Session State Transition Based Large Network IDS

Zhang Qianli
zhang@compass.net.edu.cn
Li Xing
xing@ocean.net.edu.cn

CERNET CENTER, Mainbuilding 224
Tsinghua University
Beijing 100084
China
ccert@ccert.edu.cn

Abstract

In order to present large-scale malicious attacks on an ISP network to maintain network services, we have designed a method to record key packets classified by sessions.

Session is the service provided above the IP layer. We define a TCP connection a session, a UDP packet exchange a session, or echo and echo response of ICMP to be a session. The research of network attack/intrusion/information collection has shown that most of the illegal action performed would have something special ongoing in such sessions. For example, winnuke will send OOB packets to the 139 port of a host; most of the platform detection will use strange packets too. Not only the strange packets itself, but the sequence of such packets going through the network indicate the attack. For example, teardrop will transmit packets that have abnormal fragment offset in the second packet, then cause some platform to crash. Some patterns of sessions will be created by flood based attack/information collection. For example, the SYN flood will create a pile SYN-SYN ACK-RST packets in the network, and most of scan tools will create several kind of patterns in the network, all of these patterns indicate the failure of the connection, these include SYN-SYN ACK-RST and SYN-RST and SYN-ICMP Unreachable message.

Based on this thought, we have designed the session-state transition analysis. We will define some packets as the indication of the session state. The happening of such packets causes the change of the session state. When comparing with the predefined rules, we will detect most of the DOS attacks. Another approach is to store these session states transition patterns into a database; thus we can calculate the happening rates of some specific patterns. Compared with the average level, abnormal high happening rates often indicate the possible attack or information collection. For example, we can collect a site's all

sessions' SYN-SYN ACK-RST pattern to decide whether a normal scan had happened.

The implementation includes four parts. The first is the data collection part, which collects and unwraps packets passing through the network; the second part is the signature matching part, which will match the packet signature, to filter only the specified packets; the third part will cluster such packets into sessions, and store the session specific signature chain and check whether a rule based match is satisfied; the fourth part will flush the session data into a database, and check whether a statistical based anomaly has happened.

Using such kind of techniques has several basic advantages. The first is not to violate privacy, since we are interested in only packet header to know whether a state has changed, to inspect header only also make this implementation efficient and fit for a large scale network. The other advantage is to avoid the headache to set the threshold of a statistical approach. Most scan detection tools (For example, gabriel) will calculate the burst of connections. New scan technique has appeared to avoid burst of connections, for example, slow scan and stealthy scan. Set a proper threshold is much more difficult for a large-scale network. For rule based analysis, since we use the state transition to detect intrusion, we could predict the happening of some attacks in a premature stage.

The future approach includes the content analysis based IDS, especially the remote buffer overflow detection. This part of research is underway.

References

(DED) Dorothy E. Denning, *An Intrusion-Detection Model*, IEEE Transactions on Software Engineering, Vol. SE-13, NO. 2 (Feb 1987) pp. 222-232.

(KI) Koral Ilgun, Richard A. Kemmerer, and Phillip A. Porras, *State Transition Analysis: A Rule-Based Intrusion Detection Approach*, IEEE Transactions on Software Engineering, Vol. 21, NO. 3 (March 1995) pp 181-199.

(LS) Lee Sutterfield, *Large-scale Network Intrusion Detection*, Computer Security, Vol. XIII, No. 2 (1997) pp41-48

(CS) Christoph Schuba and Gene Spafford, scan-detector program and doc

(F) Fyodor fyodor@dhp.com, Nmap doc and manual page

(H) Hyperion hyperion@hacklab.com, Watcher, Phrack53-11

(SD) Solar designer solar@false.com, *Designing and Attacking Port Scan Detection Tools*, phrack53-13

(CHR) Craig H. Rowland, portsentry doc and program

(SC) Information Sciences Institute of University of Southern California, RFC 793

(LJ) Laurent Joncheray, *A Simple Active Attack against TCP*
(MAM) Mark A. Miller, *Troubleshooting TCP/IP*
(ISS) ISS Corp, *Network-vs.Host-based Intrusion Detection*

Author S. List

Xing Li:

Xing Li received his B. S. degree in radio electronics from Tsinghua University, Beijing in 1982, and his M. S. and Ph. D. degrees in electrical engineering from Drexel University, USA in 1985 and 1989, respectively.

He is currently a Professor in the Electronic Engineering Department at Tsinghua University, Beijing, China. His research activities and interests include statistical signal processing, multimedia communication and compute networks. He has published one book and more than 70 papers in his research areas.

He is a member of Communication Expert Committee of the China National '863' High Technology Project and a member of Technical Board of the China Education and Research Network (CERNET) Project. He is a fellow of China Communication Institute, a senior member of China Electronic Institute, a member of ISOC, members of IEEE Signal Processing Society and IEEE Computer Society. He is a member of Sigma Xi. He is vice chair of APNG and a member of executive council of APNIC.

Qianli Zhang:

Qianli Zhang received his B. S. degree in signal processing from Tsinghua University, Beijing in 1997, now a second-year graduate student in CERNET Center. His research activities and interests include large-scale network IDS, operating platform security, TCP/IP protocol security analysis.