An Improved Semi-Global Alignment Algorithm for Masquerade Detection

Adesina Simon Sodiya, Olusegun Folorunso, Saidat Adebukola Onashoga, and Omoniyi Paul Ogunderu
(Corresponding author: Adesina Simon Sodiya)

Department of Computer Science, University of Agriculture, P. M. B. 2240, Abeokuta
(Email: sinaronke@yahoo.co.uk, {folorunsolusegun, bookyy2k, omoniyiogunderu}@yahoo.com)

(Received Dec. 14, 2009; revised and accepted Apr. 7, 2010)

Abstract

Masquerading is a security attack in which an intruder assumes the identity of a legitimate user. Semi-global alignment algorithm has been the best of known dynamic sequence alignment algorithm for detecting masqueraders. Though, the algorithm proves better than any other pair-wise sequence alignment algorithms such as local and global alignment algorithms, however, the problem of false positive and false negative have not been reduced to the barest minimum. Many previous works on masquerade detection using sequence alignment have difficulty at choosing the scoring system on which the algorithms base their optimal scores on. Hence, they resolved to assuming (or picking) a set of scores which they referred to as a unique scoring function for their experiment. In this work, an improved semi-global alignment called Cross-semiglobal algorithm, is designed to improve the efficiency of masquerade detection. In the previous pair-wise algorithms, a fix value is always assumed as the gaps score. In Cross-semiglobal algorithm, the scoring function on which the algorithms based their scores is constructed from legitimate users' sequence of commands. This principle was implemented using platform independent C/C++ framework. The designed was tested using a systematically generated ASCII coded sequence audit data from Windows and UNIX operating systems as simulations for standard non-intrusive and intrusion data. The result shows a reduction in false positive rate from 7.7% using semi-global alignment to 5.4% using cross-semiglobal. The detection efficiency was also improved by 7.7%.

Keywords: Cross-semiglobal algorithm, gaps scores, masquerading, sequence alignment, semi-global algorithm

occur when an intruder obtains a legitimate user's password or when a user leaves their workstation unattended without any sort of locking mechanism in place. It is difficult to detect this type of security breach at its initiation because the attacker appears to be a normal user with valid authority and privileges. This difficulty underlines the importance of equipping computer systems with the ability to distinguish masquerading attacker actions from legitimate user activities [6].

Forecasting the unknown and detecting the known threats and targeted attacks are the most concern of network security especially in large scale environment [1]. The information security industry has been very active in recent years. In order to counterwork security threats to computer systems and networks, many technologies have been developed and applied in security operations such as Intrusion Detection System (IDS), firewalls, routers. All those security application devices, whether aimed at prevention or detection of attacks, usually generate huge volumes of security audit data [37]. The traditional form of IDS and prevention systems are either signature-based or anomaly-based. Both require updates to maintain their signature database or they must have a period of time to develop a behavioral baseline to identify accurately "suspicious" or anomalous activities [1, 16].

The detection of a masquerader relies on a user signature, a sequence of commands collected from a legitimate user. This signature is compared to the current user's session. The underlying assumption is that the user signature captures detectable patterns in a user's sequence of commands. A sequence of commands produced by the legitimate user should match well with patterns in the user's signature, whereas a sequence of commands entered by a masquerader should match poorly with the user's signa-