# On using wavelets for detecting attacks to web-based applications

**Cristian Cappo**
Polytechnic Department- National University of Asuncion
Campus UNA, San Lorenzo, Paraguay
E-mail: ccappo@pol.una.py

**Raul Ceretta Nunes**
Electronic and Computer Science Department, Federal University of Santa Maria,
Technologic Center, Campus UFSM, Santa Maria, RS, Brazil
E-mail: ceretta@inf.ufsm.br

**Christian Schaerer**
Polytechnic Department- National University of Asuncion
Campus UNA, San Lorenzo, Paraguay
E-mail: cschaer@pol.una.py

## ABSTRACT

Detection attacks to web-based applications have recently received considerable attention [2, 3, 4, 6, 8], specially intrusion detection systems (IDSs) for use with HTTP. This is mainly due to the increasingly role that these applications are playing in our society, as well as, the lack of adequate techniques for debugging their possible vulnerabilities. Attacks try to exploit vulnerabilities and thus violate the security of the system.

Typically, models for detecting attacks are based in observing any substantial variation of some specific attributes with respect to a pattern behavior, which it is normally determined through a learning technique [4]. When a web-based IDS is running, whenever a new query is received, it will be compared automatically with the learned patterns. If it is detected any abnormal behavior, an alarm is activated. The challenge is to minimize the number of false alarms ensuring high detection accuracy.

Following a tendency in the literature, we have base our study in analyzing two attributes of the HTTP queries: the length and the distribution of characters. It has been shown that these attributes are the most relevant when an attack occur [2, 3, 5, 7, 8]. The proposed analysis consists in using signal processing techniques to detect any abnormal distribution in the attributes. More specifically, we use wavelet functions for detecting anomalous queries [1, 6]. For performance tests, we integrated the anomaly detector with the web server of the university. The work is in initial state; however, preliminary results are encouraging.

**Keywords***: HTTP, Anomaly Intrusion Detection, Wavelet*

### References

[1] C. Huang, S. Thareja and Y. Shin. Wavelet-based real time detection of Network Traffic Anomalies. International Journal of Network Security, Vol.6, No.3, PP.309–320, May 2008.

[2] K. Ingham and H. Inoue. Comparing anomaly detection techniques for http. In Recent Advances in Intrusion Detection (RAID), p. 42 – 62, 2007

[3] M. Kiani, A. Clark and G. Mohay. Length based modelling of HTTP traffic for detecting SQL Injection Attacks. RNSA Security Technology Conference. 2007.

[4] M. Kiani, A. Clark and G. Mohay. Evaluation of Anomaly Based Character Distribution Models in the Detection of SQL Injection Attack. Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. p 47-55. 2008.

[5] C. Kruegel, F. Valeur and G. Vigna. Intrusion Detection System and Correlation. Challenges and Solutions. Springer. 2005

[6] C. Kruegel, G. Vigna, Anomaly detection of Web-based attacks. Proceedings of the 10th ACM Conference on Computer and Communications Security. p. 251-261. 2003.

[7] W. Lu and A. Ghorbani. Network Anomaly Detection Based on Wavelet Analysis. EURASIP J. Adv. Signal Process 2009, 1 (Jan. 2009), 1-16.

[8] W. Roberton; G. Vigna; C. Kruegel; R. Kemmerer. Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks, in: Proceedings of Network and Distributed System Security Symposium Conference, 2006, Internet Society, 2006.