IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Device Tracking & Monitoring the Usage

Dr. S. Yamini

Director (Academic) & Associate Professor, Rathnavel Subramaniam College of Arts & Science (Autonomous), Sulur, Coimbatore

Abstract: An identity management system refers to an information system that can be used for identity management within or across enterprise's environment. Identity management includes managing digital identifications, their authentication, authorization, roles & permissions within environment of their operation. Digital identity is a set of attributes that uniquely describes a subject that can be a person, system, phone, tablet device, printer, server, group of users, etc..., Through this research paper, employees and their devices, can access to a different information systems, for instance to the internal web page, e-mail system, CRM (Customer Relation Management) system, VPN service and other internal applications [4]. Many of these applications require users to claim their identity usually carried out through login form where users pass their username and password. For a purpose of increasing security and usability, authentications and authorizations for different applications within an enterprise are carried out through central IDS system.

Keywords: Component; formatting; style; styling; insert (key words).

I. INTRODUCTION

The DHCP protocol lets a DHCP client to lease network configuration parameters such as an IP address. In fact parameters to lease aren't limited to IP address only and they also include:

- IP addresses and network masks
- DNS
- Default Gateways
- WINS servers

Each host set to obtain an IP address dynamically will upon boot send a DHCP request over the network (by definition this is a broadcast of all 1's) to discover whether there is a DHCP server available on the network and consequently ask for an network configuration [10]. DHCP client is then restrict to maintain a communication with DHCP server and renew its IP address regularly as Dictated by IP addresses lease time expiry.

In this case if the DHCP client fails to renew its IP address (disconnection, client is turned off) its IP address expires and DHCP server is free to lease this IP address to another DHCP client [14].

DHCP server keeps a record of all leased IP addresses and stores them into a file called dhcpd.leases which can be found in /var/lib/dhcp directory (location of this file may vary depending on Linux system in use). Having such a file allows DHCP server to keep track of all IP address leases even after its reboot or power failure.

There are some advantages of having a DHCP server connected to network

- No IP address conflicts. DHCP can guarantee that all hosts on the network will have unique IP address. DHCP server maintains a record of all IP addresses assigned and cross reference them with host's MAC addresses.
- Based on the MAC address DHCP will allow for a fixed parameter configuration for a specific host
- Efficiency with those minimum local client configuration the applicable criteria that follow.

II. NAPT

NAT-PT (Network Address Translation - Protocol Translation) gateway is a protocol translation technology, which can convert the packets between the two formats, and all of the conversion is completed by the NAT-PT gateway. Additional burden is not needed on the client, users can able to access each other completely transparent.

NAT-PT system consists of three components: NAT, address translation module; PT (protocol conversion module); ALG (Application Layer Gateway). NAT is responsible for mapping the conversion between the IPv4 and IPv6 addresses, an IPv4 address slot is configured,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Temporary mapping the IPv6 address to the global routable IPv4 address, and NAT-PT gateway is also equipped with a special IPv6 address namely prefix, Which is used for mapping IPv4 Address. DNS-ALG module is the important support in the basic services network of NAT-PT transition mechanism.

III. IDENTIFYING FROM NAPT LOGS DEVICES

Network activity can be logged in many ways, each representing a compromise between the information available, its level of detail, and the size of recorded data.

A packet capture will provide the highest quantity of information, since each packet is recorded, at least in part. Memorized data include the packet header and a portion of the payload that can (a) be empty, or (b) include a fixed number of octets at the beginning of the payload, or (c) include the entire payload [13]. A flow is a set of packets sharing some common properties (typically, at least the source and DESTINATION ADDRESSES A PORT, TOGETHER WITH THE PROTOCOL).

identification results coming from the previously described step. It is worth noting that, in the general setting, the DHCP protocol may be inactive, its logs may be unavailable and the logged MAC addresses may be spoofed which is shown in log Table 1.1.

