(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 February 2017 (09.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/020962 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 9/445* (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/EP2015/068172

(22) International Filing Date:
6 August 2015 (06.08.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building Bantian Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors; and
(71) Applicants *(for US only)*: **GAMPEL, Eran** [IL/DE]; c/o Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **MOLKHO, Adi** [IL/DE]; c/o Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **TOUITOU, Dan** [IL/DE]; c/o Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(74) Agent: **KREUZ, Georg**; Huawei Technologies Duesseldorf GmbH Riesstr. 8, 80992 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: OFFLOADING WEB SECURITY SERVICES TO CLIENT SIDE

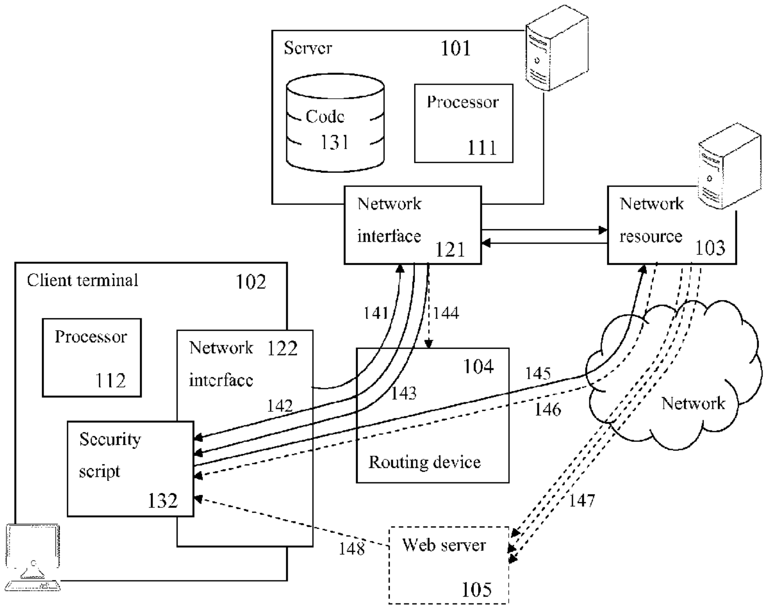


FIG. 1

(57) Abstract: A system of providing a content filtering service, comprising: a network interface adapted to receive from a client terminal via a network a request for retrieving network data from at least one network resource; a store code for storing a code to transmit to the client terminal a client side security script in response to the request; and a processor, connected to the network interface and the store code, and adapted to execute the code for transmitting the client side security script to the client terminal; wherein the client side security script is adapted to be interpreted at the client terminal for authenticating the rendering of at least part of the network data from the at least one network resource.

Title: OFFLOADING WEB SECURITY SERVICES TO CLIENT SIDE

FIELD AND BACKGROUND OF THE INVENTION

The present invention, in some embodiments thereof, relates to a content filtering service and, more particularly, but not exclusively, to a content filtering service based on a script operating at the client terminal.

Web security services like uniform resource locator (URL) filtering in Enterprise or Web Application firewall (WAF) protecting a client terminal from harmful or unwanted content are mostly implemented as a proxy. All traffic flows through the proxy, and every new Hypertext Transfer Protocol (HTTP) request, new page or dynamic request from the client terminal is being analyzed by the proxy service. The original TCP connection is terminated by the proxy, the proxy sends the request to the web server address and the requested content is received by the proxy server. The proxy then pretends to be the web server and may send to the client terminal cached content, modified content or may block content completely. The proxy's operation may be transparent to the client terminal.

SUMMARY OF THE INVENTION

The object of embodiments of the invention is to reduce load from a content filtering server by providing a content filtering service based on a security script that is distributed by the server for operating locally on a client terminal. The object is solved by the independent claims of this application, and the dependent claims protect further implementation forms.

According to a first aspect, the present invention relates to a system of providing a content filtering service, comprising: a network interface adapted to receive from a client terminal via a network a request for retrieving network data from at least one network resource; a store code for storing a code to transmit to the client terminal a client side security script in response to the request; and a processor, connected to the network interface and the store code, and adapted to execute the code for transmitting the client side security script to the client terminal; wherein the client side security script is adapted to be interpreted at the client terminal for authenticating the rendering of at least part of the network data from the at least one network resource.

In a first possible implementation form of the system according to the first aspect, the code comprises a code to: extract an identifier of the client from the request, authenticate the identifier, and instruct a routing device of the network to open a data flow for a direct retrieval of the network data from the at least one network resource by the client side security script.

In a second possible implementation form of the system according to the first implementation form of the first aspect, the code comprises a code to: provide the routing device with a first key; provide the client with a second key; and wherein the routing device matches between the first key and the second key for verifying the direct retrieval.

In a third possible implementation form of the system according to the first aspect, the client side security script is adapted to receive authentication data and install in a browser or an application running on the client terminal a browser cookie generated based on the authentication data for supporting a data flow between the network resource and the client terminal.

In a fourth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the system further comprises a web server providing a plurality of communications channels with a plurality of network resources over a single Transmission Control Protocol (TCP) connection for routing the network data to the client side security script.

In a fifth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the client side security script is adapted to be implemented by a client side processor of the client terminal for authenticating the rendering of at least part of the network data by verifying a compliance of the network data with at least one condition and for presenting the network data based on a detection of the compliance.

