ARP-Guard

3 M FUTURE

Professor Dr. Wolfram Reiners

info@3mfuture.com
Phone +49 7531 9166 00
www.3mfuture.com

ARP Spoofing Attacks Protection

Network Attacks

External attacks by hackers, viruses, worms and trojans are permanent threads to any progressive company. According to a study of Mummert Consulting in München/ Germany, at least 60 % of companies suffer from outside attacks against their IT Systems. The damages caused by these attacks become seldom public.
What is not widely known, though, is that the major portion of attacks comes from within the network. In 2002 KPMG reported that up to 80 % of all intrusions were initiated internally. Technical ignorance, curiosity and intentional manipulation of data often lead to serious damages for a company.

The Threat of Internally Initiated Attacks

Malicious software to run internal attacks can be downloaded on the Internet by everyone. By using such software, only standard network skills are needed to disturb, intercept, record or manipulate the entire communication of a single machine or a complete network segment, even if the data is transferred encrypted. Any employee can thus “look over the shoulder” of his colleague or supervisor. He can simply watch or – even worse – alter data that runs over the network. Of course one can also monitor passwords and even online banking PINs become vulnerable. Other areas of interest could be construction plans, accounting, and personal or financial information.
The usual security methods such as fire walling or virus protection cannot recognize these types of attacks. Not even sophisticated security solutions like intrusion detection systems can safely prevent abuse. Today, any skilled person can execute malicious attacks against an enterprise or organization, without the risk that his or her actions or identity will ever be revealed.

Technical Background

In 1982 the Address Resolution Protocol (ARP, RFC 826) was developed in order to establish a connection between the Internet address (IP address) and the hardware address (MAC address) within a network segment.
Using fake ARP messages (‘ARP spoofing’) an attacker can divert all communication between two machines with the result that all traffic is exchanged via his PC. By means of this so-called ARP poisoning, the attacker can

- Run Denial of Service (DoS) attacks
- Intercept data
- Collect passwords
- Manipulate and alter data.

These attacks are usually successful even with encrypted connections like SSL, SSH or PPTP.

Background on our Services

Our traditional strategy is to recognize and understand present security threats, but to take action only in the event of an actual attack. With this strategy we have been building comprehensive security into IP networks, by ensuring that the regular communication of all assigned applications remains undisturbed and work without interruption.

ARP-Guard

ARP-Guard is a system that forms an active protection shield against ARP-attacks. The ARP-Guard early warning system constantly analyzes all ARP messages, sends out appropriate alerts in real-time and identifies the source of the attack. ARP-Guard easily integrates with existing IT security environments, such as firewalls, virus scanners, or intrusion detection systems.
The ARP-Guard system consists of several sensors, which detect ARP spoofing attacks and report them to the management system for evaluation and further processing. If an attack is identified, the management system automatically informs the registered security representatives or network administrators.

LAN-Sensors and SNMP-Sensors

ARP-Guard LAN-Sensors analyze ARP messages in individual network segments. The ARP-Guard sensors are connected to the mirror port - the SPAN port - of each monitored LAN switch. ARP-Guard LAN-Sensors can be installed on dedicated PCs or workstations or on machines that serve other projects. Each ARP-Guard LAN-Sensor controls up to 8 LAN switches. For large-scale networks ARP-Guard LAN-Sensors can be set up in a cascading architecture.
In larger scale networks a full-coverage monitoring with LAN-Sensors would require a significant number of sensors to be deployed. To keep the system feasible, we also offer a solution that allows the use of already existing devices like SNMP capable routers as sensors (Simple Network Management Protocol). One SNMP-Sensor can control the ARP tables of up to several hundred routers and all relevant modifications are reported by the management system.

The Management System

All ARP-Guard sensors are connected to the ARP-Guard management system using encrypted IP connections. All messages are transmitted independent of the network they are based on. The ARP-Guard management system analyzes all incoming messages. In the event of an attack the organization's safety representatives are automatically informed by email or SMS and receive unambiguous information about the attacking machine.
As an additional security feature, all alterations of ARP tables are logged. Authorized personnel can inspect the log at any time. A web front-end allows remote access. The ARP-Guard system itself is protected against ARP poisoning attacks. Sensors and management system control each other mutually and inform the registered administrators whenever communication outages occur.

One Product - Two Service Models

It is our Customer’s choice, whether the ARP-Guard security system should be operated completely within its own network (license model) or whether we should operate the system as an Application Service Provider for our Customer (ASP). In the latter case, monitoring is entirely our responsibility and does therefore not bind any of our Customer’s internal resources.

Further Information

http://www.3mfuture.com/arp

info@3mfuture.com