GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Andrew A. Scheible
GSEC Version 1.3

Network Security for Wake-On-LAN Technology

ABSTRACT

Reliable software distribution in a large network is complicated by energy saving policies that dictate powering off computers during non-business hours. To reduce network congestion and limit user disruption, off hours are the best time to push software to corporate PCs. Wake-On-LAN (WOL) technology is intended to overcome this limitation by enabling network interface cards to recognize a special 'magic packet' that initiates an unattended power-on sequence. Transport of this packet from the software distribution servers to remote subnets containing target nodes normally requires disabling security features in the routers intended to stop 'broadcast storms' and reduce the potential of denial of service attacks.

This paper exams the function of the magic packet technology and explores options in the Cisco IOS to curb dangers to the network from WOL usage. Some attacks utilizing directed broadcasts are discussed and router features to reduce the risks are examined. Potential problems outside of network configuration that could hinder successful distributions are also discussed. Recommendations for router configurations are made to allow filtering of directed broadcast to only those used for WOL. The conclusion reached is that WOL technology can safely be used to implement software distribution, without requiring user cooperation in leaving PCs on during the distribution windows.

BACKGROUND

One component of the Tivoli Enterprise System Management (ESM) suite is software distribution. The distribution of software is bandwidth intensive and, to minimize its impact on the network and computer users, downloads should be scheduled for non-work hours. Due to energy conservation measures, PC users have been requested to power off their computers when leaving work. All of our PCs have network cards with the Wake-on-LAN feature to allow remotely powering on the PC to facilitate remote management and the downloading of software.

The initial proposal from IBM Tivoli required allowing broadcast packets to be sent across the entire network from the Tivoli Management Region (TMR) servers at the national level to power on the PCs. However, from a network perspective, this was considered an unacceptable risk. One of the benefits of a routed network is the containment of broadcasts to the local area network. In addition to the reduction of potential broadcast storms throughout the network, there also are serious security issues

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

with denial of service attacks. These attacks utilize the widespread distribution of broadcast packets in a network to launch an attack on the Internet. With a 40,000 seat network using over 1000 routers, that approach represents a huge opportunity for attackers to inflict serious disruption of the Internet originating from our networks, as well as disruption of our internal links.

After discussing our concerns with IBM Tivoli, a patch was made available in a version of the Framework software released in early 2002 that allowed the gateway servers to generate the WOL packet in only those subnets managed by the gateway server. The initial proposal for this new feature was to only turn on directed broadcasts where the WOL packets had to reach subnets outside the gateway LAN. While reducing the range of denial of service attacks, the new approach still requires reducing recommended network security features to function. The network administration impact of only allowing directed broadcasts where required represents a significant and ongoing workload as the ESM architecture evolves.

To explore the issues, a small group met to assess the alternatives and to try to mitigate the potential network impacts from utilizing WOL technology. The results indicate that we can implement WOL in a relatively secure fashion if both network and ESM managers work together to properly configure routers and assure consistency in the ESM inventories.

WAKE-ON-LAN TECHNOLOGY

A key to successful software distribution that reduces administrative overhead is to assure the software can install on a class of machines regardless of the state of the computer during the distribution window. The Tivoli ESM package gives remote managers tools to schedule jobs from centralized administrative servers. Software is bundled in a job and transmitted once over the network to a 'gateway' server closer to the destination nodes, thus reducing network traffic. Multiple copies of the software package only travel the paths from the gateway servers to those computers within their management domain. Location of the gateway systems can be designed with network capacities as a factor. Under the newest version of Tivoli Framework, the magic packet is generated from the gateway server to the end nodes under its jurisdiction. The following discussion is from an IBM information brief discussing their use of WOL technology in their PCs:

> **Definition of the Wake-up Frame**
>
> The wake-up frame contains a unique data field not normally expected in typical traffic on a LAN. When a Wake on LAN-enabled adapter on a turned-off client decodes this data field, a wake-up signal is generated. This wake-up signal causes the client to power on.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 1 shows the format of the wake-up frame. The key to the wake-up frame is the MAC address of the target client, which is repeated 16 times. This pattern of 16 addresses in the data field is not expected to occur in any normal LAN frame other than the specific wake-up frame.

