|  |
| --- |
| **FORM 2**  **THE PATENTS ACT, 1970**  **(39 Of 1970)**  **&**  **THE PATENTS RULES, 2003**  **COMPLETE SPECIFICATION**  **(See section 10 and rule 13)** |
| 1. **TITLE OF THE INVENTION:** A METHOD AND FRAMEWORK OF SANITIZED AND SECURE NETWORK ACCESS TO BYOD DEVICES IN SMALL MEDIUM NETWORKS. |
| 2. **APPLICANT (S)**  **NAME:**  1. Model Institute of Engineering and Technology  **NATIONALITY:** Indian  **ADDRESS:** Model Institute of Engineering and Technology, Kot Bhalwal, Jammu – 181122 Jammu and Kashmir  **2.** Dr. Ankur Gupta  **NATIONALITY:** Indian  **ADDRESS:** Model Institute of Engineering and Technology, Kot Bhalwal, Jammu – 181122 Jammu and Kashmir |
| 3. **PREAMBLE TO THE DESCRIPTION**  **COMPLETE SPECIFICATION**  The following specification particularly describes the invention and the manner in which it is to be performed. |

**FIELD OF THE INVENTION**

The present invention generally relates to effectively detect and prevent compromised BYOD devices from connecting to the corporate networks, thus preventing sensitive and critical business applications and services from malware attacks, and impacting network security.

**BACKGROUND OF THE INVENTION**

BYOD approach permits the users to use their private devices/gadgets to work on official job tasks instead of company-provided devices. It brings along security concerns like malware attacks, sketchy apps, uncontrolled endpoints. To Protect these endpoints, small to medium companies cannot afford the commercials associated with deploying a ready to use BYOD security solutions.

The present invention pertains to detecting, isolating, and sanitizing malicious BYOD hosts before granting full network privileged in a small office network by monitoring the behaviour pattern of critical parameters of the device over a period by isolating, scanning, sanitizing and then permitting full access to the resources each time the device connects to office network without the need to purchase costly solutions to secure BYOD access.

Prior to complete network access, the device will be audited by the Transparent sandbox framework against any Registry changes, application updates so as to detect any changes made to the device and its environment since last connection against its last known recorded System registry Log, security database and HDD checksums so as to mark the device safe/unsafe by determining the impact levels of the changes and sanitizing the device by rolling back the changes to mitigate the effect if any and thereby stopping the spread of malicious codes at the infected host itself.

This can prevent BYOD hosts infected from unsecured network at home or Public Wi-Fi to execute and propagate malicious codes and attacks in a secured office network. As the demand for mobility continues to increase, and Wi-Fi continues to replace Ethernet as the preferred corporate access layer, many organizations are facing new challenges in keeping their assets and resources secure.

**SUMMARY OF THE INVENTION**

It is therefore an object of this invention to provide a system and method of sanitised and secure network access to BYOD devices in small medium networks.

As the demand for mobility continues to increase, and Wi-Fi continues to replace Ethernet as the preferred corporate access layer, many organizations are facing new challenges in keeping their assets and resources secure.

However, there are certain challenges to securing the organization’s Wi-Fi network in a BYOD environment. In general, security risks comprise the most serious challenges in a BYOD environment. Once employees leave the company, they take their personal devices and can connect to any unsecured network at home or Public Wi-Fi and can get affected by malware/ransomware. Enforcing security policies on these endpoints on networks that are not owned by the company is not practiced by many small companies.

BYOD devices such as laptops, phones and tablets are susceptible to cyber-attacks and require constant patch updates to handle security loopholes, and even a single missed patch can leave your company, and its data, vulnerable. BYOD devices are constantly exposed to vulnerabilities, and it is difficult to control which corporate data might be accessed via these endpoints.

If an employee were to accidentally install malware onto their device, while it is connected to the unsecure home or public Wi-Fi network, and when it connects back to the corporate network it could spread the malware to other devices. The employee might even unknowingly install keylogging software, thereby enabling unauthorized users to obtain company usernames and passwords and use them to gain access to sensitive or private enterprise data.

Many organizations’ security implementations focus on the concept of a defensive perimeter, which includes firewalls, intrusion prevention systems and sandboxes as well as endpoint security products such as antivirus software. BYOD and mobile devices including laptops, smartphones and tablets defeat the goal of perimeter security, which is to block an attack at the entry to the organization. Employees, contractors, and customers use these devices inside and outside the perimeter. If their devices are infected with malware outside the perimeter, the malware will be physically carried into the network past all the network perimeter defences.

Most of the work done on detecting BYOD attacks is based on network traffic analysis. It typically involves creating a baseline of normal incoming traffic patterns and detecting any abnormal variations from the known baseline. Once determined that the host is under attack, there is an attempt to drop/ignore packets from the source IP (Internet Protocol) address from where the attack is originating. However, performance is degraded and unless high-availability and load-balancing features are implemented to defray the attack, the application/service under attack is severely impacted.

