ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Development and Deployment of Wake on Lan (WOL) Handler in Network Environment

Radheshyam Isarapu
Department of Computer Science and Systems Engineering,
Andhra University College of Engineering (Autonomous), Andhra University,
Visakhapatnam, AP- 530003, India.

D.Lalitha Bhaskari
Department of Computer Science and Systems Engineering,
Andhra University College of Engineering (Autonomous), Andhra University,
Visakhapatnam, AP- 530003, India.

Abstract:
Wake-on-LAN (WOL) is a widely supported networking standard that allows computers to be turned on remotely. The majority of desktop hardware is WOL capable, though many organizations look at this feature as a power saver utility, it poses to be a security threat to the entire network as well as for the individual workstations if any unauthorized token is raised and sent across the network. Hence this vulnerability has to be handled from the network administrative perspective. Effective usage of WOL in a network is still in fundamental phase. The aim is to develop a software package (vulnerability handler) which can be deployed into the network environment as well as the individual work stations in order to counter any unauthorized access over the workstation and the network. The proposed software handler can be deployed from the server or at the desktop system which is cross platform supported and independent of the version of the operating system. The effective functionality is on the bios of the system only.

Index Terms:
Network Security, Wake-on LAN, WOL, Hardware security.

INTRODUCTION:

In 1996, Intel and IBM formed the Advanced Manageability Alliance (AMA) with the goal of developing non-proprietary, standards-based tools, in order to simplify PC manageability (O'Malley T., 1998). The following year, this alliance introduced WOL, which allowed computers to be turned on remotely via a special network message known as a Magic packet ("Wake on LAN Technology," 2006) [1]. As a part of this initiative, baseline systems were required to have the ability to be woken up remotely by one of the three remote wakeup techniques: magic packet, packet filtering, or wake-on-ring. Protocol (WOL) is a widely supported networking standard that allows computers to be turned on and off remotely. WOL is platform independent and supported by most modern computers including both IBM compatible PCs and Apple Mac based systems. WOL is implemented using a special type of network message or packet called as Magic packet [2]. Protocol (WOL) is a widely supported networking standard that allows computers to be turned on and off remotely. WOL is platform independent and supported by most modern computers including both IBM compatible PCs and Apple Mac based systems. WOL is implemented using a special type of network message or packet called as Magic packet, which is sent to all the computers in a network or to designated client system. The magic packet contains the MAC address of the destination computer, an identifying number built into each network interface card ("NIC") or other Ethernet device in a computer, that enables it to be uniquely recognized and addressed on a network.

Cite this article as: Radheshyam Isarapu & D.Lalitha Bhaskari, "Development and Deployment of Wake on Lan (WOL) Handler in Network Environment", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6, Issue 1, 2019, Page 56-59.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Powered-down or turned off computers embedded with built in Wake-on-LAN feature which will be able to "listen" to incoming packets in low-power mode while the system is still powered down. If a magic packet is received that is directed to the device's MAC address, the network interface card (NIC) sends a signal to the computer' motherboard to initiate system wake-up, in the same way that pressing the power button would do. So we developed a software to disable the WOL as and when necessary using a software handler.

Challenges in implementing the WOL:

- Need of access and authorization across the network and remote computer systems.
- Critical shortage of network administrators who can handle WOL
- Accessing the hardware may not be possible remotely
- Connectivity (Lan/Man/Internet)
- Security and privacy of network laws are to be implemented across the unsecured networks.
- WOL requires correct hardware and software support to function; which is typically not an issue with modern computers and networks, but to develop this software we have to test computer systems across a network.

Existing system:

As per our investigations, there is no Effective usage of WOL in a network and the tools available to handle the WOL are still in fundamental phase. Aquila Wake-On LAN successfully sent the WOL packets to the destination computer, but did not let us specify how the magic packets were sent (i.e. unicast, broadcast, or subnet directed broadcast). Also, its built-in scheduling feature did not work with Windows XP On the other hand, Mat code's command line tool MC-WOL allowed us to specify how the magic packets were sent (i.e. unicast, broadcast, or subnet-directed broadcast), but it had no built-in scheduler [3].