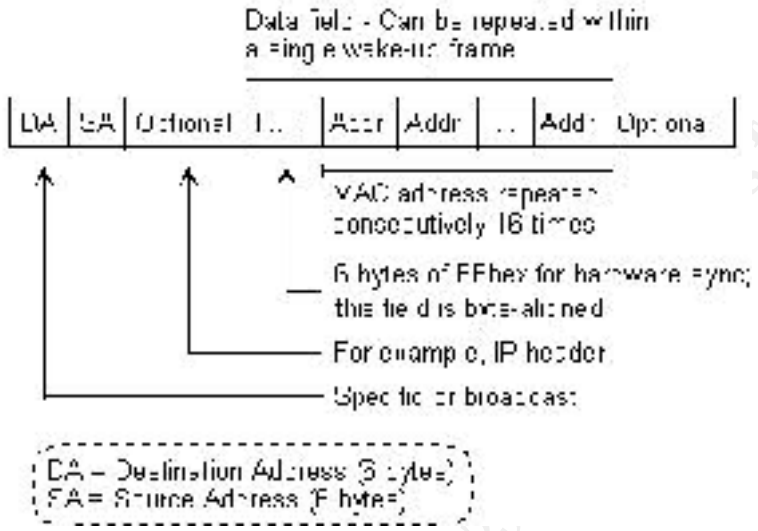


Figure 1. Format of the wake-up frame

The destination address can be either a specific address or a broadcast address. If the destination address is a specific address, the wake-up frame is sent only to the client at that address. However, since the client is powered off and no longer transmitting, some protocols remove this client's MAC address from routing tables and internal caches at other nodes. In this case, wake-up frames addressed directly to the target client are discarded because nodes and routers do not know where to send them.

The solution to this problem is to use a broadcast address. A directed broadcast has a valid network address and a broadcast host address. Network routers and nodes forward directed broadcasts to the appropriate network, where it is seen as a MAC-level broadcast and detected by the powered off client.

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

NETWORK ISSUES

One of the basic functions of a router is the suppression of broadcast packets outside of a local area network. This feature is intended to prevent broadcast storms from saturating

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the slower speed WAN links and to reduce the processing load on computers induced by broadcast traffic. However, protocols such as BOOTP, DHCP, and WOL often need to traverse subnet boundaries using broadcast packets to serve their purpose.

In order for the broadcast packet to reach a subnet outside of the LAN within which the packet was generated, the broadcast packet is often converted to a directed or layer 3 broadcast. In a layer 2 broadcast, all 32 bits of the destination address are set to 1. In a layer 3 broadcast, only the host portion of the address is set to all 1s. Since the network and subnet portions of the address are valid, the packet can be routed to the destination subnet. When it reaches the final router that connects to the subnet, if the interface is configured for directed broadcasts, the router converts the packet header to a layer 2 broadcast directed to all devices in the subnet. If directed broadcasts are not allowed, the packet is dropped.

Directed broadcasts were enabled by default in versions of the Cisco Internetwork Operating System (IOS) prior to Release 12.0. Due to the emergence of network based attacks utilizing directed broadcasts, Cisco disabled directed broadcasts by default in releases of IOS from version 12.0 forward. With the large number of routers in our network and the diverse administrative control of the routers, there is no consistency in IOS versions running on the routers. In addition, some administrators disabled directed broadcasts in pre-release 12.0 routers. Therefore, the only way to determine the state of the directed broadcasts will be an evaluation of each interface on all routers.

SECURITY ISSUES

A group of Denial of Service attacks rely on the use of directed broadcasts to heighten their effectiveness.