Table 1.1 TL-WR740N SYSTEM LOG

#

H-Ver = WR740N v4 00000000 : S-Ver = 3.16.6 Build 130529 Rel.47286n

L = 192.168.100.1 : M = 255.255.255.0

W1 = DHCP : W = 192.168.3.2 : M = 255.255.255.0 : G = 192.168.3.1

##

Oct 22 08:38:49 OTHER INFO System started

Oct 22 08:38:59 DHCP NOTICE DHCPC Send DISCOVER with request ip 0.0.0.0 and unicast flag 0

Oct 22 08:38:59 DHCP NOTICE DHCP server started

Oct 22 08:38:59 SECURITY INFO PPTP Pass-through enabled

Oct 22 08:38:59 SECURITY INFO L2TP Pass-through enabled

Oct 22 08:38:59 SECURITY INFO IPSEC Pass-through enabled

Oct 22 08:38:59 SECURITY INFO FTP ALG enabled

Oct 22 08:38:59 SECURITY INFO TFTP ALG enabled

Oct 22 08:38:59 SECURITY INFO H323 ALG enabled

Oct 22 08:39:00 SECURITY INFO RTSP ALG enabled

Oct 22 08:39:01 DHCP NOTICE DHCPC Send DISCOVER with request ip 0.0.0.0 and unicast flag 0

Oct 22 08:39:03 DHCP NOTICE DHCPC Send DISCOVER with request ip 0.0.0.0 and unicast flag 0

Oct 22 08:39:07 DHCP NOTICE DHCPC Send DISCOVER with request ip 0.0.0.0 and unicast flag 1

Oct 22 08:39:07 DHCP NOTICE DHCPC Recv OFFER from server 192.168.2.1 with ip 192.168.2.2

Oct 22 08:39:07 DHCP NOTICE DHCPC Send REQUEST to server 192.168.2.1 with request ip 192.168.2.2

Oct 22 08:39:08 DHCP NOTICE DHCPC Recv ACK from server 192.168.2.1 with ip 192.168.2.2 lease time 259200

Oct 22 08:39:08 DHCP NOTICE DHCPC:GET ip:192.168.2.2 mask:255.255.255.0 gateway:192.168.2.1 dns1:81.4.121.208 dns2:8.8.8.8 static route:0

Oct 22 08:39:08 DHCP NOTICE Dynamic IP(DHCP Client) obtained an IP successfully

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Oct 22 08:39:12 DHCP NOTICE DHCPC perform a DHCP renew

Oct 22 08:39:12 DHCP NOTICE DHCPC Send REQUEST to server 192.168.2.1 with request ip 192.168.2.2

Oct 22 08:39:13 DHCP NOTICE DHCPC Recv ACK from server 192.168.2.1 with ip 192.168.2.2 lease time 259200

Oct 22 08:39:13 DHCP NOTICE DHCPC:GET ip:192.168.2.2 mask:255.255.255.0 gateway:192.168.2.1 dns1:81.4.121.208 dns2:8.8.8.8 static route:0

Oct 22 08:39:13 DHCP NOTICE Dynamic IP(DHCP Client) obtained an IP successfully

Oct 22 08:39:58 DHCP NOTICE DHCPC Unicasting a release of 192.168.2.2 to 192.168.2.1

Oct 22 08:39:58 DHCP NOTICE DHCPC Entering released state

Oct 22 08:41:54 DHCP NOTICE DHCPC perform a DHCP renew

Oct 22 08:41:54 DHCP NOTICE DHCPC Send DISCOVER with request ip 192.168.2.2 and unicast flag 0

Oct 22 08:41:56 DHCP NOTICE DHCPC Send DISCOVER with request ip 192.168.2.2 and unicast flag 0

Oct 22 08:41:58 DHCP NOTICE DHCPC Send DISCOVER with request ip 192.168.2.2 and unicast flag 0

Oct 22 08:42:02 DHCP NOTICE DHCPC Send DISCOVER with request ip 192.168.2.2 and unicast flag 1

Oct 22 08:42:02 DHCP NOTICE DHCPC Recv OFFER from server 192.168.3.1 with ip 192.168.3.2

Oct 22 08:42:02 DHCP NOTICE DHCPC Send REQUEST to server 192.168.3.1 with request ip 192.168.3.2

