Anomaly detection for Computer Security

• Traditionally, Intrusion Detection Systems (IDS) are based on a database of signatures that describe known attacks.

  Problem: never-seen-before attacks can not be detected!!!

• Anomaly based IDS use a statistical model of the legitimate patterns. Any pattern whose statistical model deviates from that stored in the system is labeled as an attacks.

  Advantage: zero-days attacks can be detected!!!

HTTP Payload analysis

• The analysis of the bytes’ distribution in the HTTP payload of requests toward a web server allows to detect attacks against the web server

• Several solutions based on this approach (e.g. PAYL\(^1\), McPAD\(^2\)) have been proposed but they suffer of limitations due to:

  • Too high size of the features space
  • Coarse representation of the payload

HMMPayl: an application of HMM to the analysis of the HTTP payload

Davide Ariu - Giorgio Giacinto
davide.ariu@diee.unica.it
giacinto@diee.unica.it

HMMPayl: a simplified scheme

HMMPayl: an application of HMM to the analysis of the HTTP payload
Experimental Results and Conclusions

1 - Increased Classification Accuracy

2 – Benefits of the MCS approach

3 – Possibility of reducing the computational cost

HMMPayl: an application of HMM to the analysis of the HTTP payload

This research was sponsored by the Autonomous Region of Sardinia through a grant financed with the "Sardinia PO FSE 2007-2013" funds and provided according to the L.R. 7/2007.