The proposed method involves changing the perspective on detecting, isolating, sanitizing, and granting access privileges to BYOD hosts and thereby containing BYOD infections at the perimeter and preventing it from propagating to the network.

In accordance with an embodiment of the present invention includes monitoring the behaviour pattern of critical parameters of the device over a period by isolating, scanning, sanitizing and then permitting full access to the resources each time the device connects to office network.

In accordance with an embodiment of the present invention Prior to complete network access, the device will be audited by the Transparent sandbox framework against any Registry changes, application updates so as to detect any changes made to the device and its environment since last connection against its System registry Log and security database so as to mark the device safe/unsafe by determining the impact levels of the changes and sanitizing the device by rolling back the changes to mitigate the effect if any and thereby stopping the spread of malicious codes at the infected host itself.

According to second aspect of the present invention The system includes the transparent sandbox called Access Control Sandbox which is overall responsible for security authentication of BYOD devices post 802.11 phase prior to granting network privileges to the associated BYOD device. It Consists of the following Engines:

A. Device Application Checklist Engine: During the initial phase of the BYOD security authentication, this engine will probe the BYOD device for any changes in its application processes and updates and generate the status as reference for the Log engine

B. Device Profile Database Engine: Its main task is to analyse and compare the current device profile against its device profile database engine for detecting any difference in the system registry, browsing history, hard disk etc of the BYOD device. If difference is found a red flag is raised against the device and is forwarded to the Device Sanitization and Remedial Engine.

C. Device Sanitization and Remedial Engine: This Engine observes the flagged systems and its running applications /transactional data against its vulnerability detection database. If the system detects any out of oridinary application or transaction it is flagged for further investigation to its Sanitization module.

The Sanitization module will try to deliver patch updates to the BYOD device to mitigate the effect of the detected Application and data. Only after successful sanitization the Device will be Flagged as secure to access the secure corporate network segment

D. Network Access Token Engine: The Network Access Token engine offers a time-based access token to sanitised BYOD devices to restricted network resources. This token will be used in addition to the existing authentication mechanisms and will add additional security layer. The Token will be valid till the BYOD device disconnects from the network. Every time the device connects to the network and is marked sanitised a security token will be assigned to it for the session.

E. Client-side component: pen drive based Registry tracking engine. Logs the system registry changes in unsecure networks and updates the Access Control Sandbox of the changes for tracking, isolating, analysing and sanitizing

One aspect of the present invention is to enable small office networks to detect and contain malicious applications hosted on BYOD devices from infecting their computing infrastructure. This is done via Access Control Sandbox . It is a transparent security sandbox which is overall responsible for security authentication of BYOD devices post 802.11 phase prior to granting network privileges to the associated BYOD device.

Another aspect of the present invention is the creation of individual device profiles containing device registry, browsing history patterns and checksum of device hard disk etc in its device profile database. If the device profile of the reconnecting BYOD device matches that with the profile stored in the device profile database, only then it is granted full access to the secure office network or else it is referred to the sanitization engine.

Another aspect of the present invention is the real time detection of the flagged BYOD device and observing its running applications /transactional data against its vulnerability detection database. If the system detects any out of ordinary application or transaction it is flagged for further investigation to its Sanitization module. The Sanitization module will try to deliver patch updates to the BYOD device in order to mitigate the effect of the detected Application and data. Only after successful sanitization the Device will be Flagged as secure to access the secure corporate network segment

The final aspect of the present invention is The Network Access Token engine. It generates a dynamic time based access control token for the sanitised BYOD devices. After the BYOD devices authenticates itself to the network, this engine will generate a token for the device that will allow access to the device for the defined time period. The token sits with the authenticated BYOD device till the session ends or the device logs off the network. Whenever the device attempts to access a network resource, the token assigned to the device communicates with the authorization server. Access is granted or denied based on token type.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The numerous advantages of the present invention may be better understood by those skilled in the art by reference to the accompanying figures in which:

Figure 1 is an exemplary environment of different sub-systems, modules, computing devices and layers etc. for a system and method of sanitised and secure network access , in accordance with an embodiment of the present invention.

Figure 2 is a flow chart illustrating a method for operation of framework for secure and sanitised network access.

