The use of work flow topology observables in a Security Autonomous Response Network

by Adriaan Dens

Supervised by Prof. Dr. Robert Meijer and Ir. Marc Makkes
The use of work flow topology observables in a Security Autonomous Response Network
Work flow topologies

DATA: 1 JPG
Work flow topologies

DATA: 1 JPG
Work flow topologies

DATA: 1 JPG
Work flow topologies

DATA: 1 JPG
The use of work flow topology observables in a Security Autonomous Response Network
Observables of work flow topologies

• The topology
Observables of work flow topologies

• The link usage

```
DATA: JPG image, 2MB
```

```
0,05MB (extracted info)
```

```
start
```

```
kindOfAttachment
```

```
BmpParser
```

```
JpgParser
```

```
end
```

```
DocParser
```

```
ExcelParser
```

```
2MB
```

```
2MB
```

```
2MB
```
Observables of work flow topologies

- Node activity

DATA: JPG image, 2MB
The use of work flow topology observables in a Security Autonomous Response Network
Research Question

How can observables of software controlled work flow topologies be used in Security Autonomous Response networks?
Relation between amount of (meta)data and things you can do

• Controlloop needs to know about topology
• Machine learning / benchmarking / ...
• Lots of (meta)data => many things to control/check
Observables & security

*Data residing in the network tells something about the expected observables.*
Observables & security

DATA: 10x JPG image
5x Doc’s

Processed 3 JPG’s
Processed 1 Doc
Observables & security

7 JPG images
4 Doc’s

Processed 3 JPG’s
Processed 1 Doc

DATA: 10x JPG image
5x Doc’s
Observables & security

• Node activity: estimate activity...
• Link load: estimate link load...
• Topology: estimate topology...

... given data in the network

and compare to actual values of observables.
Estimating node activity and link load

- Probability of data hitting a function
- Probability of data hitting a node
- Probability of data being in the node when sampling

Link load follows same intuition
Calculation of topology

- Calculate number of nodes per function as upperbound: $1 \leq \text{real value} \leq \text{upperbound}$
- Scale down the topology => compare with original topology
Web interface of Proof of Concept
Proof of Concept

• Developed control API for mininet:
  – But too slow for big networks
  – You cannot dynamically add hosts to mininet
• Therefore, pure simulation which uses same APIs
• PoC uses CPU load as node activity parameter
Autonomous response

- Kill node
- Ignore node / Send fake data
- Extra monitoring
- Reprovisioning
- SDN flow rules
Conclusion

• Observables of work flow topologies can be used
  – By using metadata from the topology
  – Relation between knowledge of data and things you can do
  – More testing of equations is needed (finetuning)
Questions?