OTOLOGY BASED INTRUSION ALERT CORRELATION SYSTEM

By

ODUTAYOAYOOLUWA TOMILOLA

MATRIC NO: 08/1329

SUBMITTED TO

THE DEPARTMENT OF COMPUTER SCIENCE,
COLLEGE OF NATURAL SCIENCES, UNIVERSITY OF AGRICULTURE, ABEOKUTA.

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF

BACHELOR OF SCIENCE DEGREE IN COMPUTER SCIENCE.

JULY, 2012.
Alert Correlation techniques effectively improve the quality of alerts reported by Intrusion Detection System (IDS) and are sufficient to support rapid Identification of ongoing attack or predict an intruder, next likely goals. This project focuses on developing an intrusion alert correlation system using ontology. The architecture consists of IDS, Alert pre-processor and Ontology-based alert correlation system. The IDS collect security relevant information and the Alert pre-processor process the information. Ontology alert correlator has three sub-modules: Attack to Ontology, Reasoner and Output. The Attack to Ontology converts the attack information in the Database to attack individuals in the ontology. The Reasoner is used to infer attack process. An attack process is a series of attack steps which correspond to the attack individuals. The Output converts attack process from ontology to database for the Liseoffollow-up, such as risk assessment.