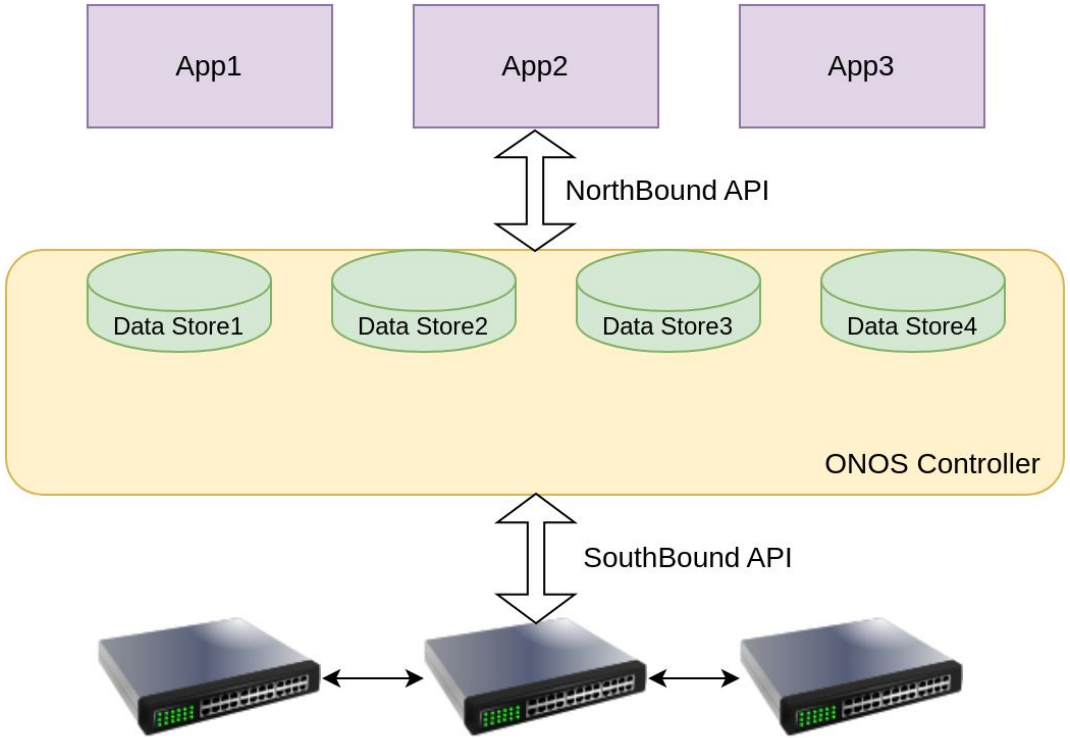
Proposal and Investigation of a framework for Cross App Poisoning attacks detection in Software Defined Networks

SAPIENZA
UNIVERSITÀ DI ROMA

Edoardo Ottavianelli,
Supervisor Prof. Marco Polverini
A.Y. 22/23

SDN Paradigm (using ONOS)



Pros:

- Programmability
- Monitoring
- Flexibility

Cons:

