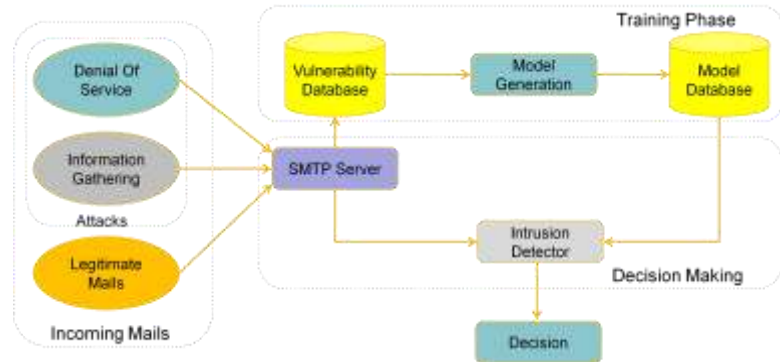


Autonomic Mail Protection System

by Mohamed Tabris

Mail systems are prone to malicious attacks which may degrade their performance or cause them to shut down; a number of techniques are used in order to prevent the intrusion. The protocols generally used in mail systems are SMTP, POP3 and IMAP. SMTP (RFC821) protocol by itself does not have any authentication commands and hence it is most vulnerable. These protocols may be used together in order to reduce the vulnerabilities for example POP3 is used along with SMTP in order to secure login in mail systems. Some of the common attacks on Mail Systems are Denial of Service (DOS). Denial-of-service attacks based on SMTP are aimed at flooding a network or computer with large email messages to prevent normal use and to cause a delay in mail delivery or even sometimes shutdown the server. In most cases a computer is affected because it cannot handle large messages e.g. > 1 Megabyte, or cannot handle the load created by receiving large numbers of messages at the same time, or running out of storage space.



Our goal is to develop an innovative anomaly based protection system for mail systems based on autonomic computing. The protection system will maintain confidentiality and provide reliable mail transfer against any type of attacks. We will also provide automated actions to respond promptly to mail attacks and exploitations. Our approach can be summarized in the following steps:

- Identifying SMTP server Vulnerabilities
- Launching Various Attacks on the server
- Collecting Data about the attacks launched and server behavior
- Generating Models based on Collected Data
- Designing an Anomaly Based Detector based on these Models

Training Phase

- In this phase we implement various kinds of attacks on the system and send out normal mail and try to find out vulnerabilities in the server.
- Identifying the features which help detect these attacks and designing Models for these features.
- These Models help define the region of normal and abnormal region.

Decision Making Module

- The Models are designed in order to detect an attack on the server.
- On detecting an attack the Models generate alerts.
- The final decision is taken by Autonomic Decision Making Module which assigns weights to every Model based on some statistics and input data during run time.
- Corrective measure is to be taken in order to prevent those attacks

Present & Future Work

- Creating a Database of Attacks and normal emails.
- Use the information from the database in order to identify the features which differentiate an abnormal behavior with a normal one.
- Designing Feature Models and Decision Making Module.