Smurf Attacks

In Smurf attacks, a packet is crafted that spoofs the source address of the intended victim. By sending the packet as an ICMP echo request (ICMP packet type 7) to the destination (reflector) address, an echo response is generated to the victim address. By using a broadcast address for the reflector, an entire group of subnet devices can be made to send an echo response to the victim. This magnifies the effectiveness of a single request packet by the size of the subnet being used. The result can be a loss of connectivity for the victim due to an overload of their network link. The reflector network will also suffer degradation due to the increased traffic. To reduce the risk of being used in a denial of service attack, all basic primers on router security suggest turning off directed-broadcasts. (For more information see http://www.pentics.net/denial-of-service/white-papers/smurf.cgi)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Fraggle Attacks

A variation of the Smurf attack, known as Fraggle, utilizes the same concept but makes use of the UDP protocol rather than ICMP. Packets are crafted and sent by the attacker using a spoofed source address of the victim. Normally, the destination port is the UDP echo port (7) but the chargen port (19), which generates a string of 72 ASCII characters sent to the victim in response to the request, is also used. On some types of nodes, the attacker can create a loop between the echo port and the chargen port magnifying the volume of traffic generated.

UDP Diagnostic Port DOS Attacks

One additional concern involves the use of the discard port (9) as the destination of the WOL packet. Cisco Systems has identified a potential denial of service attack using the UDP diagnostic services (http://www.american.com/warp/public/707/3.html). Cisco routers may have servers turned on to allow diagnostics services common to TCP and UDP. The UDP services include echo, chargen, and discard. When a host attaches to these ports, a small amount of router CPU resources are consumed. If many requests are received, the overload can cause the router to fail due to lack of CPU resources. Since the router Ethernet port is assigned an IP address in the subnet, it will respond to the broadcast packets. The potential exists for a poorly designed Tivoli job to cause a failure of the router. To prevent this occurrence, the udp small servers option should be turned off in the router. No known essential uses of these services exist in our network.

Perimeter Security

The logical choice to prevent denial of service attacks is the perimeter entry points into the network. Our Internet connection points are well defined and secured against most access problems. However, the availability of asynchronous ports on the 2500 series Cisco routers has allowed easy configuration of local dial in access. These access points are more difficult to secure due to the wide spread distribution and variable administrative control. Breach of one of these access points gives an attacker relatively unrestricted access to the internal network.

Broadcast Packet Restriction

The destination port used by the WOL packet is irrelevant in the function of the process. The payload of the repeated MAC address is the key to powering up the PC. Fortunately, the port selected in the Tivoli WOL implementation is the discard port (9). The most secure design for transport of the WOL packet with directed broadcasts would limit the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

sources of the packet to the gateway server only. This would require a different configuration on every router port. By limiting the destination port to the 'discard' port 9, the usefulness of the PC as a reflector device in a Smurf or Fraggle attack is nullified. While the broadcast packets may reach the subnet, no PCs would send a response packet to the 'victim' system. This lack of denial of service response should remove the temptation to use our network for a reflector pool to launch an attack.

ALTERNATIVES

As Is Condition

Directed broadcasts are a key to making WOL work in a WAN environment. The default setting of the routers is based on IOS versions. In IOS release 12.0 and above, directed broadcasts are turned off by default due to the security concerns. In pre-Release 12.0, it was on by default. Some network administrators turned directed broadcasts off in pre-12.0 routers due to the security concerns. This makes the reliable use of WOL unattainable in the current network due to the uncertainty of directed broadcasts reaching the intended subnet.

Non-WOL Software Distribution

Based on limited surveys, many large organizations that use software distribution consider the risks of WOL and directed broadcasts to over-ride the convenience of remotely powering up hosts that have been shut off. They opt to have time frames when all devices are left on to allow the distribution of the software during off hours. Invariably some devices are not left on during the distribution window and must be updated manually.

Full Implementation of WOL Technology

From the view of systems administration, the use of WOL technology provides a powerful tool for use in ESM to assure current and consistent versions of software exist on the corporate PCs. After studying the process and router configuration capabilities, it would appear that the security risks can be minimized (although not eliminated). Since our network uses predominantly Cisco routers, we can take advantage of features in the Cisco IOS to provide some additional security. One option includes only turning on directed broadcasts in those interfaces that are between the gateway server and subnets containing devices managed by the gateway. This reduces the 'reflector' pool available to attackers. Unfortunately, in a large, evolving network, this approach creates an additional level of administrative complexity that may not be warranted

As previously mentioned, the destination port used by the WOL packet is irrelevant in the function of the process. The payload of the repeated MAC address is the key to powering

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

up the PC. Fortunately, the port selected in the Tivoli WOL implementation is the discard port (9). Packets to this port will not generate a response that could be used in a denial of service attack.