- Security
- Complexity
- Maintenance

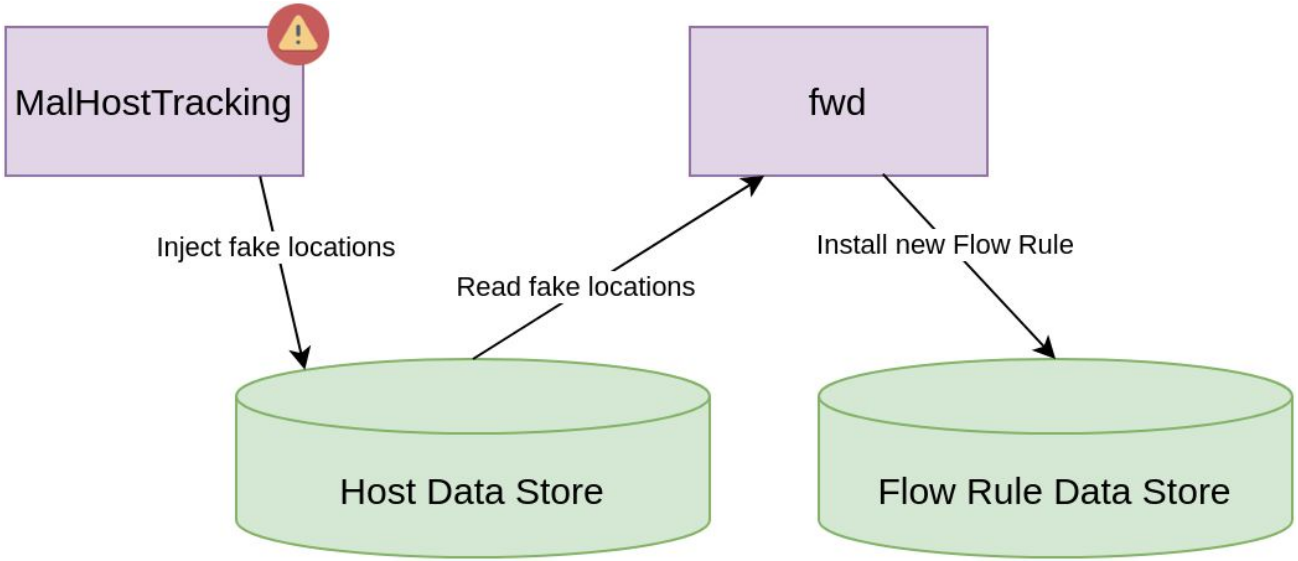
Security-Mode ONOS

```
<feature name="onos-app-sdnip" version="1.0.0"
         description="SDN-IP peering application">
    <type> ONOS Application </type>
    <role> non-admin </role>
    <uses-permission onos:name="onos.permission.INTENT_WRITE"/>
    <uses-permission onos:name="onos.permission.DEVICE_READ"/>
    <uses-permission onos:name="onos.permission.TOPOLOGY_EVENT"/>
    <uses-permission onos:name="onos.permission.PACKET_EVENT"/>
   <bundle>mvn:org.onosproject/onos-app-sdnip/1.0.0</bundle>
</feature>
```

CAP attack in ONOS

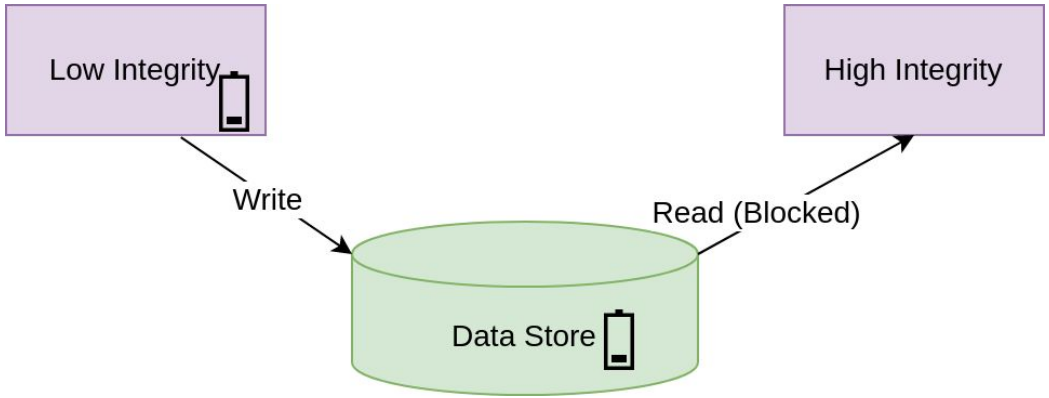
MalHostTracking:
- HOST_WRITE

fwd:
- HOST_READ
- FLOW_WRITE



ProvSDN (and vIFC)

- Based on Integrity Label Model
- Potentially malicious apps deployed in production environment
- Hooks on NorthBound API
- Based on IFC provenance graph



Limitations of existing solutions

- The integrity labels model severely limits network capabilities
- An attacker could implement a “self-revocation” attack
- High Latency due to runtime checks

