eagle* to Muammar Gaddafi.[69]

Comparison

A comprehensive comparison of various network traffic classifiers, which depend on Deep Packet Inspection (PACE, OpenDPI, 4 different configurations of L7-filter, NDPI, Libprotoident, and Cisco NBAR), is shown in the Independent Comparison of Popular DPI Tools for Traffic Classification.[70]

Hardware

There is a greater emphasis being placed on deep packet inspection - this comes in light after the rejection of both the SOPA and PIPA bills. Many current DPI methods are slow and costly, especially for high bandwidth applications. More efficient methods of DPI are being developed. Specialized routers are now able to perform DPI; routers armed with a dictionary of programs will help identify the purposes behind the LAN and internet traffic they are routing. Cisco Systems is now on their second iteration of DPI enabled routers, with their announcement of the CISCO ISR G2 router.[71]

See also

- Common carrier
- Data Retention Directive
- Deep content inspection
- ECHELON
- Firewall
- Foreign Intelligence Surveillance Act
- Golden Shield
- Intrusion prevention system
- Network neutrality
- NSA warrantless surveillance controversy
- Packet analyzer
- Stateful firewall
- Theta Networks
- Wireshark

References

1. Duncan Geere, https://www.wired.co.uk/article/how-deep-packet-inspection-works
2. Thomas Porter (2005-01-11). "The Perils of Deep Packet Inspection" (http://www.securityfocus.com/infocus/1817). securityfocus.com. Retrieved 2008-03-02.
3. Hal Abelson; Ken Ledeen; Chris Lewis (2009). "Just Deliver the Packets, in: "Essays on Deep Packet Inspection", Ottawa" (https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2009/ledeen-lewis_200903/). Office of the Privacy Commissioner of Canada. Retrieved 2010-01-08.
4. Ralf Bendrath (2009-03-16). "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection, Paper presented at the International Studies Annual Convention, New York City, 15–18 February 2009" (http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf) (PDF). International Studies Association. Retrieved 2010-01-08.
5. Ido Dubrawsky (2003-07-29). "Firewall Evolution - Deep Packet Inspection" (http://www.securityfocus.com/infocus/1716). securityfocus.com. Retrieved 2008-03-02.
6. Khachatryan, Artavazd (2020-02-01). "100Gbps Network DPI, Content Extraction on Xilinx's FPGA" (https://medium.com/grovf/100gbps-network-dpi-content-extraction-on-xilinxs-fpga-2996d661042a). *Medium*. Retrieved 2020-10-23.
7. Moscola, James, et al. "Implementation of a content-scanning module for an internet firewall." Field-Programmable Custom Computing Machines, 2003. FCCM 2003. 11th Annual IEEE Symposium on. IEEE, 2003.
8. Elan Amir (2007-10-29). "The Case for Deep Packet Inspection" (http://www.itbusinessedge.com/item/?ci=35275). itbusinessedge.com. Retrieved 2008-03-02.
9. Noferesti, Morteza; Jalili, Rasool (2020-01-15). "ACoPE: An adaptive semi-supervised learning approach for complex-policy enforcement in high-bandwidth networks" (https://www.sciencedirect.com/science/article/abs/pii/S1389128619304074). *Computer Networks*. **166**: 106943. doi:10.1016/j.comnet.2019.106943 (https://doi.org/10.1016%2Fj.comnet.2019.106943). ISSN 1389-1286 (https://www.worldcat.org/issn/1389-1286). S2CID 208094726 (https://api.semanticscholar.org/CorpusID:208094726).
10. "firewall" (https://searchsecurity.techtarget.com/definition/firewall).
11. Tahboub, Radwan; Saleh, Yousef (January 2014). "Data Leakage/Loss Prevention Systems (DLP)" (https://ieeexplore.ieee.org/document/6916624). *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*: 1–6. doi:10.1109/WCCAIS.2014.6916624 (https://doi.org/10.1109%2FWCCAIS.2014.6916624). S2CID 1022898 (https://api.semanticscholar.org/CorpusID:1022898).
12. Nate Anderson (2007-07-25). "Deep Packet Inspection meets 'Net neutrality, CALEA" (https://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars). ars technica. Retrieved 2006-02-06.

