

Making the Network a Moving Target

Cyber Security Is Overwhelmed

Government and financial networks are targeted by highly organized criminal elements and pseudo-government entities every day. Cyber security systems already make up a significant portion of the CIO's budget and these attacks result in additional financial loss. Existing cyber security solutions do not scale against the exponentially increasing number and sophistication of malware, probing and direct attacks. The U.S. President's 2009 Cyberspace Policy Review called for new approaches such as a "Moving Target" defense to make networks more resilient, eliminate whole categories of attack vectors, and give the defender more time to detect and respond to cyber attacks.

Call for Moving Target Defense

One "moving target" approach is to use operating system or application virtualization sessions that can be suspended and cleansed from cyber attacks. While this is a promising approach at the application layer, it does not protect devices which are inherently physical such as network firewalls, security management servers and industrial control systems. *Is there a moving target defense for inherently physical network devices?*

Cyber attacks against inherently physical devices take advantage of the static relationship between a device and its network protocol identities. Network equipment manufacturers consistently warn customers about network mapping based spying intrusions because cyber intruders have more exploit and detection avoidance options if they can obtain the network address of a critical device such as a firewall or virtual operating system host server.

Market trends may even be increasing the cyber risk exposure as application virtualization, borderless networks, and some network management trends serve to "flatten" the network protocol stack and increase risk factors for network mapping and other lower level cyber attacks.

A moving target approach that virtualizes network addressing could eliminate network mapping attack vectors. It could go even further by enabling a platform to host other security functions to actively deceive, lure or repel an attacker.

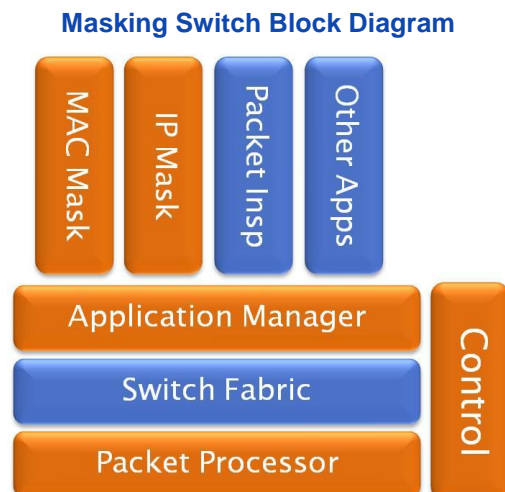
Current Solutions Stop Short

Network equipment suppliers like Cisco offer features such as port security and Layer 3 switching to partially address network mapping threats. However, physical networks remain static or slow to change and the attacker is free to gather intelligence over a long period of time and attack or exploit on their own terms. This is validated by "Red Hat" security auditors exploiting network identity vulnerabilities for penetration testing as well as firewall and switch manufacturers consistently warning customers because their products are prime targets of network mapping attempts.

How Network Masking Helps

Masking Networks makes the network itself a moving target by masking key identifying information in network packets. We do this while retaining full compatibility, wire speed, and a valid network management view.

Our "Masking Switch" dynamically masks the network addresses of all devices directly connected to its ports. In the following Masking Switch Block Diagram, the orange color indicates inherent network masking functionality and the blue color indicates complementary functions.



Wire speed performance is achieved by modifying specific portions of network packets in the Packet Processor module using digital signal processing techniques. The network masking function itself requires no MAC address and is completely



invisible to the cyber attacker. The Control and Application Manager modules provide the interfaces between the masking applications, the Packet Processor, and externally to other network masking switches and compatible network monitoring and security systems. The Switch Fabric module is swappable to support licensing of the network masking functionality to 3rd party network equipment providers.

Core network masking functionality includes a set of techniques for generating and regenerating proxy MAC addresses and modifying packet headers and data to mask the actual MAC address and network hops. TCP / IP masking and other application level functions are supported by loadable software modules, event logging, and inter-device management protocols.

Network masking provides more effective network segmentation and prevents traffic analysis. This impedes perimeter attacks, node hopping exploits and other attempts to spoof, block, or hijack a network device.

The Masking Switch forces the attacker to use more active techniques that can be easily identified by intrusion detection and network monitoring tools. Loadable software modules could also coordinate with other masking devices to present virtual network protocol stacks to mislead, detect, lure, or repel an unauthorized user, cyber intruder or malware and prevent them from gathering intelligence and exploiting the network.

Our approach is compatible with existing network security and management systems and will not impede network performance. This offers clear value as a network defense. And, teamed with other security devices, it also enhances attack detection and response.

Customer Validation

The first generation MS-100SC “Masking Shunt” won honors at CWID 2005 and was purchased and evaluated from 2006 – 2009 by the Department of Defense (JFCOM, SPAWAR and DISA). This proved the viability of network masking and also identified functional requirements for a fully commercialized Masking Switch. Our network masking approach is protected by United States Patent 7712130, issued May 4, 2010 as well as patents in other countries.

Competitive Approaches

Layer 3 Switching: Layer 3 switches limit the propagation of the MAC network address by IP switching at the hardware level and forwarding the other protocols at Layer 2, or acting in a hybrid Layer 2 / Layer 3 mode. This impedes network performance and does not fully eliminate Layer 2 propagation and risk.

Switch Port Security: Many switches have a “port security” mode where a port is configured to only allow connection by a pre-configured set of device MAC addresses. This imposes a significant network management burden with limited security gain.

Transparent Firewalls: Firewalls and IPS have operating modes in which they do not broadcast their MAC address. However, this mode necessarily limits their functionality.

Masking Networks’ approach provides a proactive and more effective moving target defense without increasing the network management burden, while maintaining full network performance and compatibility, and enabling a network masking platform to host new moving target functions.

About Masking Networks

Masking Networks adds a proactive dimension to cyber security by dynamically masking the network identity of firewalls, servers, industrial control systems, or any other attached devices. This is in line with the National Cyberspace Policy calling for breakthrough Moving Targets network security.

Our first generation network masking device demonstrated the feasibility of our approach and we are currently commercializing a programmable Masking Switch platform for government and commercial markets.

Company Information

Organization: Delaware C-Corp, HQ in Reston, VA

All products sourced and manufactured in the U.S.

DUNS: 793473716 **CAGE:** 4TGW2

SBA: Small Business

NAICS: 334210, 334220, 541511, 541512, 541712