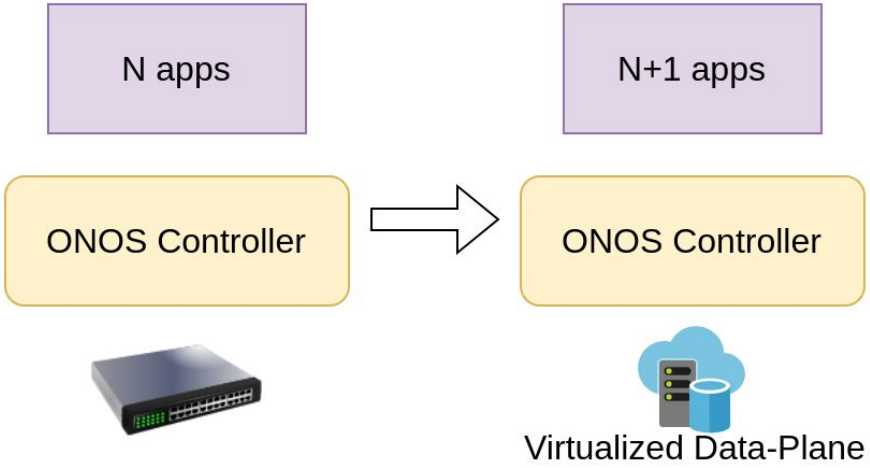
Changing detection approach

Offline detection:

