NEC's World's First Security Configuration Analyzing System Enables Automatic Detection of Network Security Problems

May 16 2005

NEC Corporation today announced that it has succeeded in the development of a security configuration analyzing system that enables automatic detection of security problems through collection and analysis of configuration parameters of security tools that work collaboratively within the network. The newly developed system can detect security issues such as when the file transfer protocol ("FTP") service is accepted by the firewall, but the FTP data stream is not monitored by any intrusion detection system ("IDS") and is thus vulnerable to infection via worm attack, and can propose configuration revision plans to correct the problem at the time of error detection.

This is the world's first system to achieve automatic detection of security problems arising from configuration mismatching among different security appliances and software tools that work in collaboration. Without this system every network administrator would have to carry out this task manually based on individual skills and experience. An automatic detection system drastically reduces the network security checking time and load in comparison to manual methods. It is based on the following two technologies:

(1) A security policy extraction technology that translates configuration parameters of different security tools into basic policy rules boasting a common format.
(2) A configuration analysis technology that compares policies by the

data flows within the network to detect policy mismatches (i.e. security problems) such as the detection of a stream that is accepted, but is not monitored.

The technological characteristics of the system are as follows.

1. Use of a common configuration policy description language

In order to describe the filtering policies of a firewall by specifying what kind of packet streams it can accept, as well as the monitoring policies of IDS by specifying what kind of attacks on what kind of packet streams require monitoring, the system collects configuration parameters and translates them into an NEC original common policy description language called security configuration coordination markup language ("SCCML.") SCCML is designed to be platform independent and to describe basic security functions such as filtering and monitoring. It enables the administrator to easily grasp the current security status of the whole network by reviewing the SCCML policies, without having to consult every individual application and software tool in the network.

2. Virtual firewall simulation

As a firewall operates with many filtering rules (sometimes there are even more than 1000,) it is difficult to perform a comprehensive test to find out exactly what kind of packet streams it accepts in practice. The new system provides an integration algorithm of SCCML-based filtering rules to monitor if there is any overlapping of relationships or if any specified packet streams are accepted or rejected by the rule set. This function is called the "virtual firewall simulator." This simulator enables the administrator to carry out a comprehensive test in just minutes.

3. Automatic mismatch detection between a filtering policy and a monitoring policy

The system offers a mismatch detection algorithm by comparing the filtering and monitoring policies related to the same packet stream such as hypertext transfer protocol ("HTTP") or FTP service. This algorithm enables administrators to automatically detect security problems, for example it may notify the administrator that "This FTP service is accepted but not monitored." To date, no efficient method has existed to compare configurations or to detect such vulnerabilities. An experiment has shown that NEC's newly developed system completed a firewall-IDS configuration comparison task within 3 minutes, while an administrator took 170 hours to carry out the same task. This achieves a time reduction ratio of 1 over 3400.

4. Identification of configuration problems

Using the mismatched SCCML description, the system strictly identifies problematic configuration parameters and offers configuration revision candidates to the administrator. The administrator can select the candidate and revise the original configuration parameters immediately after the detection of the mismatch.

In recent years, a variety of applications and software tools have been introduced in the internet and intranet to protect resources from multiple kinds of security threats. However, this also means that only limited security experts can handle them, and their maintenance has become a heavy load for enterprises. As the internet and intranet become more dynamic and prevalent, service collaboration and enterprise organizations are becoming continually subject to change. In such environments, security configuration mismatches can easily occur, and warrant a serious problem if the mismatch is not detected and the corresponding vulnerability removed immediately.

NEC believes its new security configuration analyzing system can contribute to solving these kinds of security problems, and in turn drastically reduce security management costs while simultaneously improving the reliability of internet services and enterprises as they change dynamically.

Citation: NEC's World's First Security Configuration Analyzing System Enables Automatic Detection of Network Security Problems (2005, May 16) retrieved 27 April 2024 from https://phys.org/news/2005-05-nec-world-configuration-enables-automatic.html