Real-time Optimization of Access Control Lists

Sándor Palugyai and Máté J. Csorba

Nowadays the Internet usage is progressing at a great pace. More and more people become potential users and require faster connections. Recently security has also become an important issue in business networks and at home too. Because of these facts devices have to be designed and created, which allow us to build and maintain a more secure network and their operation also has to be optimized. In this work a method is proposed for the optimization of Access Control Lists used in routers, which maintain the operation of sometimes-huge networks.

Several network devices are used nowadays in access networks, like routers. These devices control the traffic, which crosses them with the so-called Access Control Lists (ACLs). ACLs can be assigned to the input or output of one or more interfaces. Of course, the input and output lists can be applied on the incoming or outgoing packets of the router respectively. The ACLs are examined sequentially in a router, because of their nature. So the router has to check every list-entry for each packet until it finds an entry, which matches the packet. After the first match the search is stopped. In the list-entries the administrator can allow or prohibit particular hosts or networks. If an entry is at the end of a list, which can be very long in certain cases, our packet will suffer noticeable delays and if the router does not find any match, the packet will be rejected.

In our work two kind of ACLs were analyzed, the Standard and the Extended Access Lists. During filtering Standard ACLs examine only the source address of a packet, Extended Access Lists on the other hand allow us to filter by other parameters as well, like the destination address, port address, protocol id and many other attributes of the packet. With these kinds of lists packet filtering can be refined as needed. The aim of this work is to optimize the input and output lists on all interfaces of the router on-line.

At first a test suite was created to measure basic performance attributes of a router, which uses different kinds of Access Control Lists. The tests are implemented in TTCN-3 (Testing and Test Control Notation version 3) language, which can be used very efficiently for packet-based measurements and tests.

The program developed by us examines cyclically the existing lists and optimizes them (if it is necessary) according to the actual network traffic, then it waits for and adjustable time. If there is no change in the number of hits of the examined lists the frequency of the periodical examination can be set automatically to a longer time.

The optimization algorithm is implemented in TTCN-3 and Perl languages. The developed software considers guidelines, such as how can be the position of a permit-, and a deny rule changed in the list in case the network segment covered by them has common parts. Besides it also uses algorithms to reduce the redundancy in the ACLs if possible. The cyclical examination of the input/output lists is organized in a way that in case the administrator alters an element in the ACLs the software can automatically adopt the changes and use the new lists.

The implementation generates bursty network traffic during the examination and list-modification period, which produces some negligible delay. Nevertheless it is worth mentioning that the optimization could actually work much faster implemented in a router.

References

[1] Cisco. `http://www.cisco.com/`

[2] Gilbert Held: Working with Cisco Access Lists [International Journal of Network Management 9, 151-154 (1999)]

[3] Scott Hazelhurst: Algorithms for Analysing Firewall and Router Access Lists [Workshop on Dependable IP Systems and Platforms, In Proc. ICDSN, June 2000]

[4] Scott Hazelhurst: A proposal for Dynamic Access Lists for TCP/IP Packet Filtering [Sortened Version In Proc. of SAICSIT 2001]

[5] ETSI: Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; TTCN-3: Core Language [ETSI ES 201 873-1]

[6] Szabó, J.Z.: User Documentation for the TTCN-3 Test Executor Prototype [Ericsson Internal Document]