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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 September 2017 (14.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/153983 A1

(51) International Patent Classification:
G06F 21/56 (2013.01) *G06F 21/55* (2013.01)
G06F 21/60 (2013.01) *G06F 21/50* (2013.01)

(21) International Application Number:
PCT/IL2017/050277

(22) International Filing Date:
7 March 2017 (07.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/304,958 8 March 2016 (08.03.2016) US

(71) Applicant: **B. G. NEGEV TECHNOLOGIES AND APPLICATIONS LTD., AT BEN-GURION UNIVERSITY** [IL/IL]; P.O.B. 653, 8410501 Beer Sehva (IL).

(72) Inventor: **GURI, Mordechai**; 28 Emek Ayalon Street, 7170656 Modi'in (IL).

(74) Agents: **FUERST, Zadok** et al.; Luzzatto & Luzzatto, P.O. Box 5352, 8415202 Beer Sheva (IL).

(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, DJ, 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, KH, KN, KP, KR, KW, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: SYSTEM AND METHOD FOR PERFORMING IN-CLOUD SECURITY OPERATIONS ON CONNECTED DEVICES

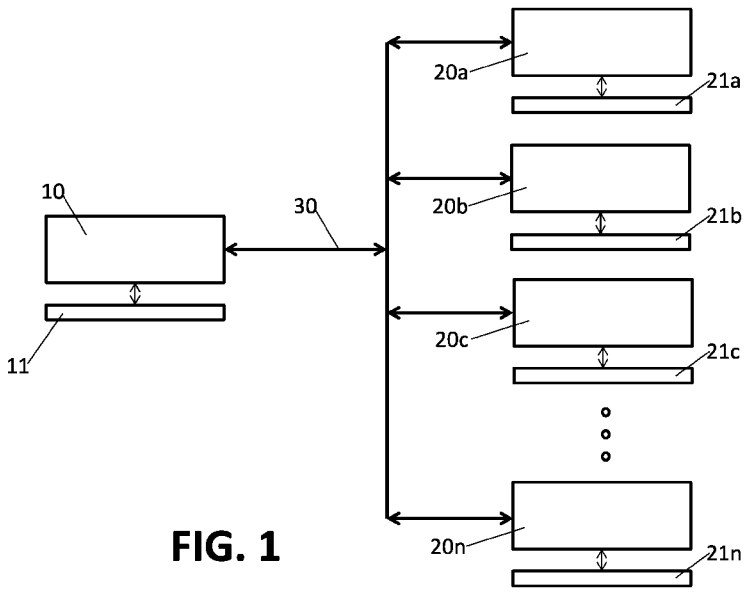

FIG. 1

(57) Abstract: The invention relates to a system for protecting IoT devices from malicious code, which comprises: (a) a memory extracting module at each of said IoT devices, for extracting a copy of at least a portion of the memory content from the IoT device, and sending the same to an in-cloud server; and (b) an in-cloude server for receiving said memory content, and performing an integrity check for a possible existance of malicious code within said memory content.

WO 2017/153983 A1

SYSTEM AND METHOD FOR PERFORMING IN-CLOUD SECURITY OPERATIONS ON CONNECTED DEVICES

Field of Invention

The field of the invention relates in general to methods and systems for securing computerized environments and devices. More specifically, the invention relates to a method and a system for checking the integrity and authenticity of "Internet of Things" (IoT) type devices, thereby detecting whether they have been infected by malicious code.

Background of the Invention

The "Internet of Things (IoT)" is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system and is able to interoperate within the existing Internet infrastructure. According to Wikipedia, Experts estimate that the IoT will consist of almost 50 billion objects ("things") by 2020.

Typically, IoT offers advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded

devices (including smart objects), is expected to be adopted in in nearly all fields of automation.

For example, the range of IoT devices includes heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist firefighters in search and rescue operations. These devices use sensors to collect useful data with the help of various existing technologies, and then autonomously flow the data between other devices. Other examples include home automation (smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens or refrigerators/freezers that use Wi-Fi for remote monitoring.

