Chapter 5
Intrusion Detection Using Machine Learning: Past and Present

Mohammed M. Mazid
CQUniversity, Australia

A B M Shawkat Ali
CQUniversity, Australia

Kevin S. Tickle
CQUniversity, Australia

ABSTRACT

Intrusion detection has received enormous attention from the beginning of computer network technology. It is the task of detecting attacks against a network and its resources. To detect and counteract any unauthorized activity, it is desirable for network and system administrators to monitor the activities in their network. Over the last few years a number of intrusion detection systems have been developed and are in use for commercial and academic institutes. But still there have some challenges to be solved. This chapter will provide the review, demonstration and future direction on intrusion detection. The authors’ emphasis on Intrusion Detection is various kinds of rule based techniques. The research aims are also to summarize the effectiveness and limitation of intrusion detection technologies in the medical diagnosis, control and model identification in engineering, decision making in marketing and finance, web and text mining, and some other research areas.

INTRODUCTION

Intrusion is a frequently used word in various sectors. As this is relating to unwanted events, users from every field have their great concern on this topic. Researchers are trying their best to define this term more elaborately and precisely. In terms of general security, intrusion is an attack that attempt from outsiders of a periphery. Intrusion in medical expression is defined as ‘a tooth is forced upward into the
In geology, an intrusion is a body of igneous rock that formed by molten magma. It cools beneath the Earth’s crust.

In terms of computer security, intrusion is a system compromise or breach of security incident regarding computer. This involves gaining control of a computer system from the owner or an authorized administrator. This can be done by an “insider” who has permission to use the computer with normal user privileges. It can be by an “outsider” from another network or perhaps even in another country. They exploit vulnerabilities in an unprotected network service on the computer to gain unauthorized entry and control.

There are various kinds of intrusions. Some of the examples are as follows:

- Virus, worm, or “Trojan horse” – these are sort of programming code created for harmful purpose. Generally these spread out through internet by downloading files, copy files from one computer to another computer, using pirated software, email, etc.
- Stealing password: Password stealing is one of the notorious types of intrusions at the present time. Hackers steal password of bank account, email account, confidential database, etc. over the internet. Different types of tools and ways are used to steal password such as – sniffer or “shoulder surfing” (watching over someone’s shoulder while they type their password), brute-force guessing, password cracking software, trial and error method, etc.
- Gaining illegal access: Hacker gains illegal access of terminal or steals information while users transferring file using less secured data transferring method such as old-style telnet, ftp, IMAP or POP email, etc.
- An exploitable vulnerability in a network services like FTP, Apache or Microsoft IIS, SSH, a name server, etc.
- Physically accessing a computer and rebooting it to an unsecured administrative mode or taking advantage of other weaknesses that come from a vendor who assumes that anyone using the keyboard and mouse directly is “trusted”

Another example of intrusion is “root kits”. “Root kits” gain elevated privileges on a computer. It is often installed by different types of “Trojan horse” programs. It hides the intruder’s presence on the system. A Trojan horse is a program that acts like a real program a user may wish to run, but also performs unauthorized actions. These Trojan horse programs will make it look like nothing at all is wrong with systems, even though it may have gigabytes of pirated software installed on it, may be flooding the network and disrupting service for everyone on local area network.

Another common post-intrusion action is to install a sniffer or password logger, perhaps by replacing the operating system’s own SSH (Secure SHell) or FTP (File Transfer Protocol) server. This exploits trust relationships that often exist with other local or university computers (e.g., the Homer or Dante clusters), other institutions and government agencies that may have a research relationship with, or even to/from people’s home computers on cable modem or DSL (Digital Subscriber Line) lines. Any one may not think about the act of logging in from one computer to another as a trust relationship, but these are indeed relationships between computers that involve a level of trust (namely secret passwords, which are the first line of defence). Intruders prey on these trust relationships to extend their reach into computer networks.

Determining whether or not an intrusion has taken place is sometimes a very difficult task. Root kits and Trojan horses make the job even more difficult and work so well because they take advantage of a
Related Content

A Hybrid Method for High-Utility Itemsets Mining in Large High-Dimensional Data
[www.igi-global.com/article/hybrid-method-high-utility-itemsets/1823?camid=4v1a](www.igi-global.com/article/hybrid-method-high-utility-itemsets/1823?camid=4v1a)

Navigation Rules for Exploring Large Multidimensional Data Cubes
[www.igi-global.com/article/navigation-rules-exploring-large-multidimensional/1773?camid=4v1a](www.igi-global.com/article/navigation-rules-exploring-large-multidimensional/1773?camid=4v1a)

Machine Learning in Studying the Organism’s Functional State of Clinically Healthy Individuals Depending on Their Immune Reactivity
Tatiana V. Sambukova (2013). *Diagnostic Test Approaches to Machine Learning and Commonsense Reasoning Systems* (pp. 221-248).
[www.igi-global.com/chapter/machine-learning-studying-organism-functional/69411?camid=4v1a](www.igi-global.com/chapter/machine-learning-studying-organism-functional/69411?camid=4v1a)

An Immune Systems Approach for Classifying Mobile Phone Usage
[www.igi-global.com/article/immune-systems-approach-classifying-mobile/1784?camid=4v1a](www.igi-global.com/article/immune-systems-approach-classifying-mobile/1784?camid=4v1a)