In a sixth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the request is a Hypertext Transfer Protocol (HTTP) Get request.

In a seventh possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the client side security script is executed by the processor in a restricted operating system environment.

In an eighth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the client side security script is adapted to be implemented by a client side processor of the client terminal for: transmitting the request for retrieving network data from the at least one network resource from the client terminal, receiving the network data from the at least one network resource, verifying a compliance of the network data with at least one condition, and parsing at least some of the network data according to the verification.

In a ninth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the client side security script is a virtual machine monitor (VMM) running a security service code and a security service abstraction layer for processing the network data.

In a tenth possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the client side security script is a virtual machine monitor (VMM) running a Document Object Model (DOM) builder and a HyperText Markup Language (HTML) parser for loading and rendering at least some of the network data on a display of the client terminal.

In an eleventh possible implementation form of the encoder device according to the first aspect as such or according to any of the preceding implementation forms of the first aspect, the system is implemented as a proxy server handling a plurality of requests from a plurality of clients for retrieving a plurality of different network documents from a plurality of network resources which are accessible via the network.

In a twelfth possible implementation form of the system according to the eleventh possible implementation form of the encoder device of the first aspect , the network interface is adapted to receive the plurality of requests from a plurality of different client terminals; wherein the code comprises instructions to transmit a plurality of client side security scripts each in response to one of the plurality of requests; wherein each one of the plurality of client side security scripts is adapted to be implemented by a client side processor of one of the plurality of client terminals for authenticating the rendering of at least part of respective the network data.

According to a second aspect, the present invention relates to an apparatus of running a content filtering service, comprising: a network interface adapted to transmit via a network a request for retrieving network data from at least one network resource and to receive a client side security script in response to the request; and a processor connected to the network interface and adapted to execute the client side security script for authenticating the network data received from the at least one network resource.

According to a third aspect, the present invention relates to a method for providing a content filtering service, comprising: at a server side: receiving from a client terminal via a network a request for retrieving a network data from at least one network resource; transmitting to the client terminal a client side security script in response to the request; at a client side: running the client side security script for authenticating content of the network document which is received in a data flow between the network resource and the client terminal.

According to a fourth aspect, the present invention relates to a computer program product comprising a readable storage medium storing program code thereon for use by a selection module, the program code comprising: instructions for receiving, at a server side, via a network, a request for retrieving network data from at least one network resource from a client terminal; instructions for transmitting from the server side to the client terminal a client side security script in response to the request; instructions for running the client side security script at a client side for authenticating the network data.

Unless otherwise defined, all technical and/or scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, exemplary methods and/or materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and are not intended to be necessarily limiting.

Implementation of the method and/or system of embodiments of the invention can involve performing or completing selected tasks manually, automatically, or a combination thereof. Moreover, according to actual instrumentation and equipment of embodiments of the method and/or system of the invention, several selected tasks could be implemented by hardware, by software or by firmware or by a combination thereof using an operating system.

For example, hardware for performing selected tasks according to embodiments of the invention could be implemented as a chip or a circuit. As software, selected tasks according to embodiments of the invention could be implemented as a plurality of software instructions being executed by a computer using any suitable operating system. In an exemplary embodiment of the invention, one or more tasks according to exemplary embodiments of method and/or system as described herein are performed by a data processor, such as a computing platform for executing a plurality of instructions. Optionally, the data processor includes a volatile memory for storing instructions and/or data and/or a non-volatile storage, for example, a magnetic hard-disk and/or removable media, for storing instructions and/or data. Optionally, a network connection is provided as well. A display and/or a user input device such as a keyboard or mouse are optionally provided as well.

BRIEF DESCRIPTION OF THE DRAWINGS

Some embodiments of the invention are herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of embodiments of the invention. In this regard, the description taken with the drawings makes apparent to those skilled in the art how embodiments of the invention may be practiced.

In the drawings:

FIG. 1 is a schematic illustration of a system having a server for generating script for filtering content from third party network sources and for forwarding the script for execution by a processor of a client terminal that accesses the third party network sources, according to some embodiments of the present invention;

FIG. 2 is a flowchart schematically representing a method for content filtering using a system such as depicted in FIG. 1, according to some embodiments of the present invention;

FIG. 3 is a schematic illustration of a structure of a code stored in a server, according to some embodiments of the present invention;

FIG. 4 is a sequence chart of an exemplary process of content filtering, according to some embodiments of the present invention; and

FIG. 5 is a schematic illustration of rendering flow using JavaScript VMM Layer, according to some embodiments of the present invention.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The present invention, in some embodiments thereof, relates to a content filtering service and, more particularly, but not exclusively, to a content filtering service based on a script operating at the client terminal.

Traffic of content in content filtering services which are implemented at proxy service hardware is limited to the processing power and forwarding capacities of the proxy service hardware. Proxy server(s) provide filtering and security service to large numbers of users simultaneously, and filtering and security services are getting more and more complicated so the processing power they consume increases accordingly. When the capacity limit is reached, some of the client terminals may experience denial of service (DoS) and/or the proxy may allow some of the traffic to pass without being analyzed so the client terminal receives unfiltered data and may be exposed to risk.

