

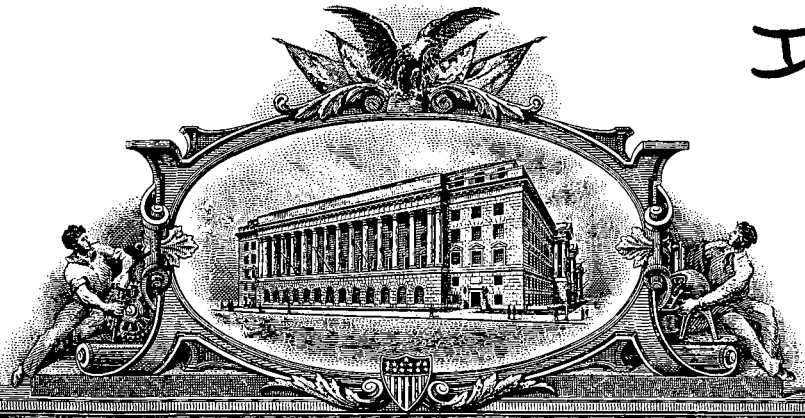
DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:	PCT/IL2017/050277
International filing date:	07 March 2017 (07.03.2017)
Document type:	Certified copy of priority document
Document details:	Country/Office: US
	Number: 62/304,958
	Filing date: 08 March 2016 (08.03.2016)
Date of receipt at the International Bureau:	23 May 2017 (23.05.2017)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)

IL 17/5027

PA 2011004



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

May 09, 2017

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *62/304,958*

FILING DATE: *March 08, 2016*

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS *US62/304,958*

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office



Sylvia Holley
SYLVIA HOLLEY
Certifying Officer

Electronic Acknowledgement Receipt

EFS ID:	25129201
Application Number:	62304958
International Application Number:	
Confirmation Number:	3559
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING ON-CLOUD MEMEORY ANALYSIS, FORENSIC AND SECURITY OPERATIONS ON CONNECTED DEVICES
First Named Inventor/Applicant Name:	Mordechai Guri
Correspondence Address:	B. \G. Negev Technologies Ltd - POB 653 - Beer Sheva - 8410501 IL - -
Filer:	Sarah Grinberg
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	08-MAR-2016
Filing Date:	
Time Stamp:	08:22:22
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$130

RAM confirmation Number	8149
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	Guri1.pdf	91908 <small>P98e7592ac21b9cb56960afa70cdf1e6ce5de69</small>	no	1

Warnings:

Information:

This is not an USPTO supplied ADS fillable form

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

2	Specification	Guri2.pdf	112216 <small>482104ad30556a2208350b2c15376ad3d55b5123</small>	no	2
---	---------------	-----------	---	----	---

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	29708 <small>dba4adbrcffa64aff3eeca0df08a5991492d14f9</small>	no	2
---	----------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes):			233832
-------------------------------------	--	--	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Please type a plus sign (+) inside this box -->

PTO/SB/16 (12-04)

Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)			
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)	
Mordechai	Guri	Modiin, Israel	
<input type="checkbox"/> Additional inventors are being named on the separately numbered sheets attached hereto			
TITLE OF THE INVENTION (280 characters max)			
SYSTEM AND METHOD FOR PERFORMING ON-CLOUD MEMEORY ANALYSIS, FORENSIC AND SECURITY OPERATIONS ON CONNECTED DEVICES			
Direct all correspondence to: CORRESPONDENCE ADDRESS			
<input type="checkbox"/> Customer Number <input type="text"/>			
OR Type Customer Number here			
<input checked="" type="checkbox"/>	Firm or Individual Name	B. G. Negev Technologies Ltd.	
Address	P.O.Box 653		
Address			
City	Beer-Sheva	State	ZIP 84105
Country	Israel	Telephone	Fax 972-8-6276420
ENCLOSED APPLICATION PARTS (check all that apply)			
<input checked="" type="checkbox"/>	Specification	Number of Pages	2 <input type="checkbox"/> CD(s), Number <input type="text"/>
<input type="checkbox"/>	Drawing(s)	Number of Sheets	<input type="text"/> <input type="checkbox"/> Other (specify) <input type="text"/>
<input checked="" type="checkbox"/>	Application Data Sheet. See 37 CFR 1.76		
<small>Application Size Fee: if the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).</small>			
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)			
<input checked="" type="checkbox"/>	Applicant claims small entity status. See 37 CFR 1.27.		
<input type="checkbox"/>	A check or money order is enclosed to cover the filing fees		
<input checked="" type="checkbox"/>	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:	<input type="text"/>	FILING FEE AMOUNT (\$) 130\$
<input checked="" type="checkbox"/>	Payment by credit card. Form PTO-2038 is attached.		
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.			
<input checked="" type="checkbox"/>	No.		
<input type="checkbox"/>	Yes, the name of the U.S. Government agency and the Government contract number are: _____		

