A method for local area network (LAN) security includes monitoring connections between ports (P2, P4, P5) of a central device (12) and a plurality peripheral devices (14a, 14b, 14c) which are respectively cable-connected to the ports (P2, P4, P5), and disabling one of the ports (P2, P4, P5) after detecting a corresponding peripheral device (14a, 14b, 14c) is disconnected from the port (P2, P4, P5).

![Diagram of network connections](image-url)
Description

[0001] The present invention relates to a method for local area network (LAN) security according to the pre-characterizing clause of claim 1.

[0002] Unauthorized access to information, and un-intended or unauthorized use of information in local area networks (LANs) may seriously damage individuals and organizations. Even though LANs can provide a high degree of privacy and security from outside threats, especially when used in conjunction with a firewall, unfortunately, there are still some ways to breach (i.e. hack) the security of LANs. For example, someone can steal a user's ID and password by using a Trojan virus.

[0003] This in mind, the present invention aims at providing a method to improve local area network (LAN) security.

[0004] This is achieved by a method for local area network according to claim 1. The dependent claims pertain to corresponding further developments and improvements.

[0005] As will be seen more clearly from the detailed description following below, the claimed method includes disabling one of ports of a central device when connection to a corresponding peripheral device is detected to be removed.

[0006] In the following, the invention is further illustrated by way of example, taking reference to the accompanying drawings. Thereof

Fig. 1 is block diagram of a local area network adopting the method of the present invention.

Fig. 2 is a flowchart describing how to control the ports of the central device shown in Fig. 1.

Fig. 3 is a diagram of a look-up table of the central device shown in Fig. 1, and

Fig. 4 is a flowchart describing how to authorize the clients to access the server shown in Fig. 1.

[0007] Please refer to Fig. 1, which is a block diagram of a local area network (LAN) 10 adopting the method of the present invention. A plurality of clients 14a-14c are connected to a central device 12 via cables 30a-30c. In this embodiment, the cables 30a-30c are RJ-45 network cables, the clients 14a-14c are personal computers, and the central device 12 can be a hub, a router, or a switch for controlling connections and communications of the clients 14a-14c with a server 20. The central device 12 has five ports P1-P5. The first port P1 is used to connect to a port S1 of the server 20 via another cable 30, and the other ports P2, P4, P5 of the central device 12 are used to connect to the ports C1-C3, respectively, of the clients 14a-14c. In this case, the port P3 is temporarily not used. The clients 14a-14c can access the server 20 via the central device 12, and the central device 12 controls the authorization of the clients 14a-14c for accessing the server 20.

[0008] Each of the clients 14a-14c respectively has a network adapter 22a, 22b, or 22c for communicating with the central device 12. According to the network protocol, such as TCP/IP, the manufacturer of the network adapter 22a-22c must assign a unique media access control (MAC) address to each of the network adapters 22a-22c. Each MAC address is burned into a nonvolatile memory of the network device, i.e. an EEPROM or a flash memory. Therefore, in theory, it is impossible that two network devices have the same MAC address. The MAC addresses of the network devices, hence, can be used to distinguish the network devices from each other.

Please refer to Fig. 2, which is a flowchart describing how to control the ports P2-P5 of the central device 12. The central device 12 has sensors or specific circuits for respectively monitoring the connection statuses of the ports P2-P5 with the clients 14a-14c (step 100). If any of the connections between ports P2-P5 and the clients 14a-14c is detected to be removed, the corresponding port P2, P4 or P5 is disabled by the central device 12 (step 102). For example, if the plug of the network cable 30c is removed from the port P5 or from the port C3, the central device 12 detects the situation and then disables the port P5. It is noted that power switches of the clients 14a-14c do not influence the monitoring by the central device 12. In other words, as long as the network cables 30a-30c are physically kept connected with the ports P2-P5 of the central device 12 and the ports C1-C3 of the network adapters 22a-22c, the central device 12 is not triggered to disable a port P2, P4, and P5. When any of the ports P2-P5 is disabled, the central device 12 forbids all packets transmitted to the disabled port until the administrator of the LAN 10 enables the disabled port. Therefore, if any of the clients 14a, 14b, or 14c is replaced, the central device 12 detects such situation by monitoring the connections with the clients 14a-14c. The security of the LAN 10, hence, is not easily broken by an unauthorized device.