According to some embodiments of the present invention, there is provided a content filtering service based on a security script that is distributed by a server for operating locally a browser or an application executed using processor(s) of a client terminal. A code executed in an enterprise server sends a security service in the form of a browser script, such as JavaScript software, that is executed by the browser of the client terminal. The script performs analysis and filtering based on a set of rules and/or conditions provided as part of the script. The server may authenticate the client terminal before sending the script, for example by a cookie key. After initial authentication, all traffic from content sources in the internet may be forwarded directly to the client terminal without additional processing in the server. Optionally, the traffic is forwarded through a routing device or a web server acting as a proxy. This eliminates the bottle neck of the processing power of the server and allows faster bandwidth.

Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not necessarily limited in its application to the details of construction and the arrangement of the components and/or methods set forth in the following description and/or illustrated in the drawings and/or the Examples. The invention is capable of other embodiments or of being practiced or carried out in various ways.

The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

Referring now to the drawings, FIG. 1 is a schematic illustration of a system having a server for generating script for filtering content from third party network sources and for forwarding the script for execution by a processor of a client terminal that accesses the third party network sources, according to some embodiments of the present invention.

The system includes a server 101 connected to client terminal(s) 102. Server 101 may include one or more computing devices, for example, a mainframe computer, an enterprise server, a workstation, multiple connected computers and/or a personal computer. Server 101 generates a security script based on web content requests from client terminals 102 for providing content filtering service to a computer network. The security script is locally used by each client terminal for processing, for instance by filtering, modifying and/or blocking, network data originated from the internet. The processed content may include, for example, potentially harmful content such as malware code, computer viruses, worms and/or trojan horses and/or designated content such as offensive, hostile, intrusive, annoying material such as adware, spam and/or spyware, and/or any other content defined by server 101.

Client terminal(s) 102 may include, for example, a mobile device such as a Smartphone, a tablet, a wearable device such as Google glass, a Smart watch, a laptop computer and/or the like, a personal computer and/or any device that has one or more network communication modules, such as a network card or chip.

The computer network may include, for example, local area network (LAN), a wireless network such as mobile network, wireless local area network (WLAN) such as Wireless Fidelity (WiFi™), a wireless personal area network (WPAN) such as Bluetooth™ protocol and/or any other network.

Reference is also made to FIG. 2, which is a flowchart schematically representing a method for content filtering using a system such as depicted in FIG. 1, according to some embodiments of the present invention.

First, as shown at 201, a request for network data stored in a network resource 103 is sent (141) from a network interface 122 of client terminal 102 and received by a network interface 121 of a server 101. The request may be, for example, for a web-document such as a HyperText Markup Language (HTML) document, an image, a text document, an executable file and/or any other file and/or data.

Optionally, the request includes an identifier of client terminal 102, for example an IP address, a MAC address and/or any other identifying code. The identifier is then authenticated by server 101, for example from a list of identifiers.

Then, as shown at 202, a security script 132 is sent (142) from server 101 to client terminal 102. This is done using a code executed by a processor 111 of server 101 and via network interface 121 of server 101.

Optionally, parameters and/or properties of security script 132 that is sent to client terminal 102 are determined by the identity of client terminal 102. The identity is determined for example by the identifier. Optionally, the parameters and/or properties are determined by the identity of the user of client terminal 102 that may be included in the request for network data. Optionally, the parameters and/or properties are determined based on the requested network data, for example, the security script may be dedicated to a specific website, country, language and/or any other parameter.

Optionally, server 101 provides a set of rules and/or conditions for filtering based on the specific identity of client terminal 102 and/or the identity of the user of client terminal 102, as may be verified by the security key. For example, rules sent to a client terminal mostly used by children may include restriction of adult content. Optionally, server 101 provides a set of rules and/or conditions for filtering based on the requested network data.

Security script 132 may be sent to client terminal 102 once after a first network data request from client terminal 102, and/or may be sent after every network data request.

Optionally, updates for security script 132 and/or for the rules and/or conditions are sent from server 101 to client terminal 102, for example periodically and/or upon an update request from client terminal 102. Optionally, security script 132 is a virtual machine monitor (VMM). Reference is now made to FIG. 3, which is a schematic illustration of a structure of a code 131 stored in server 101, according to some embodiments of the present invention. The VMM may be running a security service code 301 and a security service abstraction layer 302 for processing the network data, and/or may be running a Document Object Model (DOM) builder 303 and a HTML parser 304 for loading and rendering at least some of the network data on a display of client terminal 102.

Optionally, server 101 handles multiple requests from multiple client terminals 102 for retrieving multiple different network documents from multiple network resources 103 which are accessible via the network. Network interface 121 is adapted to receive these multiple requests from multiple different client terminals 102. Server 101 then transmits multiple security scripts to each of client terminals 102, each security script is sent in response to one of the requests. Optionally, each security script is unique to a specific client terminal.

Then, optionally, as shown at 203, a security key is also sent (143) from server 101 to client terminal 102 and optionally also sent (144) to a routing device 104 connecting client terminal 102 to the internet. The security key may be a browser cookie installed in a browser and/or an application running on client terminal 102. Optionally, Authentication data is sent from server 101 to client terminal 102 and the cookie is generated and installed by security script 132.