Respectfully submitted,

Date 8 / Mar / 2016

SIGNATURE

REGISTRATION NO.
(if appropriate)

TYPED or PRINTED NAME

Sara Grinberg

TELEPHONE

972-8-6461908

Docket Number:

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SYSTEM AND METHOD FOR PERFORMING ON-CLOUD MEMEORY ANALYSIS, FORENSIC AND SECURITY OPERATIONS ON CONNECTED DEVICES

Connected devices such as Internet of Things (IoT) are vulnerable to attacks. Such a devices can be compromised by attackers in order to steal their data or to be used as an attack platform (e.g., as a bot). The classic method in end-points and workstations involved running a detection programs on the computer to detect, scan and analyze for malicious code within the (1) persistent storage (e.g., disk) and (2) non-persistent storage (e.g., memory). Connected devices are limited due to their lower computational power.

We suggests to extract the memory (persistent or non-persistent) of connected device and send it to the cloud for further analysis. The extraction can be done from within the operating system application of module in the kernel, or from trusted layer such as hypervisor, or Trusted Execution Environment (TEE). After extracting the device internal memory the cloud can perform the following operations;

- (1) Analyze the memory to find malware using static analysis methods
- (2) Analysis the memory to find malicious behavior using behavioral and heuristics methods
- (3) Reconstruct OS state to report on important structure 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 the integrity of the OS and its memory to find fault in the integrity or hidden processes
- (5) Perform cross-view checking on resources to find rootkits and hidden operations. The cross-view collaborate with components reporting from within the OS.
- (6) Perform cross-view checking and validation on the content of memory between devices.

The management system on the cloud will;

- (1) Log the results
- (2) Report the results, raising warning or alerts in a case
- (3) Communicate and respond to the IoT

The architecture of the system appear in Figure 1.

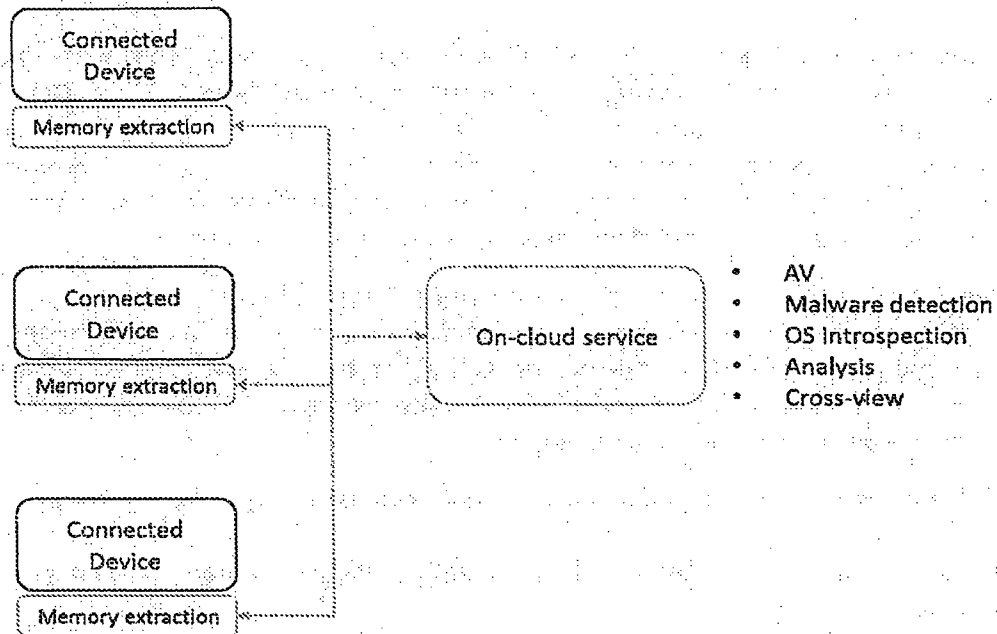


Figure 1. On-cloud service for memory analysis and security operations on connected devices