

SEIWG REPORT

IT1.75 Masking Shunt

TRIAL SUMMARY

Masking shunt (MS100SC) improves network security by preventing identification of network devices. Without masking shunt, network mechanisms operate "in the open," meaning the mechanism's Media Access Control (MAC) address can be detected and the device identified. Masking Shunt prevents a targeted fourth generation attack emanating from network intruders using sophisticated tools to discover device types and then take advantage of the specific weaknesses in the targeted device.

Masking shunt works by adding a layer of security at Data Link level of the Open Systems Interconnect (OSI) model. Masking Shunt protects the network infrastructure, including firewalls, local area networks (LANs) and critical nodes by making network devices invisible to external observation. While masking shunt prevents external devices from discovering critical internal information, it does not prevent local security devices from monitoring, managing, or manipulating incoming and outgoing data traffic. Masking Shunt improves command mission assurance, planning and execution for Homeland Defense and Civil Support by providing an additional level of security addressing information assurance, continuity of operations, anti-terrorism, force protection, and critical infrastructure protection.

Masking shunt is a reliable, plug and play, security appliance providing enhanced network security. It has few configurable switches and no operating system. Thus, once installed, support requirements are minimal. Masking Shunt has no user IDs, no passwords, no logs, no addressable ports, and no operating system to log into or inspect. Connecting masking shunt into a network requires the network to be taken off line briefly.

Masking shunt operated in the masking mode operation during CWID 2005, which camouflaged the MAC address of firewalls, network devices or information domains at the data link layer. Since masking shunt and the firewall could not be detected on the network, neither was open to a direct attack or access. Masking shunt automatically detected the MAC address of the devices on either side of masking shunt. After powering on masking shunt, the first packet in each direction was used by Masking Shunt to learn the MAC addresses of connected devices. Masking shunt also performed firewall checks, raising an alarm if traffic stopped flowing through the firewall.

To demonstrate how Masking Shunt operates, the trial placed two or three traffic-generating workstations in the demilitarized network zone (DMZ) behind the firewall. The workstations were automated to send random network traffic to demonstrate the packets leaving masking shunt contain neither the firewall MAC address nor the MAC address of the local area network (LAN)-based workstations, while the returning packets were correctly processed to the originating LAN workstations. Another workstation was set up to capture and collect inbound and outbound packets for analysis from both sides of the Cisco Pix firewall and Masking Shunt pair.

Three software products (LIBPCAP, TCPDUMP, and Ethereal Network Analyzer) were embedded in the Fedora Core 3 software suite and were required for the analyses of the packet data. LIBPCAP captures and stores the packets. TCPDUMP allowed reviewing the packets in human readable (ASCII) form. The Ethereal Network Analyzer enabled LIBPCAP and TCPDUMP in a user-friendly form. The data collected demonstrated the outgoing packets contained a variety of MAC addresses but none of them included packets containing the real Cisco firewall MAC address. CWID operators verified the masking shunt device was operating correctly by using the Ethernet frame viewer to check the modification of the MAC source address and to verify the firewall MAC address did not appear as part of the Ethernet frame source address.

SYSTEM ENGINEERING AND INTEGRATION

-- Dahlgren: Masking shunt configuration at Dahlgren consisted of three packet-generating workstations, a Windows 2000 workstation, a Linux Fedora 3 workstation, and a Solaris 8 workstation attached to a simple hub along with masking shunt. Masking shunt was attached between the simple hub and the gateway for the unclassified network at Dahlgren through another hub. A Cisco Pix 506e firewall, which would normally be placed between the protected network and the gateway, was attached to masking shunt. The three workstations emulated a DMZ network, and generated traffic by pinging the gateway. A fourth workstation with two Network Interface Cards (NICs) was attached to both hubs, in order to monitor traffic on both sides of masking shunt. The monitoring workstation existed purely for demonstration purposes, as masking shunt does not require monitoring in operational scenarios.

The monitoring workstation demonstrated the firewall was successfully obfuscated. The traffic generated by the three workstations in the DMZ was passed through masking shunt. When a packet entered the shunt, the source MAC address was copied to a buffer on the shunt. The packet was then passed to the firewall. Once the firewall acted on the packet, the packet was passed back to masking shunt. Masking shunt then replaced the source MAC address of the packet with the MAC address in buffer, decremented the hop count, incremented the Time To Live (TTL), recalculated the Cyclic Redundancy Check (CRC), and passed the packet out to the next device. The intended result was packets with false MAC addresses appearing as though each was not passed through the firewall. To an observer or potential hacker, the packets contained no firewall information at all, even though firewall protection remained intact.