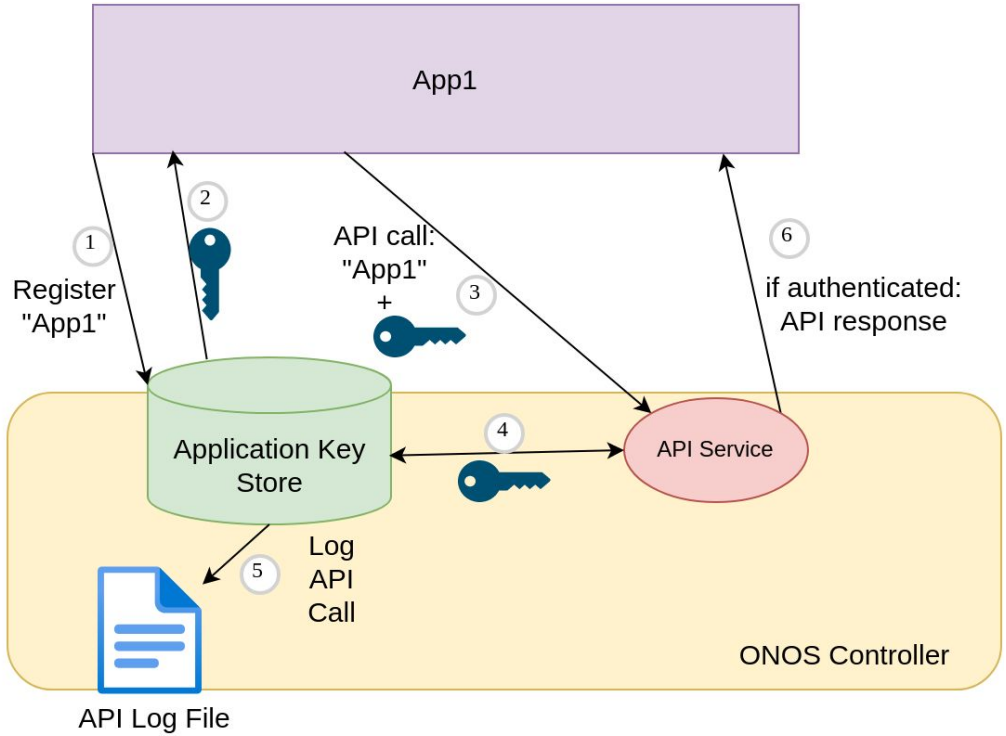
a. Replicate prod. environment

b. Extensive logging

c. Log data mining

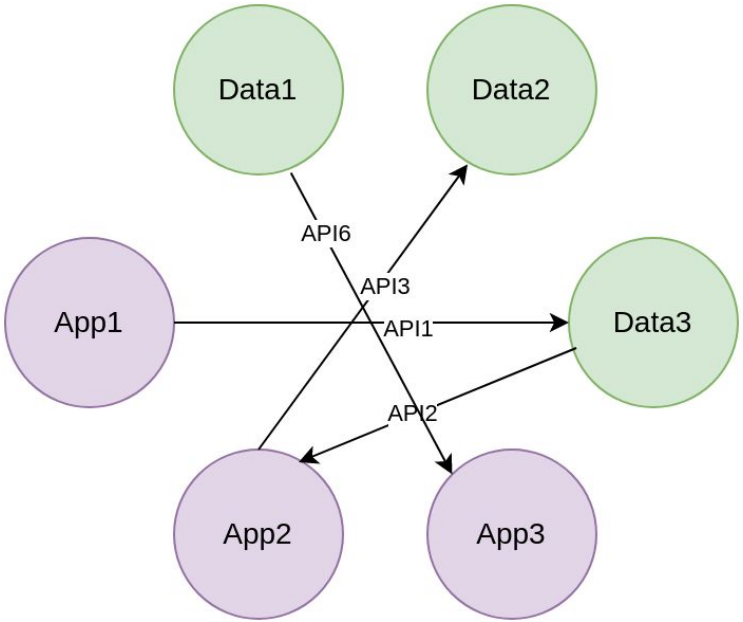


Application key store

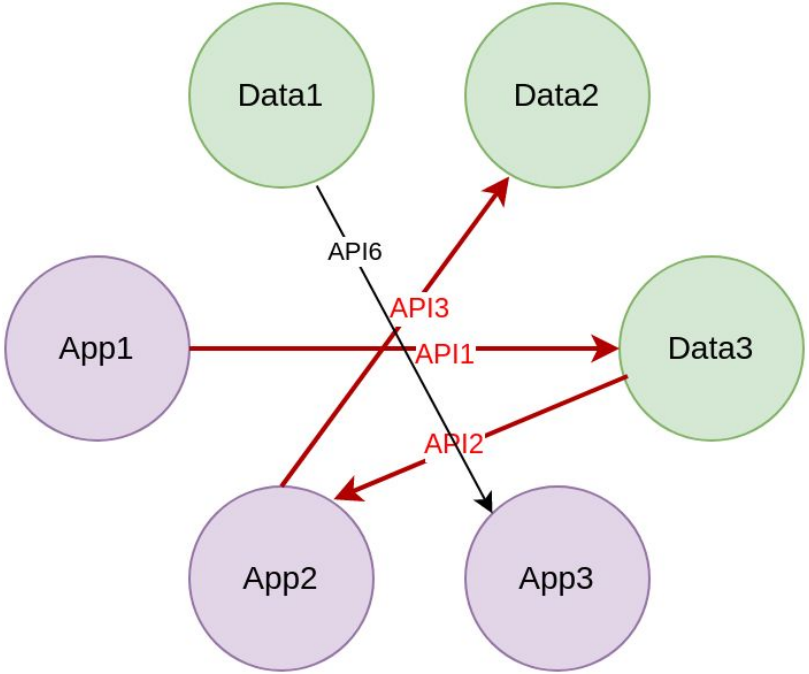


Log mining + graph construction

Timestamp	App1	API1	Parameters
Timestamp	App2	API6	Parameters
Timestamp	App2	API2	Parameters
Timestamp	App3	API5	Parameters
Timestamp	App2	API3	Parameters
. . .			
. . .			