In another embodiment, the central device 10 further controls the functionality of the ports P2-P5 by comparing the MAC addresses. Please refer to Figs. 3-4. Fig. 3 is a diagram of a look-up table of the central device 12 for recording the MAC addresses of the network adapters 22a-22c, and Fig. 4 is a flowchart for describing how to authorize the clients 14a-14c to access the server 20 by comparing the MAC addresses. The central device 12 uses the look-up table to record the MAC addresses of the clients 14a-14c and to control the authorization for accessing the server 20. In an initial state, an administrator of the LAN 10 sets up the look-up table of the central device 12. While setting up the look-up table, the MAC addresses of the authorized clients 14a-14c are recorded in association with the indices of the ports P2-P5. For example, the MAC address recorded in the look-up table corresponds to the port P2 is the MAC address AC1 of the first client 14a, the MAC address corresponding to the port P4 is the MAC address AC2 of the second client 14b, and the MAC address corresponding to the port P5 is the MAC address AC3 of the third client 14c. When
any of the clients 14a-14c asks the central device 12 for authorization to access the server 20, the central device 12 detects the MAC address of the asking client (step 110, Fig. 4) and then compares the detected MAC address with the corresponding MAC address recorded in the look-up table (step 112). For example, when the client 14b asks for authorization, the central device 12 detects the MAC address of the network adapter 22b and then compares the detected MAC address of the network adapter 22b with the MAC address AC2 in the look-up table. If the detected MAC address of the network adapter 22b is different from the MAC address AC2, the central device 12 disables the port P4 (step 116). Oppositely, if the detected MAC address of the network adapter 22b is the same as the MAC address AC2, the central device 12 authorizes the client 22b to access the server 20 (step 114). Therefore, even if a password and ID for logging onto the server 20 are stolen, as long as the MAC addresses do not match, a device with the wrong MAC address cannot access the server 20 via the central device 12 at all. Additionally, in this embodiment, when the central device 12 operates, the connections between the ports P2-P5 and the clients 14a-14c are monitored as in the previous embodiment.

[0011] Finally, in both embodiments, any disabled port can be enabled after a re-authorization procedure. Such a procedure can include repeating one of the previously described methods or can be a manual procedure carried out by a system administrator.

[0012] In comparison with the prior art, the method according to the present invention controls security by monitoring the connections between the ports of a central device and peripheral devices. If any connection is physically removed, the corresponding port of the central device is disabled. Moreover, authorized MAC addresses are compared with detected MAC addresses, so any unauthorized replacement of the network adapter can be easily detected.

Claims

1. A method for local area network (LAN) security, the method characterized by:

   - monitoring connections between ports (P2, P4, P5) of a central device (12) and a plurality of peripheral devices (14a, 14b, 14c) that are respectively cable-connected to the ports (P2, P4, P5);
   - disabling one of the ports (P2, P4, P5) if the detected MAC address of the peripheral device (14a, 14b, 14c) is disconnected from the port (P2, P4, P5).

2. The method of claim 1 further characterized by:

   - recording media access control (MAC) addresses of the peripheral devices (14a, 14b, 14c) in association with indices of the ports (P2, P4, P5).

3. The method of claim 2 further characterized by:

   - authorizing the peripheral devices (14a, 14b, 14c) to access a resource (20) via the central device (12) through the ports (P2, P4, P5); and
   - detecting the MAC address of each of the peripheral devices (14a, 14b, 14c) before authorizing the peripheral device (14a, 14b, 14c) to access the resource (20).

4. The method of claim 3 further characterized by:

   - determining whether to authorize one of the peripheral devices (14a, 14b, 14c) to access the resource (20) via the central device (12) according to the detected MAC address of the peripheral device (14a, 14b, 14c) and the MAC address recorded in association with the index of the port (P2, P4, P5) connected to the peripheral device (14a, 14b, 14c).