Actual results indicated the packets generated from the three workstations in the DMZ had the correct pairing of IP and MAC addresses. The workstations were configured to ping the gateway 3 to 5 times per second, for a total of 13 pings per second. At 13 pings per second, one packet was able to enter and leave masking shunt before the next packet arrived. The MAC address buffer on masking shunt only holds the MAC address of the last packet to enter the shunt; therefore, the packet reclaimed the original MAC address. The firewall was indeed invisible to an outside observer, however the correct mapping of IP addresses and MAC addresses from the devices on the DMZ was available, allowing a potential hacker to determine what resources exist on the DMZ, and where the resources were logically located. Dahlgren network engineers would not allow more than 13 pings per second to ensure the gateway continued to function properly. Masking Shunt engineers indicated a minimum of 20 pings per second was necessary to trigger the swapping of MAC addresses.

More workstations and more traffic would result in a higher likelihood of a packet receiving a random MAC address upon leaving masking shunt. In an operational environment, devices on the DMZ would populate the MAC address buffer, and traffic generated by a protected network behind the firewall would claim a MAC address from the DMZ. The MAC addresses of the devices in the protected network are completely obfuscated along with the firewall. Obfuscated LANs behind the firewall were not demonstrated in CWID due limited space for computers at the participating sites.

-- SPAWAR: The operator entered the Media Access Control (MAC) addresses provided by Masking Shunt for the initiation of packet traffic through the MS100SC firewall. The monitoring workstation demonstrated the results of the packet traffic visually by using a monitor. To view Masking Shunt activity, a minimum of 10,000 packets were initially processed through masking shunt device, and the monitoring workstation demonstrated masking shunt successfully hid the MAC address of the protected firewall, essentially making the firewall invisible from detection. Masking shunt protected the firewall and other LAN devices from intruders, hackers, and attackers.

OBJECTIVES

List JWID Objectives the system supports	Describe, in outline form, the data products and processes the system used to satisfy these objectives	Objective met during JWID Execution?
Provide solutions to facilitate information sharing across multiple information domains.	Masking Shunt, MS100SC masked the MAC addresses of network devices to protect networks, information domains, communities of interest, or firewalls.	Yes

CAPABILITITES DEMONSTRATED

List the unique system capabilities that this system demonstrated to support the objectives which are being addressed:

1. Masked the MAC addresses to protect firewalls, network devices, and information domains.

SYSTEM CONFIGURATION REQUIREMENTS

COMPONENT NAME: Masking Shunt System Architecture						
HARWARE COMPONENT REQUIREMENTS:						
Nomenclature	Manufacturer	Model	Ports/NICs	Additional Requirements	Quantity Required	
Masking Shunt	Research: Security, Reliability, Communications (Re:SRC)	MS100-SC	4/HP HFBR58039939	None	1	
Network Dual Speed Hub	Netgear	DS104	4	None	2	
Media Converter	Edimax	ET-9003SCM	2	None	4	
HARDWARE REQUIREMENTS:						
Platform Make and Model	Operating System	Processor Speed	RAM	Disk Space	Data Standards & Version Number	Additional Requirements
Network Firewall: Cisco Pix 506E	Cisco Pix OS	Intel Celeron D 300 MHz	32 MB	8 MB Flash	(5) Cisco Controller	None
SITES: Canberra, Wellington, Lillehammer, SPAWAR, Dahlgren						

SYSTEM CONFIGURATION REQUIREMENTS

COMPONENT NAME: Traffic Generator						
HARWARE BUILD:						
Platform Make and Model	Operating System	Processor Speed	RAM	Disk Space	Ports/NICs	Additional Requirements
ASUS 4500L	Fedora Linux Core 3 / Windows 2000 SP2	Intel Celeron D 2.93 GHz	256 MB	40 GB	(2) Intel Pro/100	None
SOFTWARE REQUIREMENTS:						
Software Application & Version Number	Operating System	Processor Speed	RAM	Disk Space	Data Standards & Version Number	Additional Requirements
OpenSTA 1.4.2	Windows 2000 (or later)	Pentium P200 MHz	80 MB	80 MB	HTTP/S 1.0/1.1	None
Macromedia Flash Player 7	Windows 2000 (or later)	Pentium III	128 MB	500 KB	N/A	Microsoft Internet Explorer 5.x, Netscape 4.7, Netscape 7.x, Mozilla 1.x, CompuServe 7, AOL 8, and Opera 7.11
Fedora Linux Core 3	Fedora Linux Core 3	Pentium IV 200 MHz	64 MB	3.0 GB		LIBPCAP 0.8.3, TCPDUMP 3.8.3, ethereal 0.9.11
SITES: Canberra, Wellington, Lillehammer, SPAWAR, Dahlgren (3 per site)						