Then, as shown at 204, security script 132 is executed by a processor 112 of client terminal 102 to send a request (145) for the network data via a network interface 122 of client terminal 102. The request may be, for example, a Hypertext Transfer Protocol (HTTP) Get request. Optionally, security script 132 is executed by processor 112 in a restricted operating system environment of client terminal 102, such as a sandbox area. Optionally, the request includes the security key sent to client terminal 102.

Then, optionally, as shown at 205, the key sent from client terminal 102 is authenticated. Optionally, this is done by server 101. Optionally, routing device 104 matches between the key received with the request from client terminal 102 to the key previously received when security script 132 and the security key were sent to client terminal 102 from server 101. The matching may be done, for example, by comparing a signature and/or a code existing in both keys.

Then, as shown at 206, the network data is transferred to client terminal 102 from network resource 103 and received by security script 132. Optionally, the data is transferred (146) by routing device 104, so no intermediate server is used. Optionally, routing device 104 opens a data flow for a direct retrieval of the network data by client terminal 102, following an instruction received from server 101 based on the identifier of client terminal 102. Optionally, the data is transferred by a web server 105 that provides multiple communications channels (147) with multiple network resources 103 over a single Transmission Control Protocol (TCP) connection (148) to client terminal 102. Web server 105 may be, for example, a WebSocket server, XMLHtppReq or any other networking protocol supported by the browser. Optionally, Transparent Cashing is integrated in web server 105.

Then, as shown at 206, security script 132 verifies that the network data is compliant with predefined condition(s). The condition(s) may include any type of rules defined in security script 132.

Then, as shown at 207, security script 132 renders and/or parses at least some of the network data on a display of client terminal 102, based on the compliance of the network data with the predefined condition(s). When the network data is compliant with the condition, the network data may be rendered completely. When the network data is partially compliant with the condition, the network data may be rendered partially or with alterations. When the network data is not compliant with the condition the network data may be blocked.

Reference is now made to FIG. 4, which is a sequence chart of an exemplary process of content filtering, according to some embodiments of the present invention. An HTTP Get request is sent (411) from browser 401 to switch 402 and the HTTP traffic is redirected (412) to a server 403. Server 403 sends (413) JavaScript package to browser 401. The JavaScript content filter 404 sends (414) the HTTP Get request to network resource 405 and receives (415) the HTML from network resource 405. The HTML is parsed (416) by JavaScript content filter 404 and content is downloaded from network resource 405. JavaScript content filter 404 may request (417) additional filter rules from server 403. Content received (418) from network resource 405 is analyzed (419) by JavaScript content filter 404 and displayed in browser 401 when it is not prohibited by the filter rules.

Reference is now made to FIG. 5, which is a schematic illustration of rendering flow using JavaScript VMM Layer, according to some embodiments of the present invention. The security service transparent http 501 sends back to the html parser 502 of the web browser 503 an empty html with page loading and a security service packages in javaScript with the requested URL embedded in the page. The

JavaScript page loading and security service layer 504 of web browser 503 then receives all network data directly from network resource 505.

The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

It is expected that during the life of a patent maturing from this application many relevant content filtering services will be developed and the scope of the term content filtering is intended to include all such new technologies *a priori*.

The terms "comprises", "comprising", "includes", "including", “having” and their conjugates mean "including but not limited to". This term encompasses the terms "consisting of" and "consisting essentially of".

As used herein, the singular form "a", "an" and "the" include plural references unless the context clearly dictates otherwise. For example, the term "a compound" or "at least one compound" may include a plurality of compounds, including mixtures thereof.

The word “exemplary” is used herein to mean “serving as an example, instance or illustration”. Any embodiment described as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments and/or to exclude the incorporation of features from other embodiments.

The word “optionally” is used herein to mean “is provided in some embodiments and not provided in other embodiments”. Any particular embodiment of the invention may include a plurality of “optional” features unless such features conflict.

It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable subcombination or as suitable in any other described embodiment of the invention. Certain features described in the context of various embodiments are not to be considered essential features of those embodiments, unless the embodiment is inoperative without those elements.

Although the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, it is intended to embrace all such alternatives, modifications and variations that fall within the spirit and broad scope of the appended claims.

All publications, patents and patent applications mentioned in this specification are herein incorporated in their entirety by reference into the specification, to the same extent as if each individual publication, patent or patent application was specifically and individually indicated to be incorporated herein by reference. In addition, citation or identification of any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention. To the extent that section headings are used, they should not be construed as necessarily limiting.

WHAT IS CLAIMED IS:

1. A system of providing a content filtering service, comprising:

a network interface (121) adapted to receive from a client terminal (102) via a network a request for retrieving network data from at least one network resource (103);

a store code (131) for storing a code to transmit to said client terminal (102) a client side security script (132) in response to said request; and

a processor (111), connected to said network interface (121) and said store code (131), and adapted to execute said code for transmitting said client side security script (132) to said client terminal;

wherein said client side security script (132) is adapted to be interpreted at said client terminal (102) for authenticating the rendering of at least part of said network data from the at least one network resource (103).

2. The system of claim 1, wherein said code comprises a code to:

extract an identifier of said client from said request,

authenticate said identifier, and

instruct a routing device (104) of said network to open a data flow for a direct retrieval of said network data from said at least one network resource (103) by said client side security script (132).

3. The system of claim 2, wherein said code comprises a code to:

provide said routing device with a first key;

provide said client with a second key; and wherein said routing device (104) matches between said first key and said second key for verifying said direct retrieval.