Oct 22 08:42:03 DHCP NOTICE DHCPC Recv ACK from server 192.168.3.1 with ip 192.168.3.2 lease time 259200

Oct 22 08:42:03 DHCP NOTICE DHCPC:GET ip:192.168.3.2 mask:255.255.255.0 gateway:192.168.3.1 dns1:192.168.3.1 dns2:0.0.0.0 static route:0

Oct 22 08:42:03 DHCP NOTICE Dynamic IP(DHCP Client) obtained an IP successfully

Oct 22 08:46:12 DHCP NOTICE DHCPS:Recv DISCOVER from 78:E4:00:1F:9C:D6

Oct 22 08:46:13 DHCP NOTICE DHCPS:Send OFFER with ip 192.168.100.8

Oct 22 08:46:13 DHCP NOTICE DHCPS:Recv REQUEST from 78:E4:00:1F:9C:D6

Oct 22 08:46:13 DHCP NOTICE DHCPS:Send ACK to 192.168.100.8

Oct 22 08:46:40 DHCP NOTICE DHCPS:Recv RELEASE from 78:E4:00:1F:9C:D6

Oct 22 08:46:40 DHCP NOTICE DHCPS:Recv DISCOVER from 78:E4:00:1F:9C:D6

Oct 22 08:46:41 DHCP NOTICE DHCPS:Send OFFER with ip 192.168.100.8

Oct 22 08:46:41 DHCP NOTICE DHCPS:Recv REQUEST from 78:E4:00:1F:9C:D6

Oct 22 08:46:41 DHCP NOTICE DHCPS:Send ACK to 192.168.100.8

Oct 22 09:41:11 DHCP NOTICE DHCPS:Recv DISCOVER from 70:0B:C0:15:FD:72

Oct 22 09:41:12 DHCP NOTICE DHCPS:Send OFFER with ip 192.168.100.3

Oct 22 09:41:12 DHCP NOTICE DHCPS:Recv REQUEST from 70:0B:C0:15:FD:72

Oct 22 09:41:12 DHCP NOTICE DHCPS:Send ACK to 192.168.100.3

Oct 22 09:46:41 DHCP NOTICE DHCPS:Recv REQUEST from 78:E4:00:1F:9C:D6

Oct 22 09:46:41 DHCP NOTICE DHCPS:Send ACK to 192.168.100.8

Oct 22 09:57:00 DHCP NOTICE DHCPS:Recv DISCOVER from 8C:89:A5:DF:F6:B1

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Oct 22 10:57:00 DHCP NOTICE DHCPS:Send ACK to 192.168.100.4

Oct 22 11:07:17 DHCP NOTICE DHCPS:Recv REQUEST from EC:A8:6B:75:9C:F9

Oct 22 11:07:17 DHCP NOTICE DHCPS:Send ACK to 192.168.100.5

Oct 22 11:08:45 DHCP NOTICE DHCPS:Recv DISCOVER from 00:EB:2D:2D:6D:A8

Oct 22 11:08:46 DHCP NOTICE DHCPS:Send OFFER with ip 192.168.100.7

Oct 22 11:08:46 DHCP NOTICE DHCPS:Recv REQUEST from 00:EB:2D:2D:6D:A8

Oct 22 11:08:46 DHCP NOTICE DHCPS:Send ACK to 192.168.100.7

Oct 22 11:57:00 DHCP NOTICE DHCPS:Recv REQUEST from 8C:89:A5:DF:F6:B1

The device is a NAT router with a DHCP server installed inbuilt. This device needs to be placed after any DSL/ADSL device, through which it can connect to the internal using traditional telephone networks. Purposely this device needs an IP address from the DSL device to communicate with him; and since it (TL-WR74ON) has a DHCP server inside, it can execute DHCP request processing for clients connected in its LAN and W-LAN controller. It needs less to specify that this device needs two above different C\classless subnet /classfull network for the two above mentioned purpose. Here in the topology, this return (TL-WR74ON) is connected with an ADSL device and between them there exists a network of 192.168.2.0/24; and on the client side, there exists a classfull network of 192.168.2.0/24.