Literature Review:

In 1998, the Intel based initiative Wired for Management introduced a new specification to help reduce the total cost of ownership of business computers. As a part of this initiative, baseline systems were required to have the ability to be woken up remotely by one of three remote wakeup techniques: magic packet, packet filtering, or wake-on-ring. This initiative, among others, provided additional support for **WOL**, but has since been replaced by the Intelligent Platform Management Interface (IPMI) and Intel Active Management Technology (AMT) standards. Major works are not happening in the area of **WOL** implementation as there are many tool which are available in open source for free to utilize the most out of this feature Unless the network hardware is configured to only allow traffic that meets specific security requirements, WOL packets can be sent by anyone on the same local area network (LAN) as the destination computer(s) are available in the network. Once a computer is powered on, attackers may be able to scan it for vulnerabilities [6].

Simply leaving the computer turned on, however, exposes the computer to vulnerability scanning even more. Whether or not WOL is implemented, strong security policies must be put in place to protect the system. Some network interface cards supports password security, but encryption is generally not supported, which leads to low level of security and vulnerable to sniffers. On a computer that is properly configured by WOL, even though if a system is completely powered down, the network interface card (NIC) [6] remains powered on and waits for a special network message called a magic packet. This magic packet helps the system to receive and implement the commands from the network administrator. Today's Information Technology environment is prone to a lot of network security threats and if WOL is not configured properly or practiced it may emerge out to be a threat to network security [3].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The majority of desktop hardware is WOL capable, though many organizations look at this feature as a power saver utility, it poses to be a security threat to the entire network as well as for the individual workstations if any unauthorized token is raised and sent across the network and hence this vulnerability has to be handled from the network administrative perspective.

Proposed system:

In this proposed system we create a software handler which can disable the Wake-On LAN on the target computer systems as well as which can enable it as and when necessary by the computer network administrator. This paper gives the basic understanding on how Wake-On LAN can be utilized to handle the network computers remotely. In this design we make use of the network functionality called magic packets [6] which are sent across the network to handle the target computer systems remotely. With the abundance of free WOL utilities, there is no reason for organizations not to implement it for its benefits in energy conservation and network administration. Magic packets can easily be sent across subnets by configuring routers to use IP directed broadcasts, and the security issues can be minimized by implementing access control lists. Also, scheduling WOL could be particularly useful for universities, as it could allow administrators to turn on computers every morning or when necessary [4].

V. Design and Methodology

Wake-on-LAN requires correct and proper configuration of the system BIOS and operating system to function. There are sometimes several interlinked settings and it may require several combinations to be tested to achieve successful WOL. BIOS configuration is usually straightforward but may be complicated by the different terminology used by each BIOS vendor. The setting is often located in either the Power or Boot sections of the BIOS configuration and may be described as Wake-on-LAN, PME, PM Wake-up Events, and Wake-up Control, Remote Wake or similar names. The following Fig. 1. Shows the typical Bios setting of Wake-On LAN functionality listed the mother board setting of a Hp ProLiant DL 385 computer system. So, if the WOL setting is enabled by default and if any unauthorized token is raised and sent across the network that may make the system behave in an undesired way [6]. Hence we develop the software handler which will automatically disable the WOL to disabled state and it is developed such that in future if the network administrator desires to enable it, then it should enable the feature in the bios [3].