4. The system of claim 1, wherein said client side security script (132) is adapted to receive authentication data and install in a browser or an application running on said client terminal (102) a browser cookie generated based on said authentication data for supporting a data flow between said network resource (103) and said client terminal (102).

5. The system of any of the previous claims, further comprising a web server (105) providing a plurality of communications channels with a plurality of network resources (103) over a single Transmission Control Protocol (TCP) connection for routing said network data to said client side security script (132).

6. The system of any of the previous claims, wherein said client side security script (132) is adapted to be implemented by a client side processor (112) of said client terminal (102) for authenticating the rendering of at least part of said network data by verifying a compliance of said network data with at least one condition and for presenting said network data based on a detection of said compliance.

7. The system of any of the previous claims, wherein said request is a Hypertext Transfer Protocol (HTTP) Get request.

8. The system of any of the previous claims, wherein said client side security script (132) is executed by said processor (112) in a restricted operating system environment.

9. The system of any of the previous claims, wherein said client side security script (132) is adapted to be implemented by a client side processor (112) of said client terminal (102) for:

transmitting said request for retrieving network data from said at least one network resource (103) from said client terminal (102),

receiving said network data from said at least one network resource (103),

verifying a compliance of said network data with at least one condition, and

parsing at least some of said network data according to said verification.

10. The system of any of the previous claims, wherein said client side security script (132) is a virtual machine monitor (VMM) running a security service code and a security service abstraction layer for processing said network data.

11. The system of any of the previous claims, wherein said client side security script (132) is a virtual machine monitor (VMM) running a Document Object Model (DOM) builder and a HyperText Markup Language (HTML) parser for loading and rendering at least some of said network data on a display of said client terminal (102).

12. The system of any of the previous claims, wherein said system is implemented as a proxy server handling a plurality of requests from a plurality of clients for

retrieving a plurality of different network documents from a plurality of network resources which are accessible via said network.

13. The system of claim 12, wherein said network interface is adapted to receive said plurality of requests from a plurality of different client terminals;

wherein said code comprises instructions to transmit a plurality of client side security scripts each in response to one of said plurality of requests;

wherein each one of said plurality of client side security scripts is adapted to be implemented by a client side processor of one of said plurality of client terminals for authenticating the rendering of at least part of respective said network data.

14. An apparatus of running a content filtering service, comprising:

a network interface adapted (122) to transmit via a network a request for retrieving network data from at least one network resource (103) and to receive a client side security script (132) in response to said request; and

a processor (112) connected to said network interface (122) and adapted to execute said client side security script (132) for authenticating said network data received from said at least one network resource (103).

15. A method for providing a content filtering service, comprising:

at a server side:

receiving from a client terminal (102) via a network a request for retrieving a network data from at least one network resource (103);

transmitting to said client terminal (102) a client side security script (132) in response to said request;

at a client side:

running said client side security script (132) for authenticating content of said network document which is received in a data flow between said network resource (103) and said client terminal (102).

16. A computer program product comprising a readable storage medium storing program code thereon for use by a selection module, the program code comprising:

instructions for receiving, at a server side, via a network, a request for retrieving network data from at least one network resource from a client terminal;

instructions for transmitting from said server side to said client terminal a client side security script in response to said request;

instructions for running said client side security script at a client side for authenticating said network data.

