AI-based Web Application Attack Detection

Mehmet Tahir SANDIKKAYA

October 15th, 2021

Istanbul Technical University
Computer Engineering Department

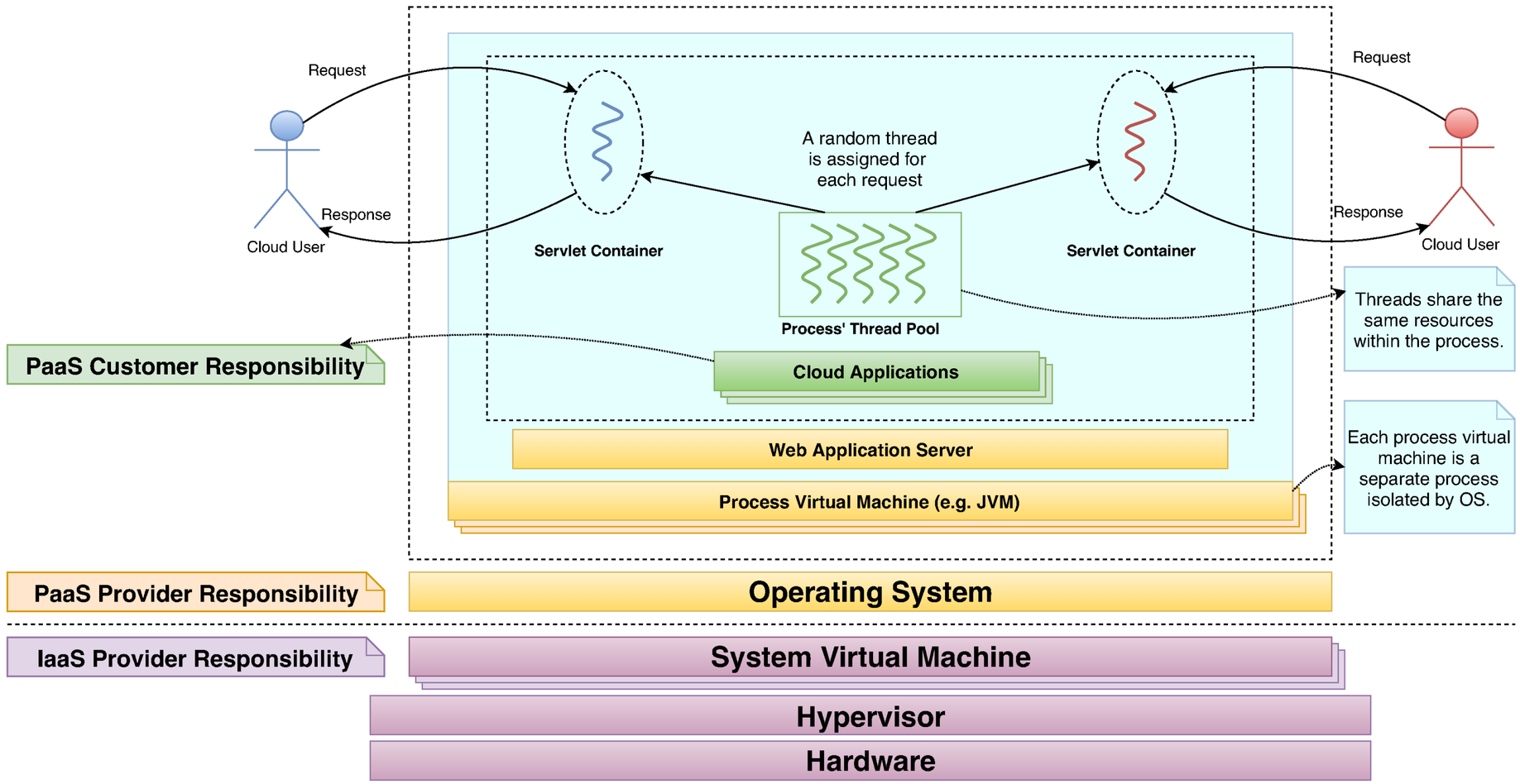
Contents

The Problem
Solutions
The Solution
The Experiment
The Results

The Problem

- ✔ Web applications mostly run in web application servers (WASs)
- ✔ WASs are processes from OS perspective
- ✔ Technically, all web applications share the same resources
- ✔ This setup was good before the cloud
- ✔ Possible conflicts:
  - ✘ Several cloud customers in the same WAS
  - ✘ Several web application users (cloud users) in the same WAS