The Cisco IOS provides a method of filtering packets known as Access Control Lists (ACL). The filtering can be applied either inbound or outbound on an interface. There are 2 varieties available, standard and extended ACLs. The standard lists only allow filtering based on source address and are numbered in the range of 1 to 99. Extended ACLs allow filtering based on transport layer protocol, source and destination address, and application port numbers. The extended ACL range is 100-199.

By using extended access control lists to block all UDP broadcast packets other than to port 9, we can eliminate the echo request packets directed at port 7, and others such as the chargen port, used by Smurf and Fraggle. The isolation of broadcasts to port 9 reduces both the broadcast storm issue and the security concerns that produced the recommendation for turning off directed broadcasts.

The use of Dynamic Host Control Protocol (DHCP) to assign IP addresses dynamically may involve the broadcast of UDP requests traversing subnet boundaries. Limiting directed broadcasts to port 9 could effect use of DHCP servers. Cisco routers use a command 'ip helper-address' to forward the requests used in DHCP to a server or subnet outside the LAN. This forwarding can either be to a specific IP address or a subnet address. Packets forwarded to specific address will not be effected by the ACL filtering. If a subnet address is used, the forwarding will fail since it is directed to ports 67 and 68 for the server and client respectively. To alleviate this problem, only specific addresses should be used for DHCP servers. If additional servers are needed for redundancy, multiple ip helper-address commands can be used for an interface.

RECOMMENDATION

Based on the above discussion, the use of WOL technology from a network perspective appears to be an acceptable solution for use in software distribution. The network can be made reasonably secure and still allow the 'magic packets' to reach their destination. Another security enhancement involves turning off UDP small servers in all routers to eliminates the potential for both intentional or unintentional UDP Diagnostic port attacks aimed at the routers. One additional feature would be to limit the source of the udp port 9 packets to only the gateway address but this would complicate the configuration instructions for the routers and is not considered worth the additional complexity. It would also prohibit another gateway from assuming the tasks of the original without re-configuring the router.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To decrease the complexity of router configuration in a network as large as ours, one option considered was to apply the ACL list to all interfaces on the router. The processing of the ACL rules increases the load on the routers. The approach of identifying the router interfaces that require the directed broadcast to a remote subnet will decrease the impacts on the network. However, this approach raises the management complexity by requiring constant router reconfigurations as the ESM architecture evolves. Therefore, the recommendation is to turn on directed broadcast with an extended ACL for all ethernet interfaces and shut off directed broadcasts for all serial interfaces.

AREAS OF POTENTIAL PROBLEMS

If WOL is the selected alternative, the benefits will only be gained if the 'magic packets' are assured of reaching the intended targets. This trial project found that the Tivoli inventory was not always correct. The inventory for a particular device is based on reading the configuration information from a PC that has been configured for communication with a gateway server. If the subnet mask is incorrect, or if the mask does not match the router configurations, the packet may be sent to the wrong subnet. If the MAC address has changed, the WOL packet may be incorrectly formed to wake the device.

In some locations, the move from routed to switched networks involved expanding the size of some of the subnets. To allow time to re-configure all devices to the new subnet parameters, the routers may have secondary addressing to cover the old subnet specifications. In a switched network, the mismatches between device and router configurations may cause the WOL packet to fail to reach the intended device. An effort will need to be made to assure the PC and router information is consistent. The Tivoli inventory will also need to be amended if the MAC address is incorrect. One advantage to this proposal may be the increase in communication between the network and ESM administration groups. This is an area that has previously been lacking.

An additional area of concern is the effect of the ACL on router performance. The ACLs allow the router to function as a packet filtering firewall. However, the incorporation of ACLs produce additional overhead on the router CPU. The switching of packets is forced to the slower processor switching to allow analysis of each packet based on conditions set forth in the list. ACL processing proceeds in a top down manner. The packet is compared against the first line and proceeds through the list until a match is found. If no match is found, an implicit 'deny all' causes the packet to be dropped. Therefore, the impacts on the processor are directly proportional to the length of the list as well as the placement of the most common matches nearer the beginning of the list.