SYSTEM SPECIFICATIONS

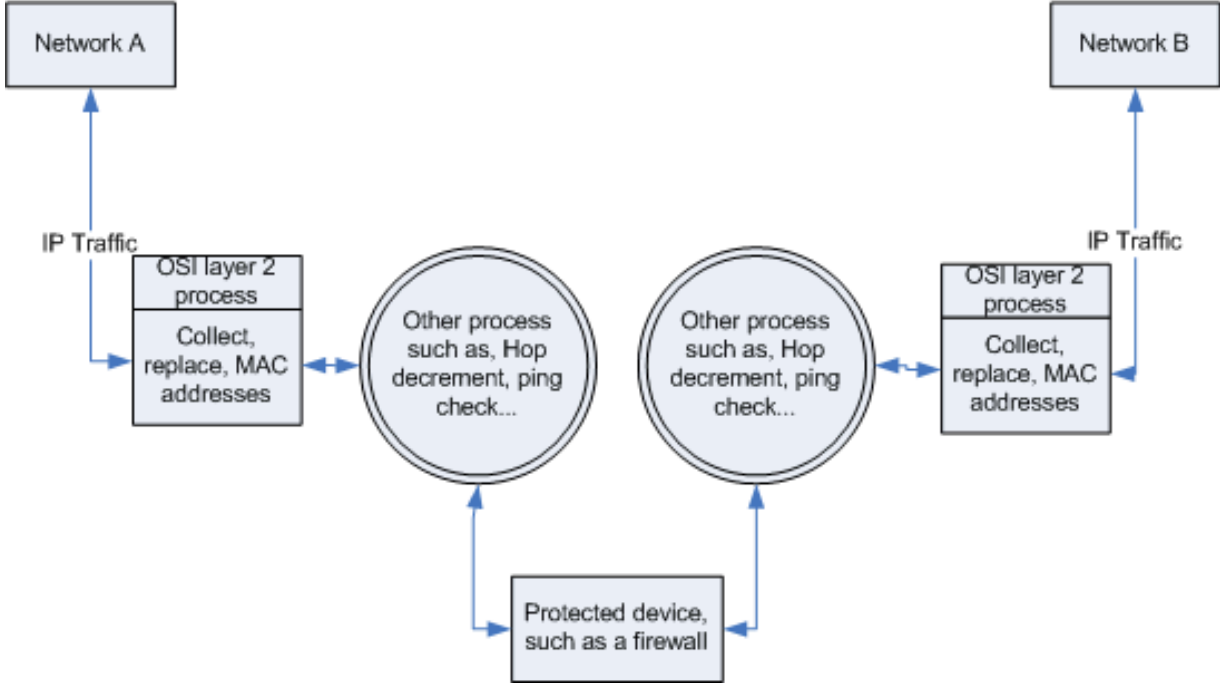
NOMENCLATURE: MC1000
General:
<ul style="list-style-type: none">• Dimensions: 481 x 180 x 44mm (WxDxH)• Weight: 2.4 Kg (Net Weight)• Temperature (Operating): 0° to +45°C• Temperature (Storage): 0° to +60°C• Humidity: 5-90% non-condensing• Power Supply voltage: 100 - 250VAC, 50-440Hz• Maximum current: 1A• Power consumption: 20 Watts
Standards:
<ul style="list-style-type: none">• Ethernet standard: IEEE 802.3u 100Base-FX full duplex.• Safety standard: Complies to relevant parts of UL 1950 3rd Edition and IEC 60950• EMI Standard: FCC Part 15 Class B
Interfaces:
<ul style="list-style-type: none">• Ethernet ports: Four 100Base-FX: SC multi-mode full duplex• Management ports: Two Out of Band Management (OOBM) ports use 4-pin RJ type connectors. (Polarity insensitive signaling using the two outer pins only.)• Fiber Optic: 1310nm multi-mode fibre