5. The method of claim 3 further characterized by:

   - forbidding one of the peripheral devices (14a, 14b, 14c) from accessing the resource (20) via the central device (12) if the detected MAC address of the peripheral device (14a, 14b, 14c) is different from the MAC address recorded in association with the index of the port (P2, P4, P5) connected to the peripheral device (14a, 14b, 14c).

6. The method of claim 3 further characterized by:

   - disabling one of the ports (P2, P4, P5) if the detected MAC address of the peripheral device (14a, 14b, 14c) connected to the port (P2, P4, P5) is different from the MAC address recorded in association with the index of the port (P2, P4, P5).

7. The method of claim 1 further characterized by:

   - enabling the disabled port (P2, P3, P4, P5) after a re-authorization procedure.
Fig. 2

Is the connection removed?

No

Yes

Disable the port
<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2</td>
<td>AC1</td>
<td>Enabled</td>
</tr>
<tr>
<td>P3</td>
<td>Null</td>
<td>Disabled</td>
</tr>
<tr>
<td>P4</td>
<td>AC2</td>
<td>Enabled</td>
</tr>
<tr>
<td>P5</td>
<td>AC3</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Fig. 3
Detect the MAC address

Is the detected MAC address different from the recorded MAC address?

- Yes
  - Disable the port

- No
  - Authorize the client to access the server

Fig. 4
## DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document with indication, where appropriate, of relevant passages</th>
<th>Relevant to claim</th>
<th>CLASSIFICATION OF THE APPLICATION (IPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 03/034687 A (SECURE GROUP AS; HANSEN, TORGEIR; GRUSD, EYSTEN; MEHLUM, THOMAS) 24 April 2003 (2003-04-24) * abstract * * page 1 - page 3 *</td>
<td>1-7</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>&quot;IEEE Standard for Local and metropolitan area networks - Port-based Network Access Control&quot; IEEE STD 802.1X-2001, 14 June 2001 (2001-06-14), pages I-VIII, I, XP002270244 * page 7 - page 12 * * page 21 - page 22 * * page 25 *</td>
<td>1-7</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 5 905 859 A (HOLLOWAY ET AL) 18 May 1999 (1999-05-18) * abstract * * column 3, line 34 - line 56 * * column 7, line 4 - line 10 * * column 7, line 66 - column 8, line 19 *</td>
<td>1-7</td>
<td></td>
</tr>
</tbody>
</table>

The present search report has been drawn up for all claims

<table>
<thead>
<tr>
<th>Place of search</th>
<th>Date of completion of the search</th>
<th>Examiner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Munich</td>
<td>11 August 2006</td>
<td>Kopp, K</td>
</tr>
</tbody>
</table>

### CATEGORY OF CITED DOCUMENTS

- **X**: particularly relevant if taken alone
- **Y**: particularly relevant if combined with another document of the same category
- **A**: technological background
- **O**: non-written disclosure
- **T**: theory or principle underlying the invention
- **E**: earlier patent document, but published on, or after the filing date
- **D**: document cited in the application
- **L**: document cited for other reasons
- **&**: member of the same patent family, corresponding document
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document with indication, where appropriate, of relevant passages</th>
<th>Relevant to claim</th>
<th>CLASSIFICATION OF THE APPLICATION (IPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 6 115 376 A (SHERER ET AL) 5 September 2000 (2000-09-05) * abstract * figure 2 * column 1, line 20 - line 25 * column 2, line 54 - column 3, line 4 * column 3, line 63 - line 65 * column 5, line 4 - line 32 * column 6, line 6 - line 45 * -----</td>
<td>1-7</td>
<td>1-7</td>
</tr>
</tbody>
</table>

The present search report has been drawn up for all claims.
ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO. EP 05 02 0928

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-08-2006

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2005055570 A1</td>
<td>10-03-2005</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>WO 03034687 A</td>
<td>24-04-2003</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>US 5905859 A</td>
<td>18-05-1999</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>US 6115376 A</td>
<td>05-09-2000</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>JP 10023036 A</td>
<td>23-01-1998</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>

For more details about this annex: see Official Journal of the European Patent Office, No. 12/82