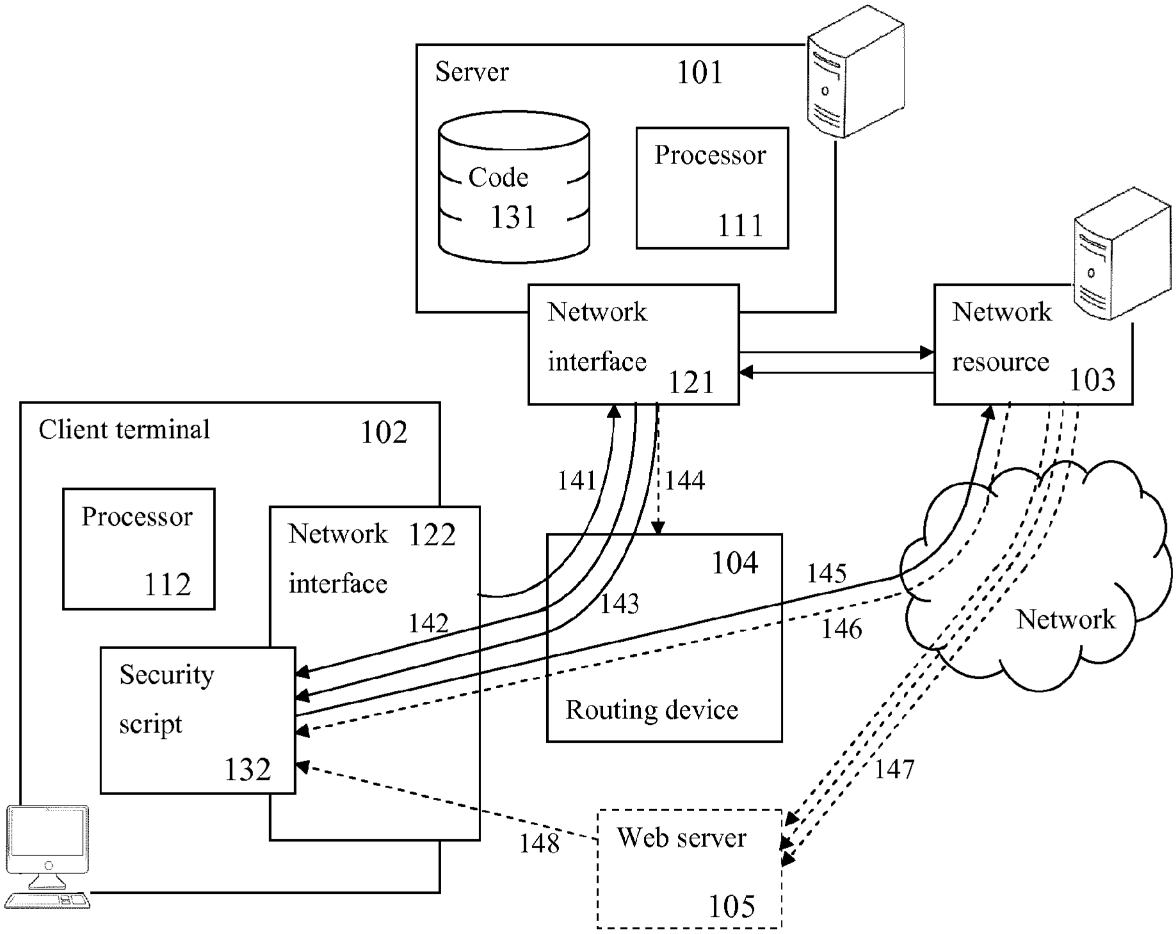
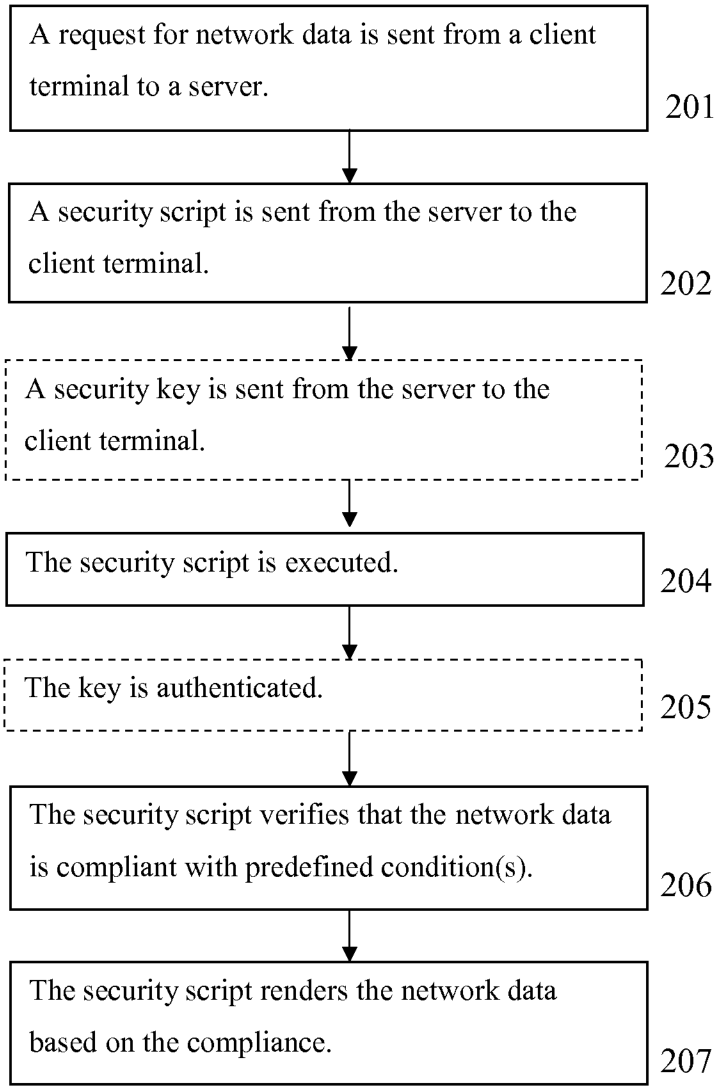

Server
101
Code
131
Processor
111
Network
interface
121
Network
resource
103
Client terminal
102
Processor
112
Network
interface
122
141
144
104
145
142
143
146
Security
script
132
Routing device
Network
147
Web server
105
148

FIG. 1



A request for network data is sent from a client terminal to a server. 201

A security script is sent from the server to the client terminal. 202

A security key is sent from the server to the client terminal. 203

The security script is executed. 204

The key is authenticated. 205

The security script verifies that the network data is compliant with predefined condition(s). 206