13. Jeff Chester (2006-02-01). "The End of the Internet?" (http://www.thenation.com/doc/20060213/chester). The Nation. Retrieved 2006-02-06.
14. Peter Whoriskey (2008-04-04). "Every Click You Make: Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising" (https://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html). *The Washington Post*. Retrieved 2008-04-08.
15. "Charter Communications: Enhanced Online Experience" (http://connect.charter.com/landing/op1.html). Retrieved 2008-05-14.
16. "Deep Packet Inspection: Taming the P2P Traffic Beast" (https://web.archive.org/web/20080302113455/http://www.lightreading.com/insider/details.asp?sku_id=1221&skuitem_itemid=957). Light Reading. Archived from the original (http://www.lightreading.com/insider/details.asp?sku_id=1221&skuitem_itemid=957) on 2008-03-02. Retrieved 2008-03-03.
17. Matt Hamblen (2007-09-17). "Ball State uses Deep Packet Inspection to ensure videoconferencing performance" (http://www.computerworld.com/article/2541004/networking/ball-state-uses-deep-packet-inspection-to-ensure-videoconferencing-performance.html). Computer World. Retrieved 2008-03-03.
18. "Allot Deploys DPI Solution at Two Tier 1 Mobile Operators to Deliver Value- Added and Tiered Service Packages" (https://news.moneycentral.msn.com/ticker/article.aspx?Feed=PR&Date=20080205&ID=8139811&Symbol=ALLT). news.moneycentral.msn.com. 2008-02-05. Retrieved 2008-03-03.
19. Jeremy Kirk (2008-02-13). "Danish ISP prepares to fight Pirate Bay injunction" (https://web.archive.org/web/20080214235115/http://www.infoworld.com/article/08/02/13/Danish-ISP-prepares-to-fight-Pirate-Bay-injunction_1.html). IDG News Service. Archived from the original (http://www.infoworld.com/article/08/02/13/Danish-ISP-prepares-to-fight-Pirate-Bay-injunction_1.html) on 2008-02-14. Retrieved 2008-03-12.
20. Matthew Clark (2005-07-05). "Eircom and BT won't oppose music firms" (https://archive.today/20070814234157/http://www.enn.ie/frontpage/news-9617239.html). enn.ie. Archived from the original (http://www.enn.ie/frontpage/news-9617239.html) on 2007-08-14. Retrieved 2008-03-12.
21. Eric Bangeman (2008-03-11). " "Year of filters" turning into year of lawsuits against ISPs" (https://arstechnica.com/news.ars/post/20080311-year-of-filters-turning-into-year-of-lawsuits-against-isps.html). ars technica. Retrieved 2008-03-12.
22. Anne Broach (2007-07-19). "MPAA: Net neutrality could hurt antipiracy tech" (http://www.news.com/8301-10784_3-9746938-7.html). CNET News. Retrieved 2008-03-12.
23. Carolyn Duffy Marsan (2007-06-27). "OEM provider Bivio targets government market" (http://www.networkworld.com/newsletters/isp/2007/0625isp1.html). Network World. Retrieved 2008-03-13.
24. J. I. Nelson (2006-09-26). "How the NSA warrantless wiretap system works" (http://www.nerdylorrin.net/jerry/politics/Warrantless/WarrantlessFACTS.html). Retrieved 2008-03-03.
25. Bellovin, Steven M.; Matt Blaze; Whitfield Diffie; Susan Landau; Peter G. Neumann; Jennifer Rexford (January–February 2008). "Risking Communications Security: Potential Hazards of the Protect America Act" (https://web.archive.org/web/20080227135042/http://www.crypto.com/papers/paa-ieee.pdf) (PDF). *IEEE Security and Privacy*. IEEE Computer Society. **6** (1): 24–33. doi:10.1109/MSP.2008.17 (https://doi.org/10.1109%2FMSP.2008.17). S2CID 874506 (https://api.semanticscholar.org/CorpusID:874506). Archived from the original (http://www.crypto.com/papers/paa-ieee.pdf) (PDF) on 2008-02-27. Retrieved 2008-03-03.
26. Robert Poe (2006-05-17). "The Ultimate Net Monitoring Tool" (https://www.wired.com/science/discoveries/news/2006/05/70914). *Wired*. Retrieved 2008-03-03.
27. Carol D. Leonnig (2007-01-07). "Report Rebuts Bush on Spying - Domestic Action's Legality Challenged" (https://www.washingtonpost.com/wp-dyn/content/article/2006/01/06/AR2006010601772.html). *The Washington Post*. Retrieved 2008-03-03.