As discussed, the IoT devices that are used in many fields and structures, are manufactured by a huge number of different manufacturers. While the protocol for interconnectivity and communication between various of these device has been defined and standartized, still a vast majority of these devices are characterized by:

a. They apply a great variety of proprietary operating systems (OS), software and hardware;

b. They have a limited, in many cases very limited processing power; and

c. The devices are in many cases very cheap.

Although the IoT devices are typically characterized by said (a) – (c) above, still these devices in many cases are used to control or sense very critical elements. The exploitation of these devices by hostile entities, for example, by injection of malicious code, can cause very significant damages, such as stealing of data, manipulation of the operation of the devices, or using the attacked device as a platform for attacking other device (e.g., bot). Therefore, in contrast to (a) the low cost of each of said devices; (b) the fact that the devices may have a very limited

processing power; and (c) the fact that each of the devices may have a different proprietary oprating system that may require a dedicated protection software; there is still a real need to protect the IoT devices from damages resulting from malicious code. This is particularly due to the fact that all these devices are accessible to hackers via the Internet.

The prior art techniques that have been so far adopted for protecting IoT devices from malicious code are typically tradional, for example:

a. Use of a firewall, which substantially isolates the internal network of the IoT devices from the external domain;
b. The use of conventional anti-virus software, whenever possible. This is, however, impractical in IoT devices having proprietary operating systems, in view of the huge variety of the proprietary operating systems involved. Furthermore, this is in many cases impractical in view of the high difference between the value of the IoT device and the cost of developing such software to account for this large variety of proprietary operating systems. Finally, the limited processing power of the IoT devices does not always enable the use of anti-virus software.
c. The use of network based security systems such as firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These systems are monitoring the network traffic and try to detect attacks or malicious activities. However, this approach is limited only to attacks that can be detect from the network traffic. Moreover, this approach is very limited in detecting attacks that are hiding within encrypted traffic.

More specifically, the prior art has typically applies the classic approach that is typically used for end-points and workstations, which involves running detection programs on the IoT devices to detect, scan and analyze for malicious code within the (1) persistent storage (e.g., disk) and (2) non-persistent storage (e.g., memory).

However, this approach is not applicable in many case, in view of the limited computational power of the IoT device.

In another aspect, cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

It is therefore an object of the present invention to provide a method and system for protecting IoT devices from malicious code.

It is another object of the present invention to provide a method and system that can protect IoT devices, that wereotherwise remained unprotected.

It is still another object of the present invention to provide such a system that can detect malicious code in IoT devices, provide an alert, and remove the malicious code.

It is still another object of the present invention to provide upgrades and updates to the operating systems of the IoT devices, whether these operating systems are standard, or proprietary.

Other objects and advantages of the invention will become apparent as the description proceeds.

Summary of the Invention

The invention relates to a system for protecting IoT devices from malicaious code, which comprises: (a) a memory extracting module at each of said IoT devices, for extracting a copy of at least a portion of the memory content from the IoT device, and sending the same to an in-cloud server; and (b) an in-cloude server for receiving said memory content, and performing an integrity check for a possible existance of malicious code within said memory content.

In an embodiment of the invention, said in-cloud server performs one or more of the following: (a) analysis of the memory to find malware using static analysis methods; analysis of the memory to find malicious behavior using behavioral and heuristics methods; (b) reconstruction of the state of an OS of the IoT to determine and report important structural elements; (c) check of the integrity of the OS and its memory to possibly find fault in the integrity or hidden processes; (d) a cross-view check on resources to find rootkits and hidden operations; and (e) a cross-view check and validation of memory contents of plurality of IoT devices.

In an embodiment of the invention, and following said integrity check, said in-cloud server performs one or more of the following:
(1) logging of the results;
(2) reporting the results, raising a warning or an alert in a case of detection of an unexpected code or behaveior; or
(3) communicating and responding to an IoT request.

In an embodiment of the invention, the memory, a copy of which is sent to the in-cloud server, is either a persistent memory or a non-persistent memory.

In an embodiment of the invention, said memory extraction module is embedded within a kernel of a respective operating system of the IoT device.