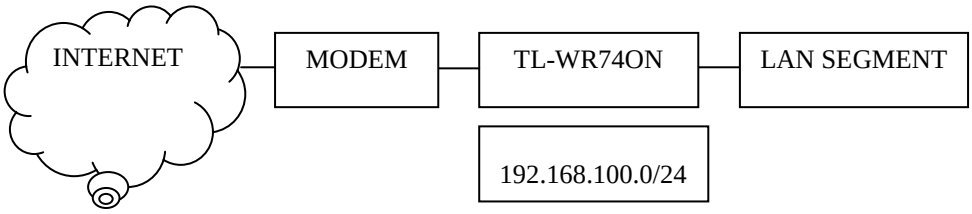

Figure 1.1: Topology where the TL-WR740N is connected

As per the Figure 1.1, this device is acts as a DHCP of the modem to get an IP on its WAN port and also receives like a DHCPS for the LAN segment to provide them IP. The details of the DORA exchange for both as a DHCPC (client) and (server) DHCPS are explained below:

IV. DHCPC

Step 1: It is sending a DHCP Discover request as 0.0.0.0 as its source IP through its WAN port towards 255.255.255.255 as an all subnet broadcast; hoping to get a probe response from any connected and up DHCP server.

Step 2: The modem received this device's DHCPD request and replied with a DHCP offer message containing own IP as 192.168.2.1 and offering IP as 192.168.2.2

Step 3: After receiving the DHCPO message from the server, the TL-WR74ON makes a request message DHCPR to 192.168.2.1, confirming that it needs IP from that device only.

Step 4: The modem sends this device a DHCP Acknowledge and has assigned an IP of 192.168.2.2 with CIDR/24 with a lease time of 259200 seconds.

Step 5: Now, this device TL-WR74ON is having an IP and other L3 optional parameters from the DHCP server 192.168.2.1. The parameters which it accepts are:

- IP: 192.168.2.2
- MASK: 255.255.255.0
- DEFAULT GATEWAY: 192.168.2.1
- PREFFERED DNS: 81.4.121.208
- ALTERNATE DNS: 8.8.8.8

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Step 6:

This marks the end of the DHCP DORA process inside this TL-WR74ON as a DHCP client.

Step 7:

After the maturity of the lease duration, the TL-WR74ON announces a unicasting release request of the Ip 192.168.2.2 to the DHCP-S 192.168.2.1.

Step 8: The IP released request has been accepted by the DHCPS.

Step 9: Since this device is up, running and connected, it made another renew/reissue release request to the server at 192.168.2.1 using the traditional DORA process; Started with Discover over again.

IV.I DHCP SERVER

This device has been configured with a pool of 192.168.100.0/24 IP's for generating distribution on its LAN ports. Similarly like the precious one, the device will also execute the DORA process that new as a DHCP server. The following narration explains the process.

Step 1: TL-WR74ON receives a DHCP Discover request from a client, whose MAC address is 78:E4:00:1F:9C:D6 for IP and other L3 parameters.

Step 2: Upon receiving that broadcast from 78:E4:00:1F:9C:D6; It sends an IP offer of 192.168.100.8 to same MAC.

Step 3: The client sends a DHCP request for seeking permission to the IP 192.168.100.8; here it's been logged as a request received from 78:E4:00:1F:9C:D6.

Step 4: Upon the final configuration received from the client using the IP, this device sends out an acknowledgement to the MAC 78:E4:00:1F:9C:D6 to be the IP 192.168.100.8.