**DETAILED DESCRIPTION**

The detailed description set forth below is intended as a description of various configurations of the subject technology and is not intended to represent the only configurations in which the subject technology may be practiced. The appended drawings are incorporated herein and constitute a part of the detailed description. The detailed description includes specific details for the purpose of providing a thorough understanding of the subject technology. However, it will be apparent to those skilled in the art that the subject technology may be practiced without these specific details. Like or similar components are labelled with identical element numbers for ease of understanding. As used throughout this description, the word "may" is used in a permissive sense (i.e. meaning having the potential to), rather than the mandatory sense, (i.e. meaning must). Further, the words "a" or "an" mean "at least one” and the word “plurality” means “one or more” unless otherwise mentioned. Furthermore, the terminology and phraseology used herein is solely used for descriptive purposes and should not be construed as limiting in scope. Language such as "including," "comprising," "having," "containing," or "involving," and variations thereof, is intended to be broad and encompass the subject matter listed thereafter, equivalents, and additional subject matter not recited, and is not intended to exclude other additives, components, integers or steps. Likewise, the term "comprising" is considered synonymous with the terms "including" or "containing" for applicable legal purposes.

Figure 1. is an exemplary environment 100 for a secure and sanitised network access framework capable of detecting, sanitizing and authenticating byod devices for secure and malware free network access. Figure 1. illustrates a central access control sandbox. It is a transparent sandbox responsible for security authentication of BYOD devices post 802.11 phase prior to granting network privileges to the associated BYOD device 106 consisting of multiple engines/modules, 112, 114, 116, device application checklist engine database engine, Device application checklist engine, device sanitization and remedial engine and Network access engine respectively. Device application checklist engine will probe the BYOD device for any changes in its application processes and updates and generate the current status as reference for the Log engine. Device profile database engine will analyse and compare the current device profile against its device profile database engine for detecting any difference in the system registry, browsing history, hard disk etc of the BYOD device. If difference is found a red flag is raised against the device and is forwarded to the Device Sanitization and Remedial Engine. Device santization and remedial engine observes the flagged system and its running applications/trandactional data against its vulnerability detection database. Network Access token engine offers a time based access tokens to to sanitized Byod devices.

Various embodiments of the present invention may now be understood with the exemplary environment 100 as a reference.

FIG 2. is a flow chart illustrating a method for a secure and sanitised network access framework capable of detecting, sanitizing and authenticating byod devices for secure and malware free network access, in accordance with an embodiment of the present invention.

The method starts at step 1 when the Byod device initiates to connect to the wireless access layer and gets authenticated at step 2;

At step 3,the Byod device is redirected to the access control sandbox for security authentication post 802.11, It is a transparent sandbox responsible for security authentication of BYOD devices post 802.11 phase prior to granting network privileges to the associated BYOD device;

At step 3, 4 and 5, the device application checklist engine, a sub-component of the access control sandbox, will probe the byod device for any deviations in its applications and updates and forward the received byod status to the device profile database engine at step 6;

If there is no major variation in the device profile, the BYOD device is granted access to the secure network at step 12;

At step 8, if variation is detected at step 6, the Byod device is referred to the device sanitization and remedial engine;

At step 9, the device sanitization and remedial engine tries to immunize the detected byod device and delivers critical remedial instructions and patch updates;

At step 10 and 11, Post device remedial and sanitization process Byod device is rendered secure access to the critical network resources and granted a time based network access token at step 12, by the token generation engine;

At step 13 the system ceases operation when the Byod device is granted access to the secured network resources;

The previous description is provided to enable any person skilled in the art to practice the various aspects described herein. The previous description provides various examples of the subject technology, and the subject technology is not limited to these examples. Various modifications to these aspects will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects. For example, while the foregoing was described in the context of determining inconsistencies between architectural and structural drawings, it will be understood that other applications may use aspects of the proposed system and method to address related use cases/scenarios. Thus, the claims are not intended to be limited to the aspects shown herein but is to be accorded the full scope consistent with the language claims.

**We claim:**

1. A method for detecting and containing BYOD devices from propagating malware and malicious code/attacks on the network infrastructure, the method comprising:

instantiating and implementing a security authentication of BYOD devices post 802.11 phase prior to granting network privileges to the associated BYOD device;

maintaining a centralized device profile database engine consisting of device for detecting any difference in the system registry, browsing history, hard disk etc of the BYOD device;

maintaining a device profile log of the BYOD device in insecure networks on a portable drive;

comparing the centrally maintained device profile against the current logged device profile on the client portable drive;

if the current device profile matches the profile stored in the centralized profile database the BYOD device is granted access to the resources;

if the current device profile does not match the profile stored in the centralized profile database, the BYOD device is redirected to the sanitization and remedial module for analysis against its application vulnerability database for verifying the vulnerability status of the applications;

performing run time comparison of the detected applications with the trends of known malicious applications and if match is found then the sanitization and remedial module will run the processes to sanitize the BYOD device for network access;

If no matches against known malicious applications are found the BYOD device is still monitored for any resource usage trends which deviate from normal application behaviour baseline for detection and classification;

wherein the database of known malicious applications is updated based on run-time monitoring and analysis, both automated and human, of the application in question;