In an embodiment of the invention, said memory extraction module is positioned within a trusted layer at the IoT device.

In an embodiment of the invention, said memory extraction module is positioned within a Trusted Execution Environment at the processor of the IoT device.

Brief description of the Drawings

In the drawings:

- Fig. 1 illustrates the general structure of the system of the present invention.

Detailed Description of Preferred Embodiments of the Invention

As noted, there are many cases in which the classical techniques are not applicable for protecting IoT devices from damages of malicious codes. The present invention provides alternative system and method for protecting IoT devices.

Fig. 1 shows a general structure of the system of the present invention. The system comprises in general an in-cloud protection server 10, which is used to protect a plurality of remote IoT devices 20a – 20n from malicious code. Several of the devices 20a- 20n may be stand-alone devices, others may be a part of IoT networks. In general, the in-cloud server 10 may serve a very large number of IoT devices. For example, a single in-cloud server may serve hundreds of thouthands, even millions of IoT devices 20, that are spread along the globe.

Each of the devices 20a-20n comprises a memory extraction modul 21a-21n, respectively. In one embodiment, the memory extraction module 21 is embedded within the kernel of the respective operating system of device 20. In another embodiment, the memory extraction module 21 is positioned within a trusted layer, such as hypervisor, at device 20. In still another embodiment, the memory extraction module may be positioned within a Trusted Execution Environment (TEE) at the processor of the IoT device.

The memory extraction modules 21 at each of the devices 20 extracts, either upon demand from server 10, or independently the memory content (persistent and/or non persistent), and transmits the same to the in-cloud server 10 for inspection and verification.

Upon receipt of the memory content (or a portion thereof) of a device 20 from a respective memory extraction module 21, the in-cloud server 10 performs one or more of the following operations:

(1) Analysis of the memory to find malware using static analysis methods;

(2) Analysis of the memory to find malicious behavior using behavioral and heuristics methods;

(3) Reconstruction of the state of the OS to determine and report important structural elements, such as:

a. Process/thread list
b. Communication ports
c. Kernel modules
d. Objects in memory
e. Object in cache
f. Open/close files
g. System status
h. Bootstrap information
i. Memory corruptions

(4) Check of the integrity of the OS and its memory to find fault in the integrity or hidden processes;

(5) A cross-view check on resources to find rootkits and hidden operations. The cross-view collaborates with components as reported from within the OS; and.

(6) A cross-view check and validation of memory contents of plurality of IoT devices.

Following the above perations, the in-cloud server may perform one ore more of the following operations:

(1) Logging of the results;
(2) Reporting the results, raising a warning or an alert in a case of detection of an unexpected code or behaveior; or
(3) Communicating and responding to an IoT request.

For its proper operation, server 10 has a database 11 that contains authentic and reliable data for comparison and verification with the memory content which is received from the IoT devices. For example, the database 11 may contain a copy of the authentic OS which is used in each IoT device 20 and its version number. The database content, whether relating to standard data or proprietary data, is accumulated by the operator of server 10, for example, by contacting the manufacturers of devices 20. The fact that a single server 10 can serve a huge number of devices 20 significantly reduces the costs of obtaining such data. Moreover, the communication between server 10 and devices 20 is typically performed over a secured channel 30. The system of the present invention also overcomes the problem which is associated with the typical IoT devices, namely the lack of sufficient processing power to perform the integrity check in the classical approach.

Server 10 may also perform an update of the OS of each of the IoT devices, when it becomes necessary. The integrity check and/or update may be performed from time to time, or periodically.

As shown, the in-cloud system of the present invention provides protection to IoT devices from damages resulting from malicious code. The system of the present invention provides such a protection in cases where the classical approach is either inapplicable (for example due to lack of sufficient processing power), or impractical (for example, due to the relatively high costs involved in providing of such protection).

While some embodiments of the invention have been described by way of illustration, it will be apparent that the invention can be carried into practice with many modifications, variations and adaptations, and with the use of numerous equivalents or alternative solutions that are within the scope of persons skilled in the art, without departing from the spirit of the invention or exceeding the scope of the claims.

