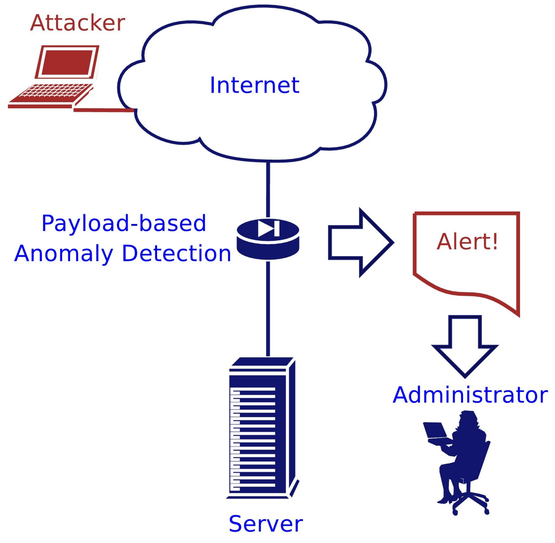
Combining Multiple One-Class Classifiers for Hardening Payload-based Anomaly Detection Systems

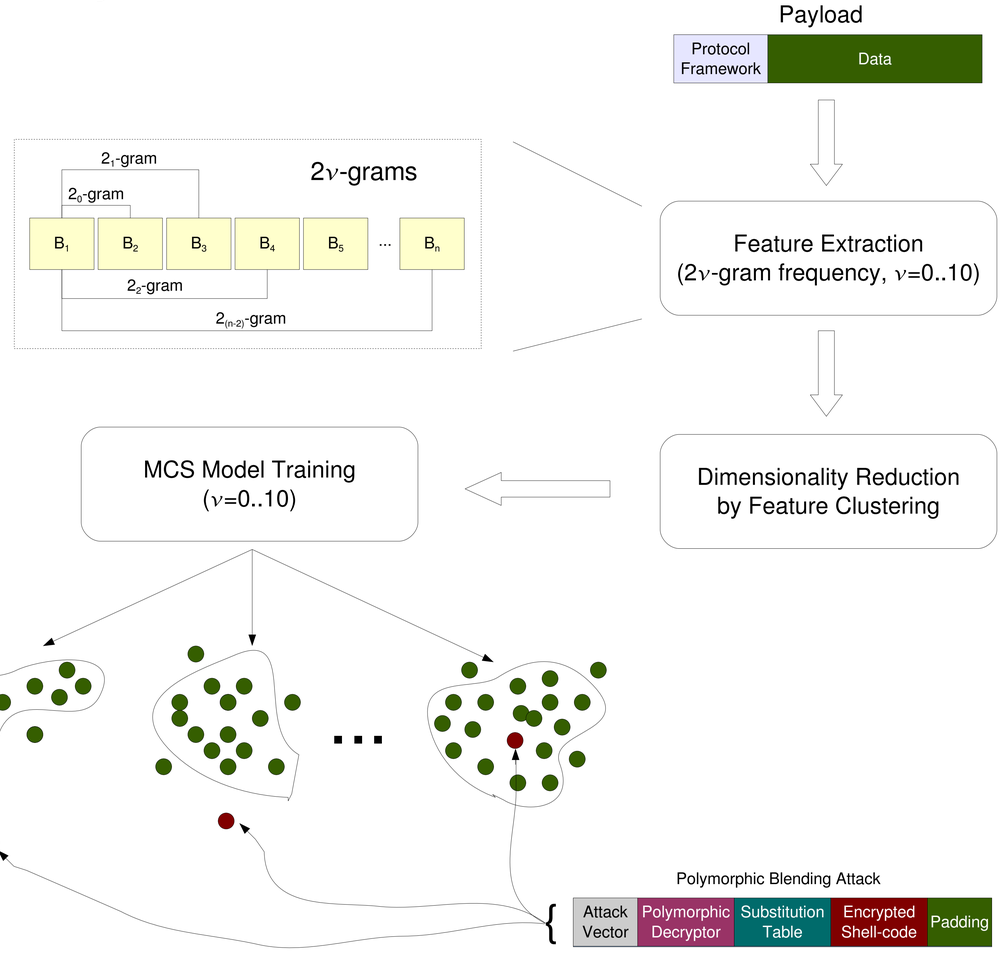
Roberto Perdisci, Guofei Gu, Wenke Lee

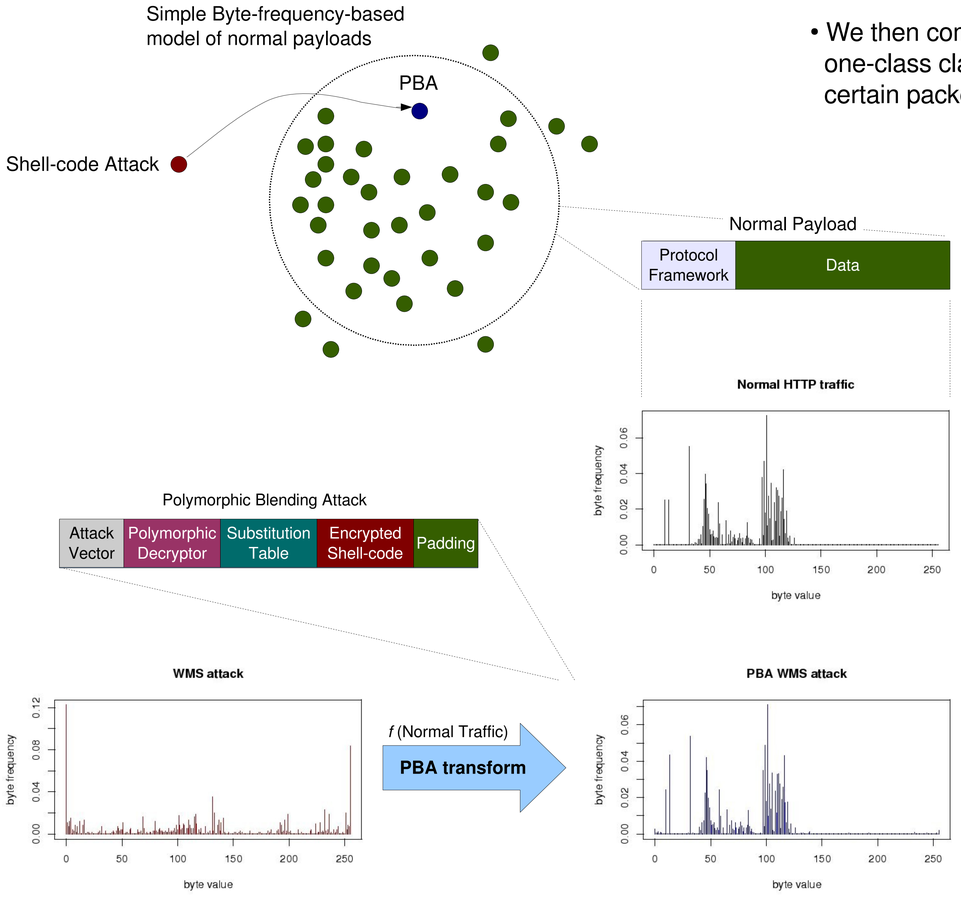
College of Computing, Georgia Institute of Technology, Atlanta, GA 30332, USA
DIEE, University of Cagliari, 09123 Cagliari, Italy

perdisci@damballa.com {guofei,wenke}@cc.gatech.edu



- Models of normal traffic based solely on byte frequency do not capture enough structural information
- A 2-gram frequency-based model may be used, but it has been shown that it may be easily evaded as well
- In order to make evasion more difficult we propose to extract multiple sets of features measuring the frequency of 2ν-grams
- We build a one-class classifier on each different feature space obtained by varying the parameter ν
- We then combine the output of each one-class classifier to decide if a certain packed is anomalous or not





P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, W. Lee. "Polymorphic Blending Attack". Usenix Security 2006.

Experimental Results

Dataset:
- 5 days of normal HTTP traffic
- 11 non-polymorphic attacks
- 6 polymorphic attacks generated using CLET
- 1 Polymorphic Blending Attack

Tab. 1 – Results obtained using 1-gram PAYL

DFP(%)	RFP(%)	Detected attacks	DR(%)
0.0	0.00022	1	0.8
0.01	0.01451	4	17.5
0.1	0.15275	17	69.1
1.0	0.92694	17	72.2
2.0	1.86263	17	72.2
5.0	5.69681	18	73.8
10.0	11.05049	18	78.6

Tab. 2 – Results obtained using 2ν-gram + Multiple Classifiers

DFP(%)	RFP(%)	Detected attacks	DR(%)
0.0	0.0	0	0
0.01	0.00381	17	68.5
0.1	0.07460	17	79.0
1.0	0.49102	18	99.2
2.0	1.14952	18	99.2
5.0	3.47902	18	99.2
10.0	7.50843	18	100

R. Perdisci, G. Gu, W. Lee. "Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems". ICMD 2006.