The security script renders the network data based on the compliance. 207

FIG. 2

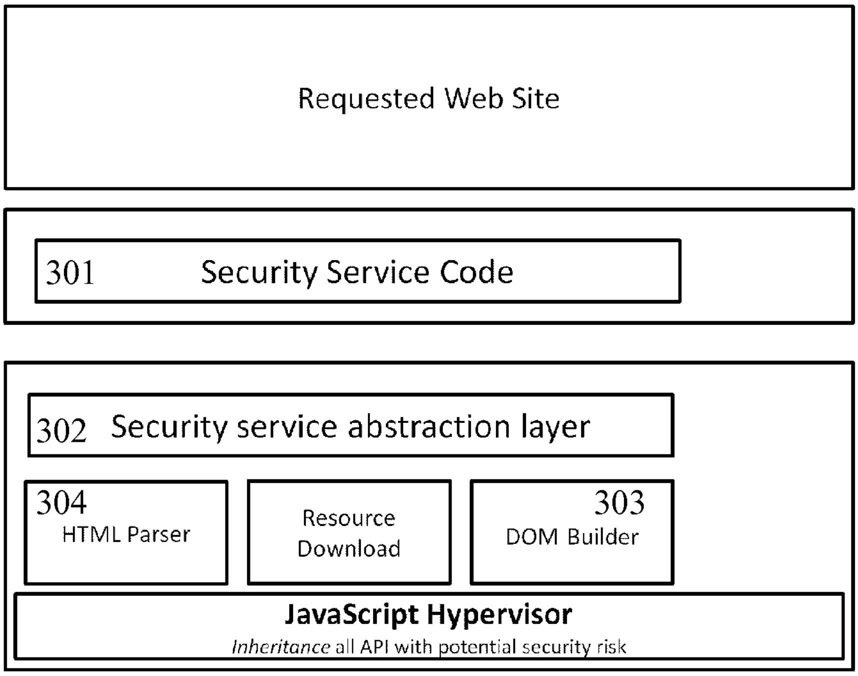

Requested Web Site
301
Security Service Code
302
Security service abstraction layer
304
HTML Parser
Resource Download
303
DOM Builder
JavaScript Hypervisor
Inheritance all API with potential security risk

FIG. 3

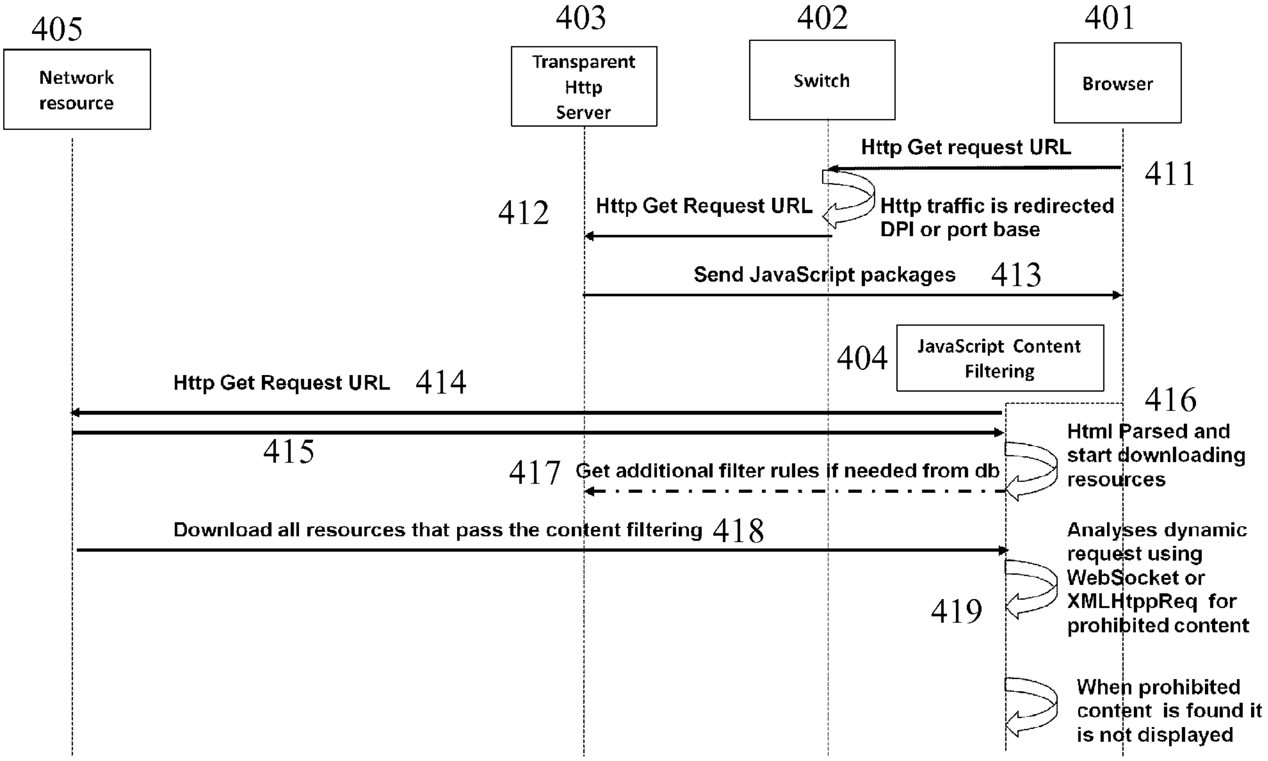

405
Network resource
403
Transparent Http Server
402
Switch
401
Browser
Http Get request URL
411
412
Http Get Request URL
Http traffic is redirected DPI or port base
Send JavaScript packages
413
404
JavaScript Content Filtering
Http Get Request URL
414
416
415
Html Parsed and start downloading resources
417
Get additional filter rules if needed from db
Download all resources that pass the content filtering
418
Analyses dynamic request using WebSocket or XMLHtppReq for prohibited content
419
When prohibited content is found it is not displayed