1. A method as recited in Claim 1, wherein the BYOD registry log, including number of files, their size and checksum’s, of every application installed by the end-user on the BYOD device is checked against the centrally stored BYOD device registry log and compared with known malicious applications and execute permissions denied if match found;
2. A method as recited in Claim 1, wherein the device monitoring and remedial engine monitors detected applications and simultaneously checks the resource usage data for each detected application against the run-time behavioural profiles stored in its vulnerability database of known malicious applications, effectively and efficiently identifying malicious applications;
3. A method as recited in Claim 1, wherein if the system detects any suspicious application or transaction, it is flagged for further investigation to its sanitization module. The sanitization module will try to deliver patch updates and necessary instructions to the BYOD device in order to mitigate the effect of the detected suspicious application and data, Only after successful sanitization the device will be flagged as secure to access the secure network segment;
4. A method as recited in Claim 1, wherein the database of known malicious applications is updated and accessed by device sanitization and remedial engine for early detection and containing malicious applications to misuse computing infrastructure;
5. A method as recited in Claim 1, wherein a Network Access Token engine offers a time-based access token to sanitised BYOD devices to restricted network resources

Date: **Dinesh Jotwani**

Place: **IN/PA 359**

**ABSTRACT**

**A METHOD AND FRAMEWORK OF SANITIZED AND SECURE NETWORK ACCESS TO BYOD DEVICES IN SMALL MEDIUM NETWORKS**

As the demand for mobility continues to increase, and Wi-Fi continues to replace Ethernet as the preferred corporate access layer, many organizations are facing new challenges in keeping their assets and resources secure.

However, there are certain challenges to securing the organization’s Wi-Fi network in a BYOD environment. In general, security risks comprise the most serious challenges in a BYOD environment. Once employees leave the company, they take their personal devices and can connect to any unsecured network at home or Public Wi-Fi and can get affected by malware/ransomware. Enforcing security policies on these endpoints on networks that are not owned by the company is not practiced by many small companies.

BYOD devices such as laptops, phones and tablets are susceptible to cyber-attacks and require constant patch updates to handle security loopholes, and even a single missed patch can leave your company, and its data, vulnerable. BYOD devices are constantly exposed to vulnerabilities, and it is difficult to control which corporate data might be accessed via these endpoints.

If an employee were to accidentally install malware onto their device, while it is connected to the unsecure home or public WiFi network, and when it connects back to the corporate network it could spread the malware to other devices. The employee might even unknowingly install keylogging software, thereby enabling unauthorized users to obtain company usernames and passwords and use them to gain access to sensitive or private enterprise data.

Representative FIG 1

A computer with a blue screen

Description automatically generated with low confidenceA computer with a blue screen

Description automatically generated with low confidenceA picture containing text, phone, cellphone, monitor

Description automatically generated

**WIRELESS ACCESS LAYER (802.11 AUTHENTICATION)**

(Redirect to Sandbox Device Profile)

DEVICE SANITIZATION AND REMEDIAL ENGINE

DEVICE APP CHECKLIST ENGINE

DEVICE PROFILE DATABASE ENGINE

DEVICE PROFILE DB

EE

DB

**ACCESS CONTROL SANDBOX**

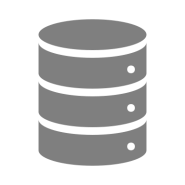
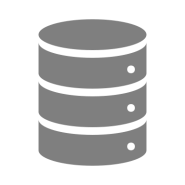
**DEVICE PROFILE**

DEVICE REGISTRY, BROWSING HISTORY, CHECKSUM OF HDD

Network Access Token Generation Engine

**UN-IMMUNIZED INFECTED ACCESS**

**IMMUNIZED NORMAL ACCESS**

**NETWORK ACCESS DENIED**

Fig. 1 Depicting the sequence of operations involved in the proposed method

FLOWCHART

START

1

BYOD USER

2 5

**REQUEST CURRENT DEVICE PROFILE FROM THE BYOD DEVICE**

USER RESPONSE

**SENDS CURRENT DEVICE PROFILE TO DEVICE APPLICATION CHECKLIST ENGINE**

802.11 CONNECTION REQUEST

**APPROVED**

NO

3 YES

DEVICE APPLICATION CHECKLIST ENGINE

DEVICE PROFILE DATABASE ENGINE

DEVICE SANITIZATION AND REMEDIAL ENGINE

VARIATION IN DEVICE PROFILE

4

6

DELIVER PATCH UPDATES FOR DEVICE SANITIZATION

7

NO

8 YES

9 10

11

Network Access Token Generation Engine

**Secure Corporate Network**

Network

13 12

SECURE DEVICE ACCESS