AVAILABLE SYSTEM DOCUMENTATION

SYSTEM DOCUMENTATION	
Standard Operating Procedures available for use during JWID Execution?	No
Operational Requirements Document (ORD) exists for this system?	No
Interface Design Specification (IDS) Document exists for this system?	No
Integrated Logistics Support Plan (ILSP) exists for this system?	No
Concept Of Operations exists for this system?	Yes

DATA FLOW DIAGRAM

Re:SRC MS100-SC Data Flow Diagram
(Masking mode)



CONCLUSIONS

Masking Shunt is implemented as a hardware solution and does not use an operating system; the internal functioning of the device cannot be compromised from the network. Once properly installed, Masking Shunt has virtually no adverse effect on tactics, techniques, or procedures, beyond ensuring Masking Shunt had the same physical security rendered to any important network device. By adding an additional layer of security to any network, Masking Shunt fulfills DoD security requirements and concerns. Masking Shunt is currently deployed at the DISA Continuity and Test Facility (DCTF) Slidell, LA to support network defense tactics, techniques and procedures as part of protective screening mechanisms at the perimeter for intrusion defense, and securing internal nodes and LANS against network mapping. By scrambling all outgoing packet MAC addresses Masking Shunt protected the firewall from discovery at the Data Link Layer and provided an extra level of security to help prevent unwanted discovery of local area network devices. Operating in the masking mode, it rendered firewalls and intrusion detection devices invisible from detection, thereby mitigating and defeating dangerous internal and external network attacks.

Masking Shunt has the capability to operate in a cascade mode which provides a redundancy switch over, to route traffic to an alternative network, while one of the device ports can be used for the transparent traffic monitoring. A Masking Shunt in full cascade mode can be used for networks with two or more firewalls in a redundant configuration. Two Masking Shunts mask the two firewalls. A third Masking Shunt is used to route traffic to a backup firewall if a failure exists to the primary firewall. Loss of power to one of masking shunt devices in mask mode generates alarms, causing the unit in cascade mode to switch to the redundant network. Due to the nature of the CWID architecture and security requirements, the cascade functionality could not be demonstrated.

Future developments for Masking Shunt indicate the current model Masking Shunt will be manufactured in much smaller sizes for easier portability and tactical deployment. It will include changes for IPv6 and will expand improvements at the protocol layer for packet protection to provide additional security of other network devices. Masking Shunt is available from Re:SRC LTD based in New Zealand or from the Re:SRC US office in Camden, New Jersey.

Masking Shunt obfuscates the MAC addresses of network devices, making the MAC address appear to be another device by randomly replacing and changing the MAC addresses of the protected devices. This forces potential intruders to run more extensive and specific testing protocols and processes to determine firewall MAC addresses, and in doing so, the intruder is more likely to be identified and countered. Masking shunt also protects the publicly viewable portions of LANs, such as web sites, viewed externally, while secure portions of the internal network stay protected from observation. Masking Shunt has the capability to provide information assurance benefits to all COCOMS and Services.

RECOMMENDATIONS

Effectively obscuring the MAC address to forestall network intruders from detecting and monitoring firewall activity, Masking Shunt demonstrated the ability to become a formidable security tool in combating network intruders. Any decision to purchase and deploy Masking Shunt should be based on a site security risk analysis, review of intruder threats, and a determination of the best means and tools for defending against attempted network intrusions. Masking Shunt was found to provide an invaluable service to network security personnel by effectively hiding the MAC source address of firewalls and the network behind the firewall. Its capability to make network devices invisible to intruders is invaluable in mitigating potential attacks to DoD, DHS, and coalition networks. In combination with other intrusion detection systems, Masking Shunt provides an additional level of network security. Recommend presenting the tool to services and COCOMs for procurement.

HIGHLIGHTS

- Provided an extra level of security to be used in conjunction with other intrusion detection systems to help prevent unwanted discovery of local area networks for the purpose of spying or hacking, providing the opportunity to expose network intrusion attempts.
- Effectively hid the MAC addresses of firewalls preventing the intrusion of the network and network devices.
- Obfuscated the MAC addresses of network devices, making the MAC address appear to be another device by randomly replacing and changing the MAC addresses of the protected devices.