IV.II NAT LOG

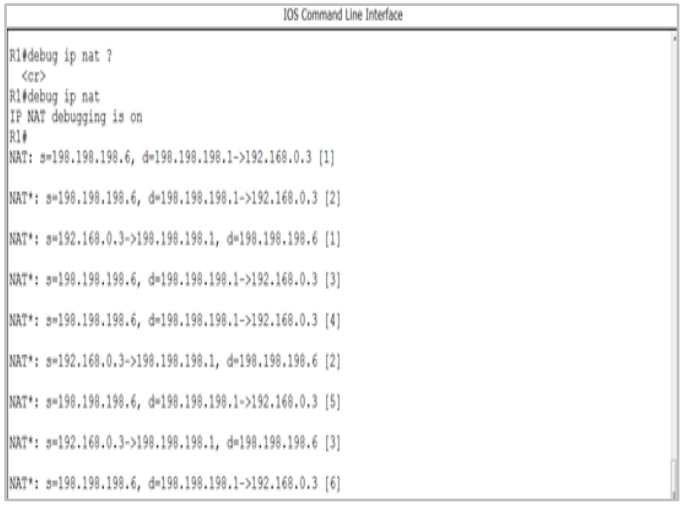

Figure 1.2: NAT table entries

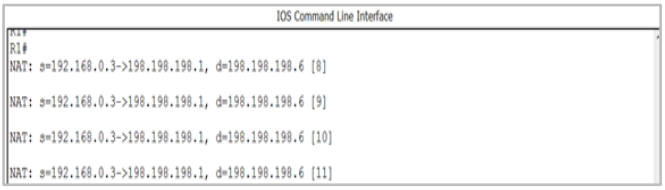

Figure 1.3: NAT Table entries

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

As per the Figure 1.2 & Figure 1.3, the thesis uses a topology of a router performing port address translation and is also connected to two different network viz., 198.198.198.0 and 192.168.0.0. In this diagram, the flow of translation is described as follows:

- NAT: s=198.198.198.6, d=198.198.198.1 192.168.0.3

In this line, a NAT request has been logged for 192.168.0.3 sourcing from 198.198.198.6 and passing through the gateway 198.198.198.1 where the address is getting translated.

- NAT *: s=198.198.198.6, d=198.198.198.1 192.168.0.3

In translator part here is same, only exception is it has been marked as with an asterix (*) which means it will be fast routed to the destination.

- NAT *: s=192.198.0.3 198.198.198.1 d= 198.198.198.6

This entry is for the return traffic from 192.168.0.3 to 198.198.198.6: but after translations, the original IP (192.168.0.3) will be abstracted and it will be represented as 198.198.198.1 is sourcing the data to 198.198.198.6.

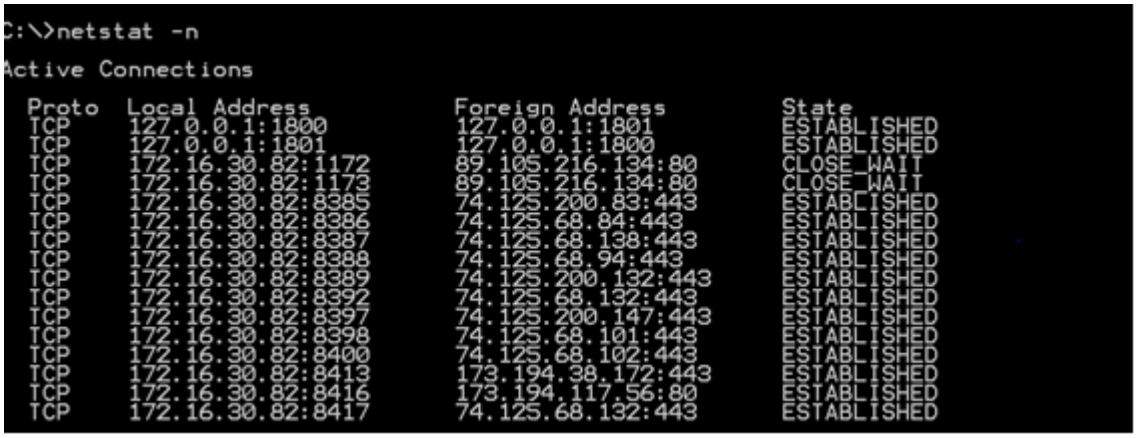

Figure 1.4: Net Stat output in users' system

The screen shot which is shown in Figure 1.4 has been taken from the client's console that is accessing internet after passing through a port address translation process. The output contains several columns that demands suitable and necessary explanation:

This column lists the most vital part of the user tracking system. It reflects the TCP sockets of the client from this output has been taken (IP: 172.16.30.80) which shows that the client alone is accessing 14 internet work resource and 2 loopback queries. Save and except the loop back queries, the 14 cross network queries is of absolutely different and so they are categorized in different TCP sockets.

