Toward Just-in-Time Patching for Containerized Applications

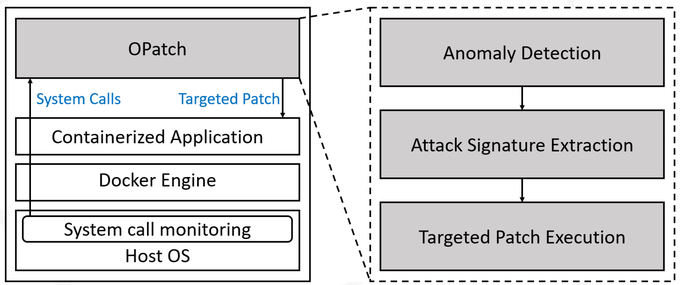
Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, Xiaohui Gu
North Carolina State University

Motivation

Containerized applications pose a set of new security challenges to distributed computing environments

- An alarming degree of vulnerability exposures exist in official image repositories (Shu et al. 2017)
- Significant resource increase in resource-limited containers can result after patching
- Traditional patching schemes that follow a scheduled whole upgrade approach (e.g., every Tuesday), do not work well for short-lived containers

Overview



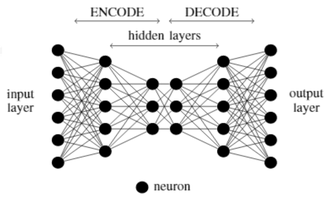
OPatch is composed of three modules

- **Anomaly Detection** detects vulnerability exploits
- **Attack Signature Extraction** creates a signature to map exploits to the culprit vulnerability identifier
- **Targeted Patch Execution** triggers the proper software library update

Anomaly Detection

OPatch applies the unsupervised autoencoder neural network to detect abnormal system call frequency changes

- Does not require labelled training data which makes it robust to unknown attacks
- Achieves good accuracy with relatively few neurons and low training cost



Attack Signature Extraction

Attacks are characterized by a Secure Hash Algorithm (SHA) signature of the top frequent system calls

Application	Top System Calls				
Apache ActiveMQ	write	fcntl	geteuid	getegid	switch
ImageMagick	read	lseek	open	switch	futex
Nginx	switch	poll	stat	writev	read

Targeted Patch Execution

Targeted patching only installs the packages required by the application

```
#!/bin/bash
# A Sample Targeted Patching for Ghostscript

# download files
apt-get update
apt-get -y install wget gcc make
wget https://github.com/.../ghostscript-x.xx.
    tar.gz
tar xvf ghostscript-x.xx.tar.gz

# install files
cd ghostscript-x.xx
./configure
make install

# remove files
apt-get purge -y wget gcc make
apt-get autoremove -y
cd ..
rm -r ghostscript-x.xx.tar.gz ghostscript-x.xx
```

Whole Upgrade only updates applications handled by the package manager

```
> apt-get update
> apt-get upgrade
```

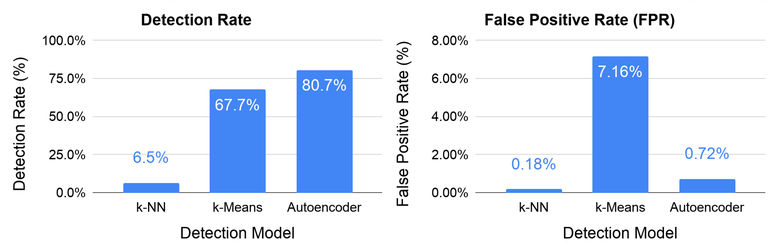
Contribution

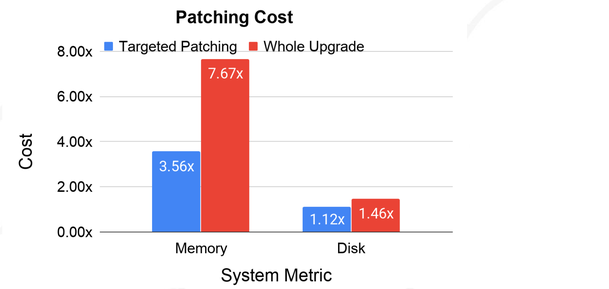
OPatch is a new on-demand targeted patching framework for container environments

- We perform lightweight vulnerability exploit detection
- We achieve practical and effective security protection using a signature extraction scheme for identifying vulnerabilities
- We evaluate OPatch on 31 real world security vulnerability exploits in 23 commonly used server applications

Results

- We evaluated OPatch over **31** real-world vulnerabilities discovered in **23** common containerized applications





Conclusion

Our initial experimental results of OPatch are promising

- We can increase detection rate to over 80% and reduce false alarm rate to 0.7%
- Compared to the whole upgrade approach, OPatch can reduce the memory overhead by up to 84% and disk overhead by up to 40%

HOTSOS 2020
7TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 7-8, 2020 | LAWRENCE, KANSAS