28. Cheryl Gerber (2008-09-18). "Deep Security: DISA Beefs Up Security with Deep Packet Inspection of IP Transmissions" (https://web.archive.org/web/20110726003528/https://www.dpacket.org/articles/deep-security-disa-beefs-security-deep-packet-inpection-ip-transmissions). Archived from the original (https://www.dpacket.org/articles/deep-security-disa-beefs-security-deep-packet-inpection-ip-transmissions) on 2011-07-26. Retrieved 2008-10-30.
29. Ben Elgin; Bruce Einhorn (2006-01-12). "The Great Firewall of China" (https://web.archive.org/web/20080228174845/http://www.businessweek.com/technology/content/jan2006/tc20060112_434051.htm). Business Week. Archived from the original (http://www.businessweek.com/technology/content/jan2006/tc20060112_434051.htm) on 2008-02-28. Retrieved 2008-03-13.
30. "Internet Filtering in China in 2004-2005: A Country Study" (https://web.archive.org/web/20070928135524/http://www.opennetinitiative.net/studies/china/). Open Net Initiative. Archived from the original (http://www.opennetinitiative.net/studies/china/) on 2007-09-28. Retrieved 2008-03-13.
31. Guy Kewney, China blocks Skype, VoIP (https://www.theregister.co.uk/2005/09/12/china_blocks_skype/), The Register, 2005
32. "China Blocks YouTube, Restores Flickr and Blogspot" (http://www.pcworld.com/article/id,138599-c,sites/article.html). PC World. 2007-10-18. Retrieved 2008-03-03.
33. Christensen, Christian. "Iran: Networked dissent". *Le Monde Diplomatique 1*.
34. "Perusa :: Who we are" (https://web.archive.org/web/20150924071637/http://www.perusa-partners.de/english/who_we_are.php). *perusa-partners.de*. Archived from the original (http://www.perusa-partners.de/english/who_we_are.php) on 2015-09-24.
35. "Iran's Web Spying Aided By Western Technology" (https://www.wsj.com/articles/SB124562668777335653) by Christopher Rhoads in New York and Loretta Chao in Beijing, *The Wall Street Journal*, June 22, 2009. Retrieved 6/22/09.
36. "Questions about WSJ story on Net Management in Iran" (http://www.isen.com/blog/2009/06/questions-about-wsj-story-on-net.html) by David S. Isenberg, isen.blog, June 23, 2009. Retrieved 6/22/09.
37. "Provision of Lawful Intercept capability in Iran" (http://www.nokiasiemensnetworks.com/global/Press/Press+releases/news-archive/Provision+of+Lawful+Intercept+capability+in+Iran.htm) Archived (https://web.archive.org/web/20090625174434/http://www.nokiasiemensnetworks.com/global/Press/Press+releases/news-archive/Provision+of+Lawful+Intercept+capability+in+Iran.htm) June 25, 2009, at the Wayback Machine Company press release. June 22, 2009. Retrieved 6/22/09.
38. "Web Pries Lid of Iranian Censorship" (https://www.nytimes.com/2009/06/23/world/middleeast/23censor.html?_r=1&hp) by Brian Stelter and Brad Stone, *The New York Times*, June 22, 2009. Retrieved June 23, 2009.
39. February 14, 2012 "Breaking and Bending Censorship with Walid Al-Saqaf" (http://www.arsehsevom.net/2012/02/breaking-and-bending-censorship-with-walid-al-saqaf/) Archived (https://web.archive.org/web/20130502112534/http://www.arsehsevom.net/2012/02/breaking-and-bending-censorship-with-walid-al-saqaf/) May 2, 2013, at the Wayback Machine, an Interview with Arseh Sevom (http://www.arsehsevom.net/). Last viewed February 23, 2012.
40. "Roskomnadzor to deploy new blocking technology (in Russian)" (https://www.bbc.com/russian/features-46596673). *BBC News Русская Служба*. 18 December 2018.
41. Constitution of the Russian Federation (english translation) (http://www.government.ru/eng/gov/base/54.html)Archived (https://web.archive.org/web/20130504062759/http://www.government.ru/eng/gov/base/54.html) May 4, 2013, at the Wayback Machine
42. "Deep packet inspection rears it ugly head" (https://majid.info/blog/telco-snooping/). Retrieved 28 April 2015.