An important point to notice here is that while socketing the source requests, the port numbers used are between the range of 1025 to 65535.But the data's are destined for well-known ports i.e. between 0 1024.

- Foreign Address

This column reflects the destination of the requests. Since the destination is a public data area, the sockets are having public IP address.

- Protocol

This column reflects the name of protocol used for delivery mechanism.

- Connection State

This column reflects the state of the connection in terms of whether its running, established closed and or terminated it may also reflect the TCP handshaking process, if and when it happens.

V. CONCLUSION

Finally, at its end, this paper needs to highlight and take into account the necessity of travelling and monitoring the internal users upon their internal activity and external activity as well. Further, this paper takes into consideration explaining, discussing and implementing the various user-cum-device tracking mechanisms like NAPT logs, DHCP logs, Cisco switches logs of port security and interface statistics as being dumped in and syslog and Simple Network Management Protocol (SNMP) databases. It also stretches the necessity of maintaining the logs from various perspective and various sources of the same in order to track the users most effectively and appropriately. Even on a greater extent this paper explains the individual sockets which are highlighted in the captured logs, so that the current state of the user can be understood by the authenticator properly and effectively.

REFERENCES

[1] Adams and Sasse M.A., "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, (1999).
[2] Ahn, L., von, Blum, M., Hopper, N.J. and Langford, J. CAPTCHA: Telling humans and computers apart. In Advances in Cryptology, Euro-crypt '03, volume 2656 of Lecture Notes in Computer Science, (2003), 294–311.
[3] Ahn, L. Von, Blum, M., Hopper, N.J., and Langford, J," CAPTCHA: Using hard AI problems for security", Springer Berlin Heidelberg, Pages- 294-311.
[4] Aniello Castiglione, Alfredo De Santis, Ugo Fiore, Francesco Palmieri, Device Tracking in Private Networks via NAPT Log Analysis, Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, (2012).
[5] Ayannuga Olanrewaju O. and Folorunso Olusegun, "Graphic-Text Authentication of a Window-based Application," International Journal of Computer Applications, Vol. 21, No. 6, pp. 36-42, (May 2011).
[6] Bao Wen, S., "Planning and Design of e-Commerce System," Higher Education Press, Beijing, (May 2008), pp. 300-310.
[7] Behrouz A. Forouzan "Data Communication and Networking," (2nd ed.,) China Machine Press, Beijing, (2002) pp. 305-308.
[8] Ben Maddock, Port Knocking: An Overview of Concepts, Issues and Implementations, SANS GIAC GSEC Practical (2004).
[9] Doverspike, B. and Cortez, R., "Restoration in carrier networks," in Proc.7th International Workshop on the Design of Reliable CommunicationNetworks, 2009, pp. 45–54.
[10] Erlbaum, R. and Sidi, M., "Topological design of local-area networks using genetic algorithms," IEEE/ACM Trans. Networking, vol. 4, pp.766–778, 1996.
[11] Gong, Yi. W., "Computer Network" Tsinghua University Press, Beijing, March. 2007. Pp.168 175.
[12] Hong Ma, Yongjuan Wu, Yan Ma, Zhenhua Wang, and Optimization Scheme of CGN logs, Proceedings of IEEE CCIS2012.
[13] Sivakumar, S., Logging of NAT Events, Internet-Draft, Expires: April 26, 2012. Stuart Cheshire, NAT Port Mapping Protocol (NAT- PMP), Internet-Draft, Expires 16th October 2008
[14] Sun Pengcheng, Zhou Lihua, Research on Log Management System in Linux, Electronic Sci. & Tech.2007 (07), 72-74.1989.