CLAIMS

1. A system for protecting IoT devices from malicious code, which comprises:
   a. a memory extracting module at each of said IoT devices, for extracting a copy of at least a portion of the memory content from the IoT device, and sending the same to an in-cloud server; and
   b. an in-cloude server for receiving said memory content, and performing an integrity check for a possible existance of malicious code within said memory content.

2. A system according to claim 1, wherein said in-cloud server performs one or more of the following:
   a. analysis of the memory to find malware using static analysis methods;
   b. analysis of the memory to find malicious behavior using behavioral and heuristics methods;
   c. reconstruction of the state of an OS of the IoT to determine and report important structural elements;
   d. check of the integrity of the OS and its memory to possibly find fault in the integrity or hidden processes;
   e. a cross-view check on resources to find rootkits and hidden operations; and
   f. a cross-view check and validation of memory contents of plurality of IoT devices.

3. A system according to claim 1, wherein following said integrity check, said in-cloud server performs one or more of the following:
   (1) logging of the results;
   (2) reporting the results, raising a warning or an alert in a case of detection of an unexpected code or behaveior; or
   (3) communicating and responding to an IoT request.

4. A system according to claim 1, wherein the memory, a copy of which is sent to the in-cloud server, is either a persistent memory or a non-persistent memory.

5. A system according to claim 1, wherein said memory extraction module is embedded within a kernel of a respective operating system of the IoT device.

6. A system according to claim 1, wherein said memory extraction module is positioned within a trusted layer at the IoT device.

7. A system according to claim 1, wherein said memory extraction module is positioned within a Trusted Execution Environment at the processor of the IoT device.