43. Goh Kheng Teong (2013-05-20). "DAP complains to MCMC over blockade on its websites, videos, FB, social media networks" (http://www.malaysia-chronicle.com/index.php?option=com_k2&view=item&id=102522:dap-complains-to-mcmc-over-blockade-on-its-websites-videos-fb-social-media-networks&Itemid=2). Retrieved 2013-05-21.
44. "In Malaysia, online election battles take a nasty turn" (https://web.archive.org/web/20130507112012/http://www.themalaysianinsider.com/malaysia/article/in-malaysia-online-election-battles-take-a-nasty-turn). Reuters. 2013-05-04. Archived from the original (http://www.themalaysianinsider.com/malaysia/article/in-malaysia-online-election-battles-take-a-nasty-turn/) on 2013-05-07. Retrieved 2013-05-22.
45. "Egypt has blocked encrypted messaging app Signal" (https://www.engadget.com/2016/12/20/egypt-blocks-signal/).
46. "Archived copy" (https://web.archive.org/web/20170423151418/http://www.huffpostarabi.com/2017/04/21/story_n_16149218.html). Archived from the original (http://www.huffpostarabi.com/2017/04/21/story_n_16149218.html) on 2017-04-23. Retrieved 2017-04-22.
47. https://www.mic.gov.vn/Pages/TinTuc/143083/Ra-mat-Nen-tang-cung-cap-dich-vu-Trung-tam-dieu-hanh-an-toan--an-ninh-mang-dap-ung-yeu-cau-ket-noi--chia-se-thong-tin.html
48. https://khonggianmang.vn/
49. Genny Pershing. "Network Neutrality: Historic Neutrality" (https://web.archive.org/web/20080511161247/http://www.cybertelecom.org/ci/neutral.htm). Cybertelecom. Archived from the original (http://www.cybertelecom.org/ci/neutral.htm#his) on 2008-05-11. Retrieved 2008-06-26.
50. Genny Pershing. "Network Neutrality: Insufficient Harm" (https://web.archive.org/web/20080511161247/http://www.cybertelecom.org/ci/neutral.htm). Cybertelecom. Archived from the original (http://www.cybertelecom.org/ci/neutral.htm#ins) on 2008-05-11. Retrieved 2008-06-26.
51. "Archived copy" (https://web.archive.org/web/20131025002710/http://www.projectpact.eu/documents-1/). Archived from the original (http://www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf) (PDF) on 2013-10-25. Retrieved 2013-10-11.
52. Sherry Justine, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy, Blindbox: Deep packet inspection over encrypted traffic (http://dl.acm.org/citation.cfm?id=2787502), ACM SIGCOMM Computer Communication Review, 2015
53. "Best Practices - HTTPS Inspection" (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202). *Check Point Support Center*. 2017-07-21. "With HTTPS Inspection, the Security Gateway can inspect the traffic that is encrypted by HTTPS. The Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in a log."
54. "SecureSphere WAF Specifications" (https://www.imperva.com/Products/WebApplicationFirewall-WAF). "SecureSphere WAF Specifications [...] HTTPS/SSL Inspection: Passive decryption or termination"
55. "What is SSL Inspection? How does it work? - The SSL Store™" (https://www.thesslstore.com/blog/ssl-inspection/). *Hashed Out by The SSL Store™*. 2018-08-03. Retrieved 2019-06-26.
56. Raney, Steve (2004). "Suburban silver bullet: Personal rapid transit shuttle and wireless commuting assistant with cellular location tracking". *Transportation Research Record*. **1872**: 62–70. doi:10.3141/1872-08 (https://doi.org/10.3141%2F1872-08). S2CID 110849717 (https://api.semanticscholar.org/CorpusID:110849717).
57. "OpenDPI.org" (https://web.archive.org/web/20151207050407/http://www.opendpi.org/). Archived from the original (http://www.opendpi.org/) on 2015-12-07.