Search for potential CAP attacks



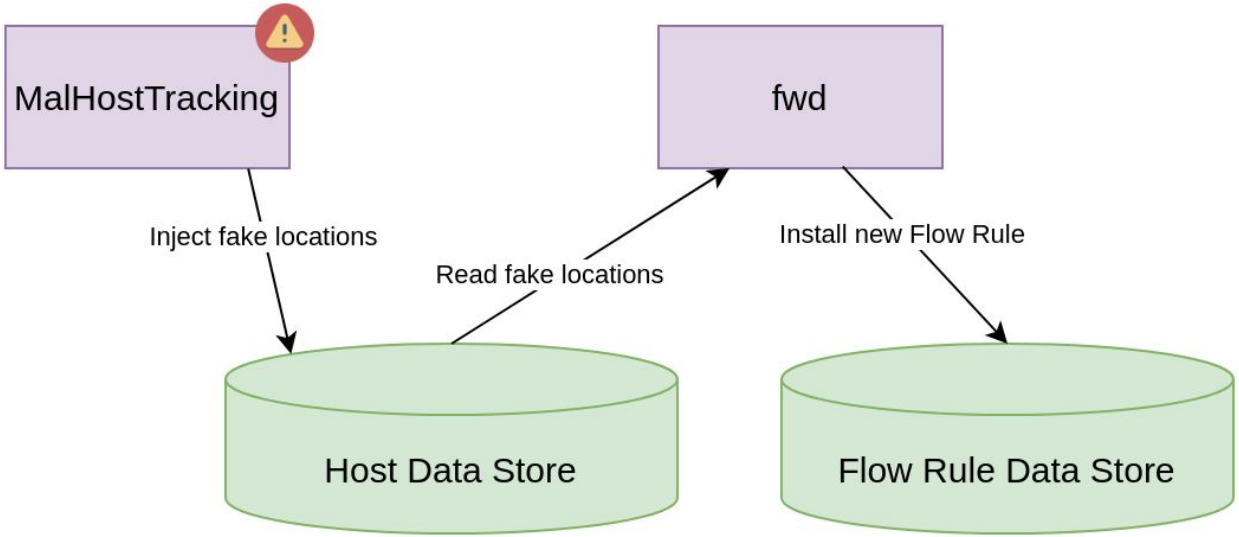
CAP Attack vector set:
Cv(G) = {app0, obj1, app2, obj3, …, appN-1, objN} |
N >= 3; N is odd

Search potential CAP attacks using a time section:

Timestamp	*App1*	*API1*	*Parameters*	1s
Timestamp	App2	API6	Parameters	
Timestamp	*App2*	*API2*	*Parameters*	
Timestamp	App3	API5	Parameters	
Timestamp	*App2*	*API3*	*Parameters*	
Timestamp	App2	API3	Parameters	

. . .
. . .

Tests and results 1



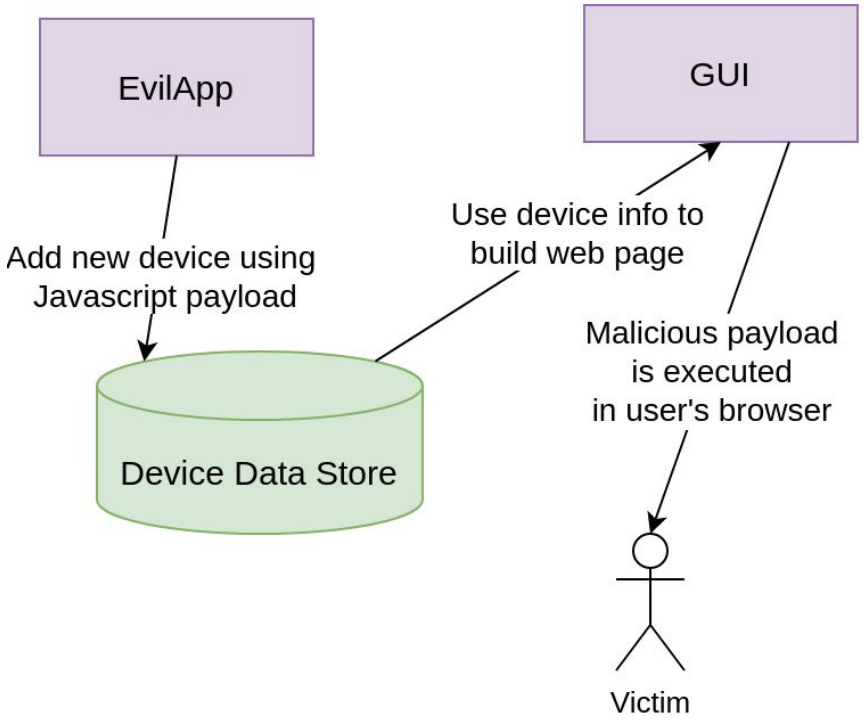
- Exploited 240 CAP attacks
- Virtualized 4 hosts and 4 switches using Mininet
- No one of the hosts can receive packets

