CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

Getting Deeper into the Application of Markov Chains to Web Intrusion Detection

Carmen Torrano-Gimenez[1]

Web applications are target of numerous and sophisticated attacks, what makes vital to count with appropriate protecting systems. Web Application Firewalls (WAF) analyze HTTP traffic searching for intrusions in the aim of protecting web applications. This presentation shows how Markov chains can be applied to detect anomalies in the HTTP traffic. For that, this mathematical model is used as part of the detection engine of the WAF. The approach of the WAF is anomaly-based, i.e., the normal behavior of the web application is defined and actions that deviate from it are considered anomalous. The normal behavior is described by using two detection models: a length model and a structure model. The last one is in charge of modeling how the characters of the HTTP request are distributed, and here is, precisely, where Markov chains are applied.

The proposed models are experimentally evaluated. Since existing datasets present certain disadvantages, our own dataset (called CSIC) is used for this task. The evaluation is done in terms of the detection results, processing time and number of training requests used.

[1]Departamento de Tratamiento de la Información y Criptografía
Consejo Superior de Investigaciones Científicas
Serrano,144. Madrid, Spain
carmen.torrano@iec.csic.es