1/1

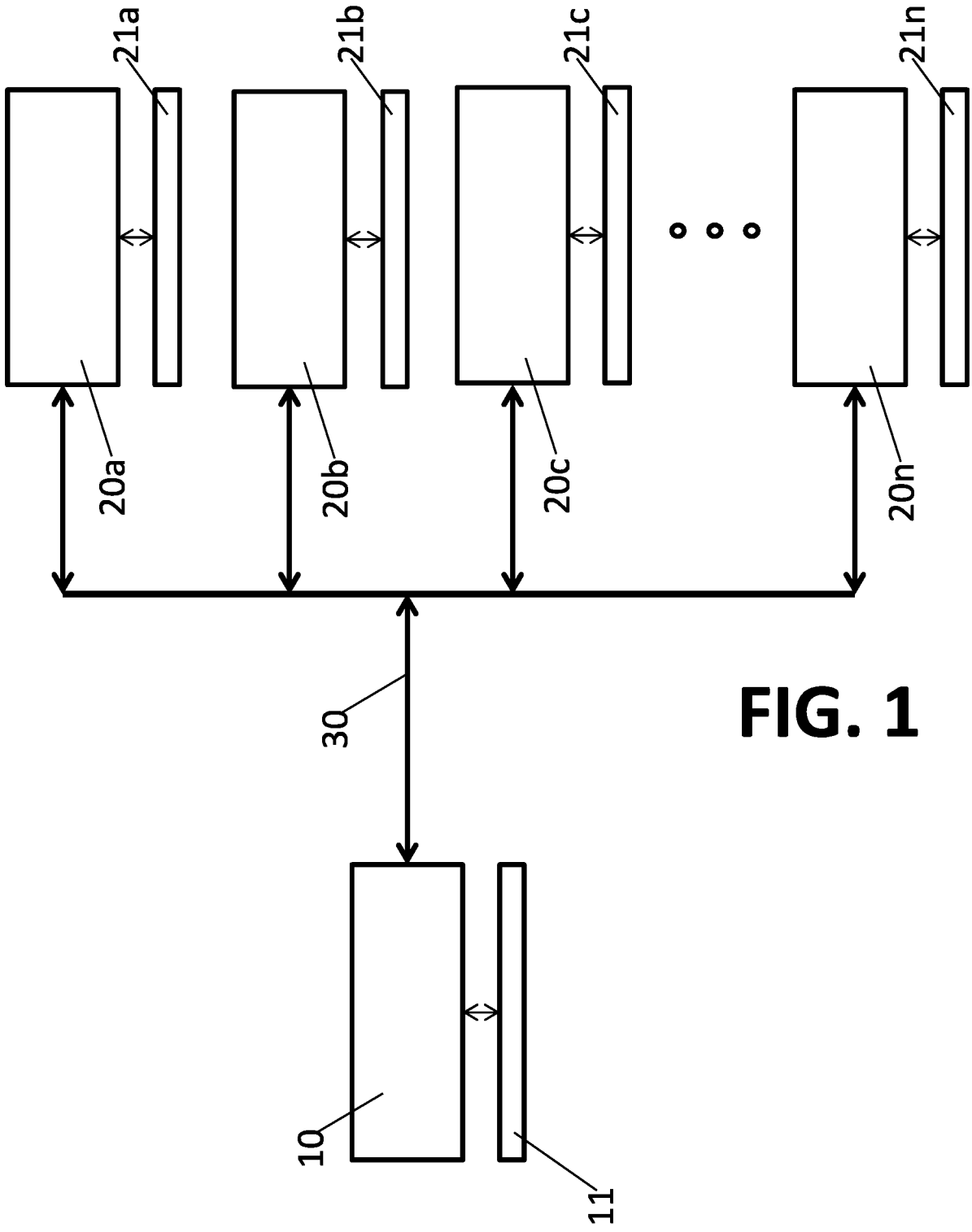

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2017/050277

A. CLASSIFICATION OF SUBJECT MATTER
IPC (2017.01) G06F 21/56, G06F 21/60, G06F 21/55, G06F 21/50

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)
IPC (2017.01) G06F 21/56, G06F 21/60, G06F 21/55, G06F 21/50, H04L 29/00, G06F 11/00, G06F 12/14

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)
See extra sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007277241 A1 SYMANTEC CORPORATION 29 Nov 2007 (2007/11/29) Abstract, ¶¶ 0008, 0022, 0023, 0061, 0062	1-7
Y	US 2014047544 A1 JAKOBSSON BJORN MARKUS 13 Feb 2014 (2014/02/13) Abstract, ¶¶0024, 0025, 0028, 0029, 0039, 0040, 0046, 0051-0055, 0063, Fig 6	1-7
A	US 8904525 B1 Hodgman et al. 02 Dec 2014 (2014/12/02) Entire Document	1-7
A	US 2013227636 A1 APPTHORITY INC 29 Aug 2013 (2013/08/29) Entire Document	1-7
A	US 2013111547 A1 SCARGO INC 02 May 2013 (2013/05/02) Entire Document	1-7

☐ 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
11 Jun 2017	14 Jun 2017
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer COPPENHAGEN Uri Telephone No. 972-2-5657811

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2017/050277

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 2007277241 A1	29 Nov 2007	US 2007277241 A1	29 Nov 2007
		US 7870394 B2	11 Jan 2011
US 2014047544 A1	13 Feb 2014	US 2014047544 A1	13 Feb 2014
		US 9411955 B2	09 Aug 2016
US 8904525 B1	02 Dec 2014	US 8904525 B1	02 Dec 2014
US 2013227636 A1	29 Aug 2013	US 2013227636 A1	29 Aug 2013
		US 8918881 B2	23 Dec 2014
		US 2015143455 A1	21 May 2015
		US 9438631 B2	06 Sep 2016
		WO 2013126259 A1	29 Aug 2013
US 2013111547 A1	02 May 2013	US 2013111547 A1	02 May 2013
		US 9223978 B2	29 Dec 2015
		US 2015350237 A1	03 Dec 2015
		US 9460285 B2	04 Oct 2016
		US 2016373486 A1	22 Dec 2016
		WO 2013063474 A1	02 May 2013

B. FIELDS SEARCHED:

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

Databases consulted: Esp@cenet, Google Patents

Search terms used: malicious code, malware, internet of things device, iot device, device, cloud, network, extract, copy, audit, check, verify, screen, scan, monitor, memory, cache, data, integrity