Tests and results 2

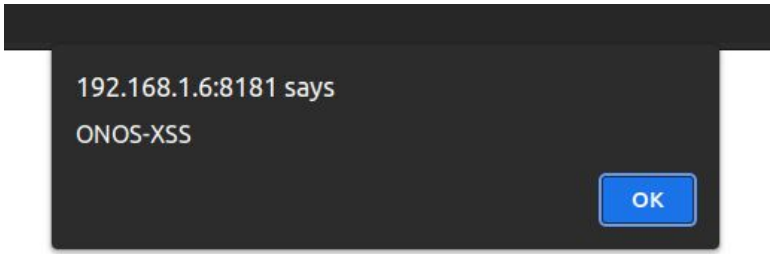
N#	Time section (milliseconds)	potential CAP attacks found	Exec. time
1	10000	26572	5.263378 sec.
2	5000	9211	2.749676 sec.
3	2000	2900	1.213360 sec.
4	1000	1340	76 ms
5	500	584	45 ms
6	200	200	< 2 ms
7	100	200	< 2 ms
8	50	200	< 1 ms
9	10	152	< 1 ms
10	1	43	< 1 ms

- Less than 1ms of overhead
- Secure defense mechanism
- Complete control over the test environment
- Network capabilities not limited

CAP Attack targeting Web app



- HttpOnly flag set 😭
- Keylogger 😈
- Phishing 😈

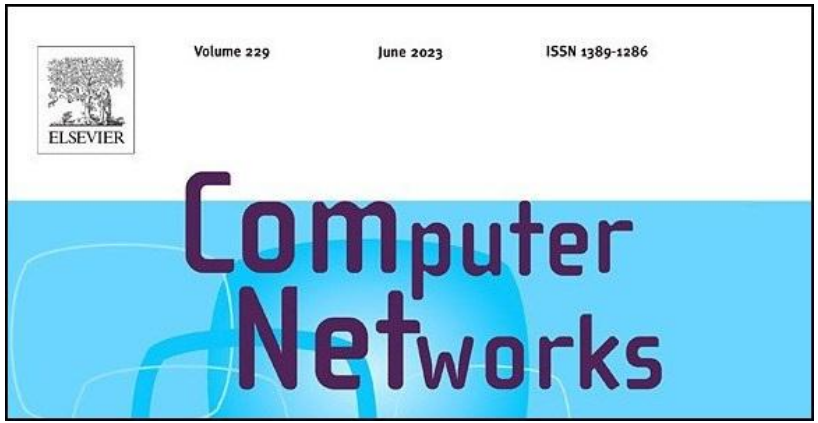


Paper + CVEs

Cross App Poisoning Attacks Detection in Software Defined Networks

Edoardo Ottavianelli, Marco Polverini

Department of Information engineering, Electronics and Telecommunications (DIET)
University of Roma "Sapienza" - Via Eudossiana 18, 00184 Roma, Italy
Telephone: +39 0644585371, e-mail: name.surname@uniromal.it



CVE-ID	
CVE-2023-24279	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A cross-site scripting (XSS) vulnerability in Open Networking Foundation ONOS from version

CVE-ID	
CVE-2023-30093	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A cross-site scripting (XSS) vulnerability in Open Networking Foundation ONOS from version v1.9.0 to v2.7.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter of the API documentation dashboard.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.edoardoottavianelli.it/CVE-2023-30093/
- MISC:https://www.youtube.com/watch?v=jZr2JhDd_S8

Assigning CNA

MITRE Corporation

Future work

- Add auth support for all ONOS API
- Improve Log data mining
- Continue vulnerability research