The Cisco Technical Assistance Center (TAC) was consulted on the impacts of a 2 line ACL to filter directed broadcasts (Cisco TAC Case #C585246 on 04/11/2002). The reply

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

indicated impacts should be minimal with this short of an ACL. The Cisco engineer felt the only concern would be on a router with CPU utilization greater than 50%.

The Cisco IOS 'show processor' command can be used to view the router CPU statistics. The CPU utilization is listed for a 5 second, 1 minute, and 5 minute average. Our routers generally average below 20% CPU utilization. To confirm the expected lack of CPU impact, several routers of varying sizes were monitored to determine the average utilization. The ACL list was added to the Ethernet interfaces and again monitored for CPU utilization. No increased processor load was observed. Normally directed broadcasts would be a small percentage of the protocol distribution. In the event of a denial of service attack using directed broadcasts, this percentage could be much higher. The 'show processor' command could be used to help identify an attack in progress if the utilization becomes much higher than normally expected.

STEPS REQUIRED FOR IMPLEMENTATION

To assure that the directed broadcasts from the gateway server can be routed to the end node, the following changes should be made to the router configurations:

Log on to the router in enable mode and enter the configuration mode:

```
configure terminal
```

Enter the following global commands on all routers:

```
no service udp-small-servers
no service tcp-small-servers
access-list 150 permit udp any any eq discard
access-list 150 deny   ip any any
```

On all ethernet and fast ethernet interfaces:

```
interface Ethernet x
ip directed-broadcast 150
```

On all serial interfaces

```
Interface serial y
no ip directed-broadcast
```

Note: the access control list must be in the extended range (100-199). If the router already uses access list 150, a change must be made. For consistency nationally, to facilitate troubleshooting, it is recommended that the directed-broadcast access list be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

150. ACLs have an implicit deny statement at the end of the list. The ip deny any any statement is added for clarity. For assistance in making the change, please contact your regional network representative or any member of the national network team.

CONCLUSION

Although implementation of software distribution using directed broadcasts with WOL technology has not been started enterprise-wide in the production network, it appears to be feasible to incorporate it in a secure manner. Preliminary tests in both a lab environment and in limited tests in the production network have shown that simple extended ACLs limit the potential threat of utilizing directed broadcasts to launch denial of service attacks. The recommended approach is designed to allow changes within the ESM architecture without requiring constant router re-configurations. While the initial workload of configuring the network routers with the recommended changes will be high, the long-term impacts will be small. The benefits of more reliable automated software updating are considered worth the effort.

REFERENCES

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

Huegen Craig A. "The Latest in Denial Of Service Attacks: 'SMURFING' Description and Information To Minimize Effects"
URL: http://www.pentics.net/denial-of-service/white-papers/smurf.cgi (29 March 2002)

Ferguson, P./Senie, D. "RFC 2267: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing"
URL: ftp://ftp.isi.edu/in-notes/rfc2267.txt (29 March 2002)

Cisco Systems. "Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks" Cisco White Papers
URL: http://www.american.com/warp/public/707/3.html (29 March 2002)

Advanced Micro Devices. "Magic Packet Technology' White Papers
URL: http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/20213.pdf (27 March 2002)

Cisco Systems. "Knowledge: Understanding DHCP"
URL: http://www.cisco.com/warp/public/779/smbiz/service/knowledge/tcpip/dhcp.htm (30 March 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Postel, J. “RFC 868: Discard Protocol” Internet RFC/STD/FYI/BCP Archives URL: http://www.faqs.org/rfcs/rfc863.html (28 March 2002)

Wnstrom, Micheal J. Managing Cisco Network Security. Indianapolis: Cisco Press, 2001 720-737

Stevens, W. Richard. TCP/IP Illustrated, Volume1. Reading: Addison Wesley Publishing, 1994 Various

© SANS Institute 2000 - 2002, Author retains full rights.