FIG. 4

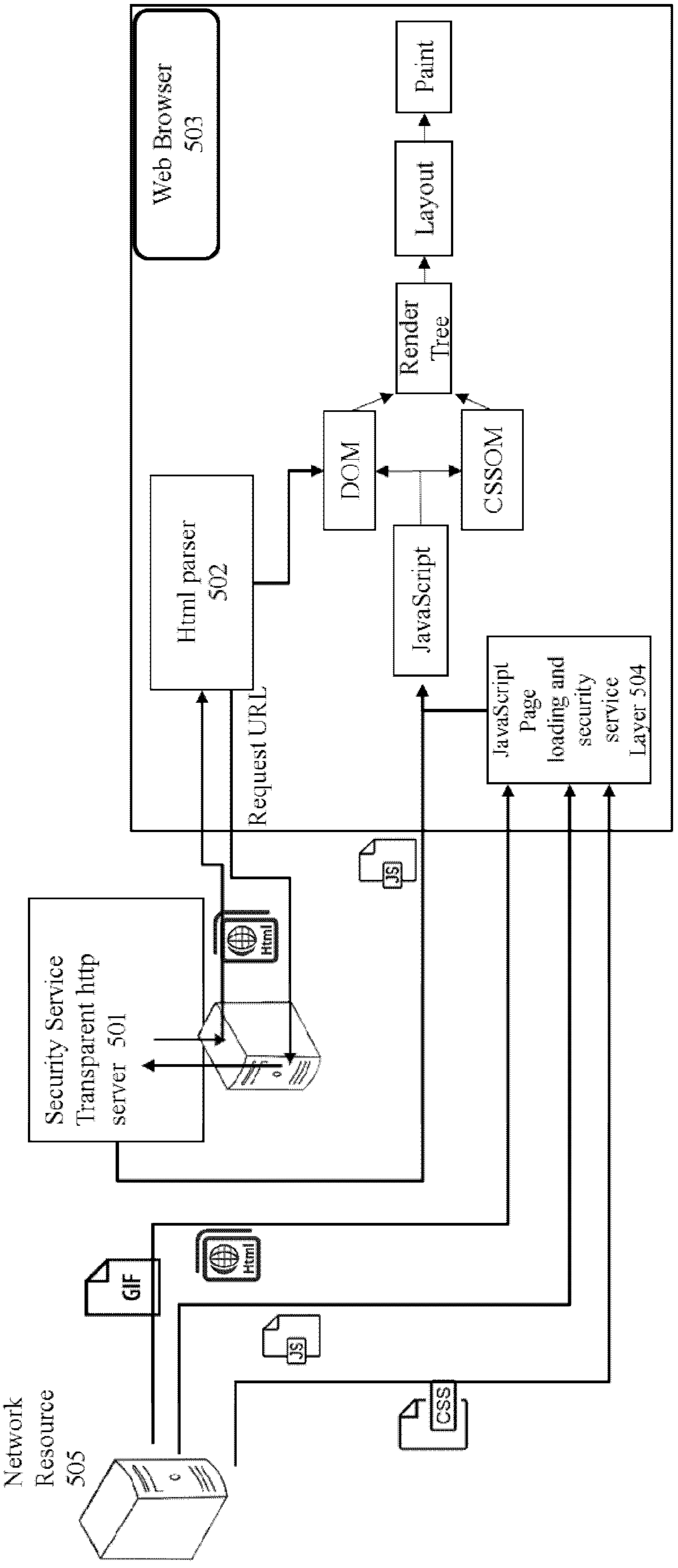

Web Browser
503
Paint
Layout
Render
Tree
DOM
CSSOM
Html parser
502
JavaScript
JavaScript
Page
loading and
security
service
Layer 504
Request URL
JS
Html
Security Service
Transparent http
server 501
GIF
Html
JS
CSS
Network
Resource
505

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/068172

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/08 G06F9/445
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/325627 A1 (FEE PAUL [GB]) 30 October 2014 (2014-10-30) paragraph [0040] - paragraph [0068] -----	1-16
X	US 6 223 287 B1 (DOUGLAS DANIEL G [US] ET AL) 24 April 2001 (2001-04-24) column 3, line 37 - column 5, line 41 -----	1-16
A	EP 2 264 957 A1 (HUAWEI TECH CO LTD [CN]) 22 December 2010 (2010-12-22) paragraph [0012] - paragraph [0017] paragraph [0038] - paragraph [0042] paragraph [0071] - paragraph [0081] -----	1-16
A	KR 2015 0085188 K1 (CONTENTS MAN CORP CO LTD [KR]) 23 July 2015 (2015-07-23) paragraph [0019] - paragraph [0034] paragraph [0040] - paragraph [0047] -----	1-16

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 March 2016	29/03/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Olaechea, Javier

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/068172

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014325627 A1	30-10-2014	US 2014325627 A1 WO 2014179040 A1	30-10-2014 06-11-2014
US 6223287 B1	24-04-2001	NONE	
EP 2264957 A1	22-12-2010	CN 101547166 A EP 2264957 A1 WO 2009117905 A1	30-09-2009 22-12-2010 01-10-2009
KR 20150085188 K1	23-07-2015	NONE	