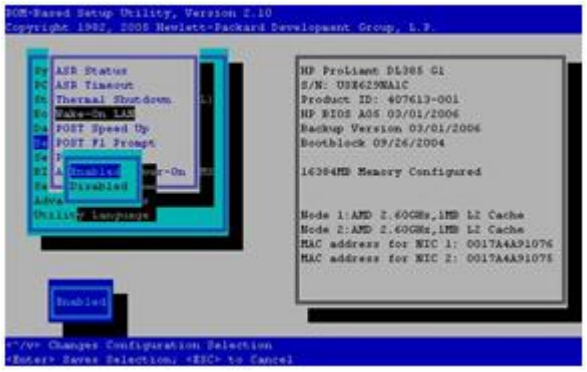

Fig.(1) Bios setting of WOL in Hp ProLiant DL 385

Our goal in creating this software is to demonstrate and develop WOL handler that could be implemented easily and inexpensively, using existing software tools, and without the use of a local agent (software that is installed on client computers). In order to simulate the bios settings in the hardware configuration we need to have administrator privileges over the individual computer system. So one has to remember that all the work is done in this paper expecting the administrator has over all permissions over the network and the system. We have checked the operability, functionality and performance in the windows and Ubuntu environments using the PowerShell and Ethtool simultaneously [7].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

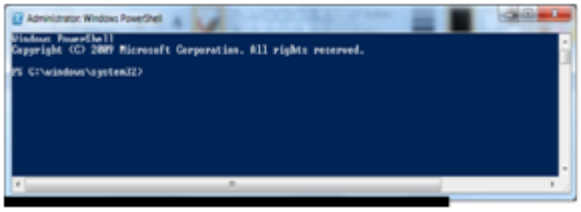

Fig (2.) In windows environment using Powershell utility

Fig (2.1) command to disable WOL in NIC adapter

Fig (2.2) successful execution of command

In Ubuntu Environment using Ethtool

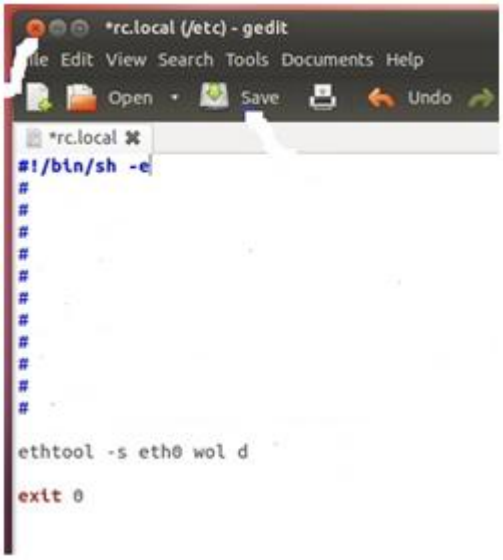

Fig (3) Using Ethtool to know the status of WOL

Conclusion:

So far there is no utility which can scan and disable the Wake-On LAN feature at the bios –level. In this paper we have developed a model such that it scans the systems in the network range and disables the WOL in the bios of the mother board so as to make the system robust non-vulnerable sniffers and prevent security attacks. The code is tested in dot net framework developed in visual studio, and c#.

References:

[1]. IBM Personal Systems Group. "Information Brief – Wake on LAN URL:http://www.pc.ibm.com/us/infobrf/iblan.html (27 March 2002).

[2]. Manageability Alliance (AMA) Implementing Wake-on-LAN in Institutional Networks - Patrick Luberus, Abilene Christian University **(**Journal of Applied Business and Economics vol.6(1) 2014 **).**

[3]. Wake-On-LAN Explained. Data Synergy TechNote: Revision 5.2 January 2018.

[4]. EMBEDDED SERVER WITH WAKE ON LAN FUNCTION Mircea Popa1, Member IEEE, Titus Slavici2.
1"Politehnica" University, Faculty of Automation and Computers, Timisoara, Romania.
2"Politehnica" University, Faculty of Mechanics, Timisoara, Romania.

[5]. Wake on LAN Technology Rev 2 – White Paper Publication June 1, 2006

[6] Network Security for Wake-On-LAN Technology Andrew A. Scheible, Global Information Assurance Certification Paper Version 1.3.

[7]. Measure and Evaluate Delay Time for Wakeup on Lan (WOL) Method of OpenFlow Switch Journal of Electrical and Electronic Engineering 2016; 4(3): 68-72 doi: 10.11648/j.jeee.20160403.15 ISSN: 2329-1613 (Print); ISSN: 2329-1605.