The Problem



From: [Sandikkaya et al., 2019]

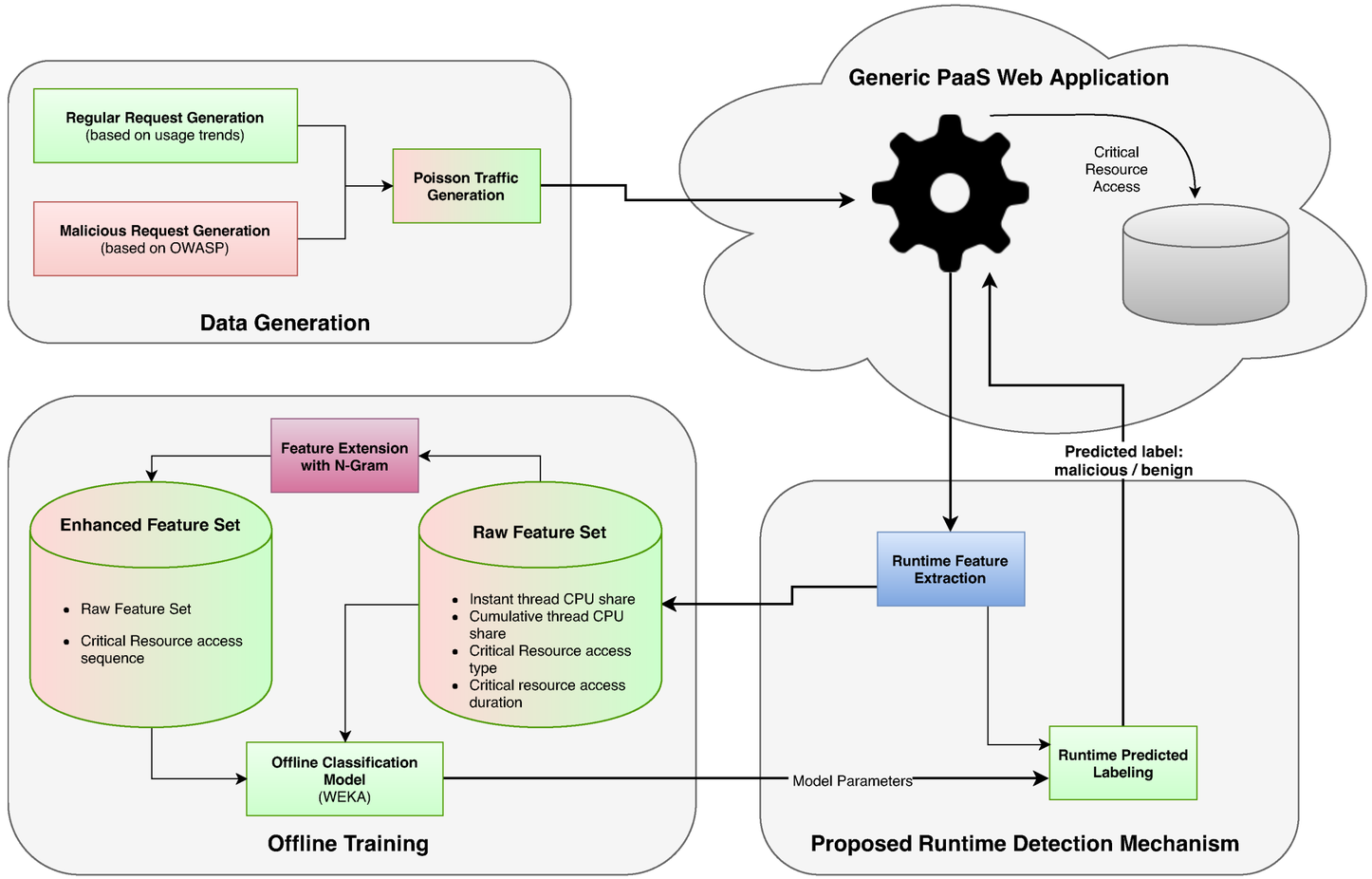
Solutions

- ✔ Isolation
- ✔ Access control
- ✔ Misbehavior detection New!
  - ✘ Must be managed by the PaaS provider
  - ✘ Must be independent from the users