58. ntop (2 February 2012). "nDPI - Open and Extensible LGPLv3 Deep Packet Inspection Library" (http://www.ntop.org/products/ndpi/). ntop.org. Retrieved 23 March 2015.
59. Fichtner, Franco. "Bye bye OpenDPI" (http://lastsummer.de/bye-bye-opendpi/). *lastsummer.de*. Retrieved 23 March 2015.
60. "Deep packet inspection engine goes open source" (https://arstechnica.com/open-source/news/2009/09/deep-packet-inspection-engine-goes-open-source.ars). *Ars Technica*. 9 September 2009.
61. "nDPI" (http://www.ntop.org/products/ndpi/). *ntop*. 2 February 2012.
62. "Application Layer Packet Classifier for Linux" (http://l7-filter.sourceforge.net/). *sourceforge.net*.
63. "A fond farewell to l7-filter" (https://l7-filter.clearfoundation.com/).
64. "SourceForge.net Repository - [hippie] Index of /" (http://hippie.cvs.sourceforge.net/viewvc/hippie/). *sourceforge.net*.
65. "HiPPIE - Free download" (http://www.linux112.com/hippie-p313520.html). *linux112.com*.
66. hjelmvik. "SPID Statistical Protocol IDentification" (http://sourceforge.net/projects/spid/). *SourceForge*.
67. Tstat project home (http://tstat.tlc.polito.it/index.shtml)
68. "WAND Network Research Group: libprotoident" (http://research.wand.net.nz/software/libprotoident.php). *wand.net.nz*.
69. *Spy-Gear Business to Be Sold - Amesys to Sell Business That Provided Surveillance Technology Used by Gadhafi (http://www.wallstreetjournal.de/article/SB10001424052970203961204577269391401776590.html)*, the Wall Street Journal, German edition, March 9, 2012.
70. Tomasz Bujlow; Valentín Carela-Español; Pere Barlet-Ros (2015). "Independent Comparison of Popular DPI Tools for Traffic Classification" (http://tomasz.bujlow.com/publications/2014_journal_elsevier_comnet_independent_comparison.htm). *Computer Networks*. In press (Computer Networks). **76**: 75–89. CiteSeerX 10.1.1.697.8589 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.697.8589). doi:10.1016/j.comnet.2014.11.001 (https://doi.org/10.1016%2Fj.comnet.2014.11.001). Retrieved 2014-11-10.
71. Application Visibility and Control. (n.d.). In Cisco Systems (http://www.cisco.com/en/US/prod/routers/application_visibility_control.html)

External links

- What is "Deep Inspection"? (http://www.ranum.com/security/computer_security/editorials/deepinspect/) by Marcus J. Ranum. Retrieved 10 December 2018.
- A collection of essays from industry experts (https://web.archive.org/web/20090408150009/http://dpi.priv.gc.ca/)
- What Is Deep Packet Inspection and Why the Controversy (http://netequalizernews.com/2011/02/08/what-is-deep-packet-inspection-and-why-the-controversy/)
- White Paper "Deep Packet Inspection – Technology, Applications & Net Neutrality" (https://web.archive.org/web/20091104045628/http://www.ipoque.com/resources/white-papers)
- Egypt's cyber-crackdown aided by US Company (http://therealnews.com/t2/latest-news/best-of-web?task=videodirectlink&id=9042) - DPI used by Egyptian government in recent internet crackdown
- Deep Packet Inspection puts its stamp on an evolving Internet (https://web.archive.org/web/20120308084342/http://advancedtca-systems.com/deep-stamp-an-evolving-internet/)
- Deep Packet Inspection Using Quotient Filter (https://ieeexplore.ieee.org/document/7548376/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Deep_packet_inspection&oldid=1055909567"