Improving Security of a Web System Using Biology Inspired Methods

Filip Šoltés
Supervisor: Assoc. Professor Ladislav Hudec

STU FIIT
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF INFORMATICS AND INFORMATION TECHNOLOGIES

Computational Intelligence in Intrusion Detection

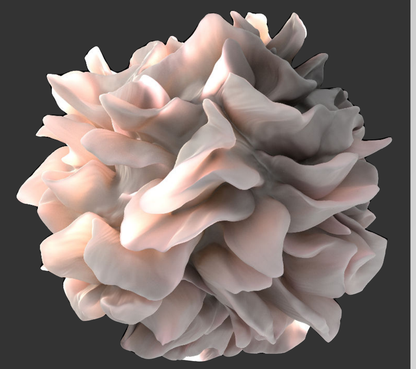
- adaptation
- fault tolerance
- error resilience with noisy data
- suitable for anomaly detection model

Our Goals

- the system will be applicable in real size web systems
- minimization of resource consumption on monitored system
- minimization of required user interaction

Deterministic Dendritic Cell Algorithm

- young algorithm (first prototpe 2005)
- populational, stochastic algorithm
- does not need extensive training
- low CPU requirements
- low FP counts
- antigen - signal



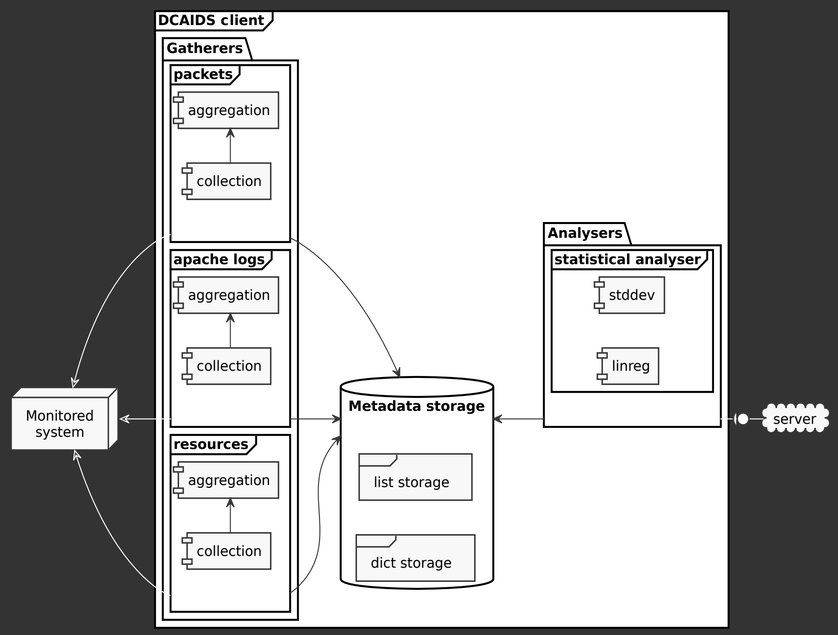
Dendritic Cell

DDCA Tuning

- original DDCA has no tuning mechanism
- our attempt - EA to set signal weights

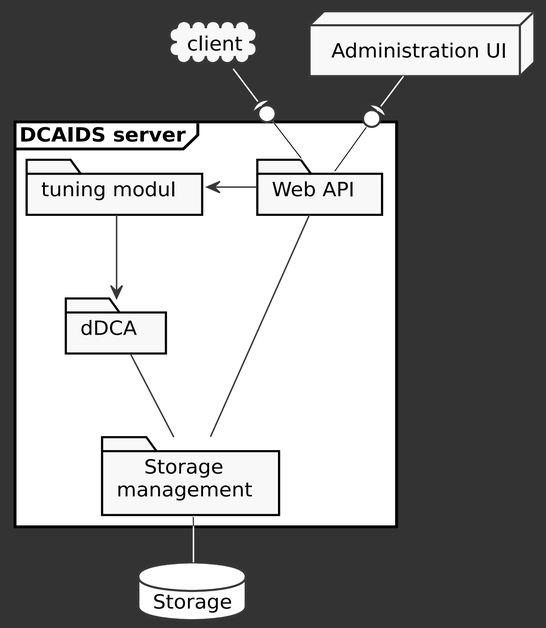
Architecture

Client Side



- data collecting
- aggregation and analysis
- transformation to signals and antigens

Server Side



- deep signal analysis
- antigen state assigment

Evaluation

- CSIC 2010 and Smihla datasets
- compare to PHPIDS
- two different sets of parameters

Table 1: Results of the final test dataset *CSIC 2010*.

System	DCAIDS				PHPIDS
Configuration	1		2		-
Tuning	no	yes	no	yes	-
TPR	48.9990	64.9189	81.9157	87.8811	15.6034
FPR	6.9291	6.2723	14.4035	12.7115	0.5555

Table 2: Results of the final test dataset *Smihla*.

System	DCAIDS				PHPIDS
Configuration	1		2		-
Tuning	no	yes	no	yes	-
TPR	98.9674	98.2388	95.2130	96.7488	97.4751
FPR	52.8751	38.9312	8.0179	7.6819	0.3108