The Solution

- ✔ Determine what is ordinary and malicious
- ✔ Monitor user-independent resource access
  - ✘ Map REST to CRUD
  - ✘ No user info, no code sequence
- ✔ Data set generation
  - ✘ Ordinary tasks on a case-study ticketing application (wrt rates)
  - ✘ Naive implementations of OWASP Top Ten [owa, 2017] (wrt rates)

The Solution



From: [Sandikkaya et al., 2019]

Rates of the generated operations

Name	Rate
Regular create	0.20
Regular read	0.59
Regular update	0.10
Regular delete	0.10
All malicious requests	0.01

From: [Sandikkaya et al., 2019]

Rates of the generated malicious attack types

Name	Rate
Cross-Site-Scripting (XSS)	0.23
Security Misconfiguration	0.22
Sensitive Data Exposure	0.20
Code Injection	0.12
Broken Authentication	0.10
Broken Access Control	0.07
Using Components with Known Vulnerabilities	0.03
XML External Entities	0.01
Insecure deserialization	0.01
Insufficient Logging and Monitoring	0.01

From: [Sandikkaya et al., 2019]

Rates of the caused CRUD operations at the web application database

Name	Rate
Malicious create	0.01
Malicious read	0.83
Malicious update	0.08
Malicious delete	0.08

From: [Sandikkaya et al., 2019]

Classification Results

Classifier	Feature Set	err	F-measure	Precision	Recall	TP	FP	FN	TN
Random Forest	Enhanced	**0.022**	**0.989**	**0.994**	0.984	984	**6**	**16**	98994
RndCommitte-RndForest	Enhanced	0.024	0.988	0.994	0.982	982	6	18	98994
RndCommitte-RndTree	Enhanced	0.025	0.987	0.990	0.985	985	10	15	98990
AdaBoost-J48	Enhanced	0.029	0.985	0.994	0.977	977	6	23	98994
1NN-LinearSearch	Enhanced	0.042	0.979	0.979	0.979	979	21	21	98979
3NN-LinearSearch	Enhanced	0.047	0.977	0.976	0.977	977	24	23	98976
Bagging-J48	Enhanced	0.045	0.977	0.987	0.968	968	13	32	98987
5NN-LinearSearch	Enhanced	0.055	0.972	0.974	0.971	971	26	29	98974
RndCommitte-RndForest	Raw	0.146	0.924	0.964	0.887	887	113	33	98967
Random Forest	Raw	0.146	0.924	0.963	0.888	888	34	112	98966
AdaBoost-J48	Raw	0.163	0.915	0.955	0.878	878	41	112	98959
Bagging-J48	Raw	0.165	0.914	0.956	0.875	875	40	125	98960
RndCommitte-RndTree	Raw	0.177	0.910	0.926	0.895	895	72	105	98928
3NN-LinearSearch	Raw	0.268	0.864	0.878	0.850	850	118	150	98882
BayesNet-k2LocalSrc-SmplEst'r	Enhanced	0.320	0.856	0.777	0.954	954	274	46	98726
5NN-LinearSearch	Raw	0.280	0.855	0.886	0.826	826	106	174	98894
1NN-LinearSearch	Raw	0.295	0.853	0.851	0.855	855	150	145	98850
BayesNet-k2LocalSrc-SmplEst'r	Raw	0.458	0.743	0.820	0.675	675	143	325	98857

From: [Sandikkaya et al., 2019]

The Results

- ✔ Trade-off in between expensive isolation and cheaper classification
- ✔ Promising results (but not field-tested)
- ✔ Easy to implement
- ✔ Focus is on the behavior not on the user
- ✔ Privacy-friendly (both for the cloud user and the cloud customer)
- ✔ Ability to detect insider attacks or coffee-break attacks

Thank you for listening

Please contact via:
sandikkaya@itu.edu.tr

References

[owa, 2017] (2017). OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. Technical report, The Open Web Application Security Project. Retrieved from `https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf`.

[Sandikkaya et al., 2019] Sandikkaya, M. T., Yaslan, Y., and Özdemir, C. D. (2019). DeMETER in clouds: detection of malicious external thread execution in runtime with machine learning in PaaS clouds. *Cluster Computing*.