Ontological representation of networks for IDS in cyber-physical systems

Vasily A. Sartakov
Ksys labs
AIST 2015

Sverdlovsk

Cyber-Physics Systems

- Critical Infrastructure
  - Hardware/software
  - Compound (consist of different elements)
  - Data transfer and control
  - Represented as Net (Communication)

Software

- Functions
- Requires updates
  - Vulnerabilities
  - Malicious
  - Intrusions

Scope

- Intrusion Detection System
- Ontological representation
  - Communications
  - Specification

Assumptions (model of an intruder)

- Intrusion is carried out inside the network
- Abnormal affection of some elements of the critical infrastructure object on the others

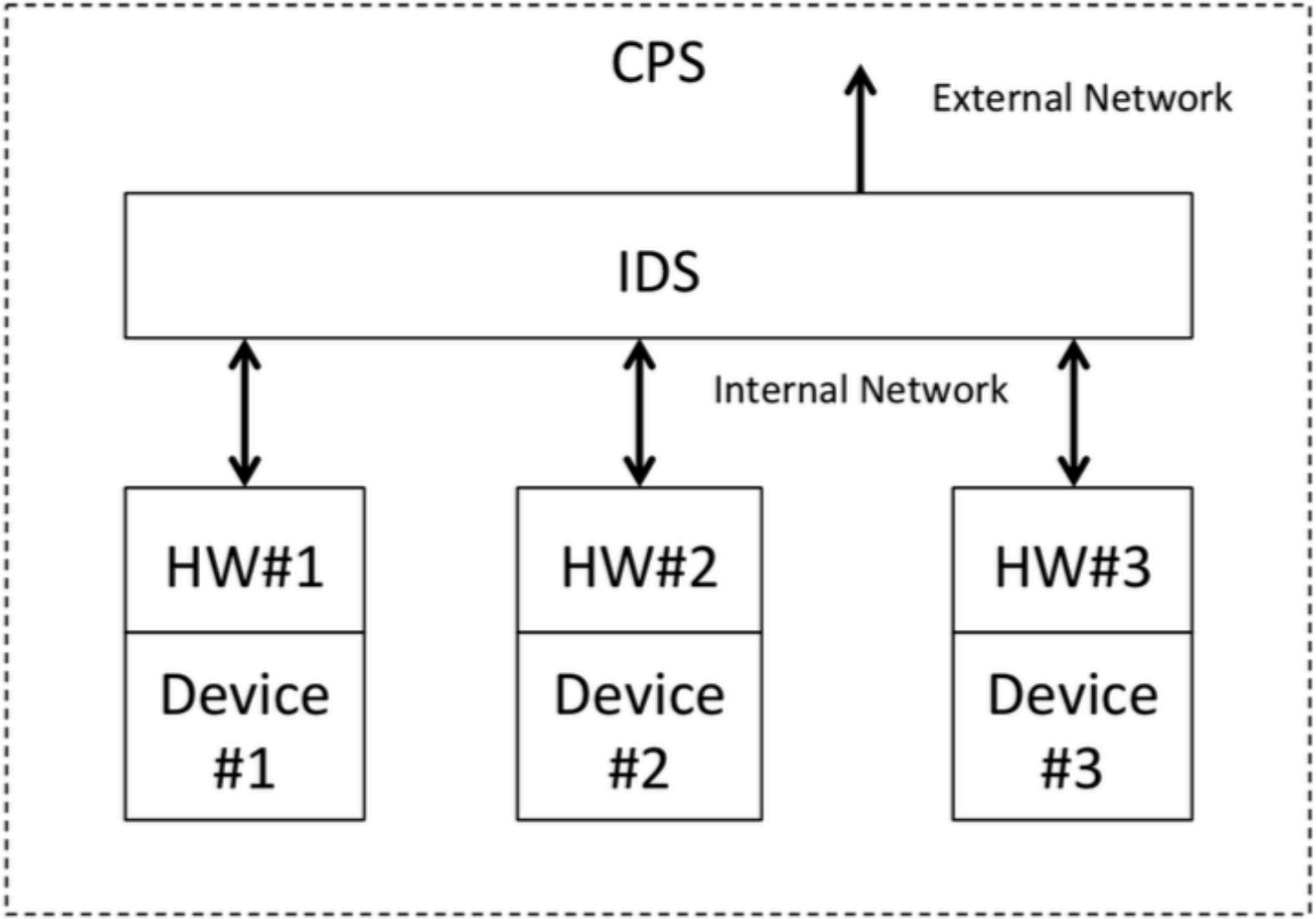
IDS

- Anomaly-based
- Signature analysis
- Probabilistic
- Specification

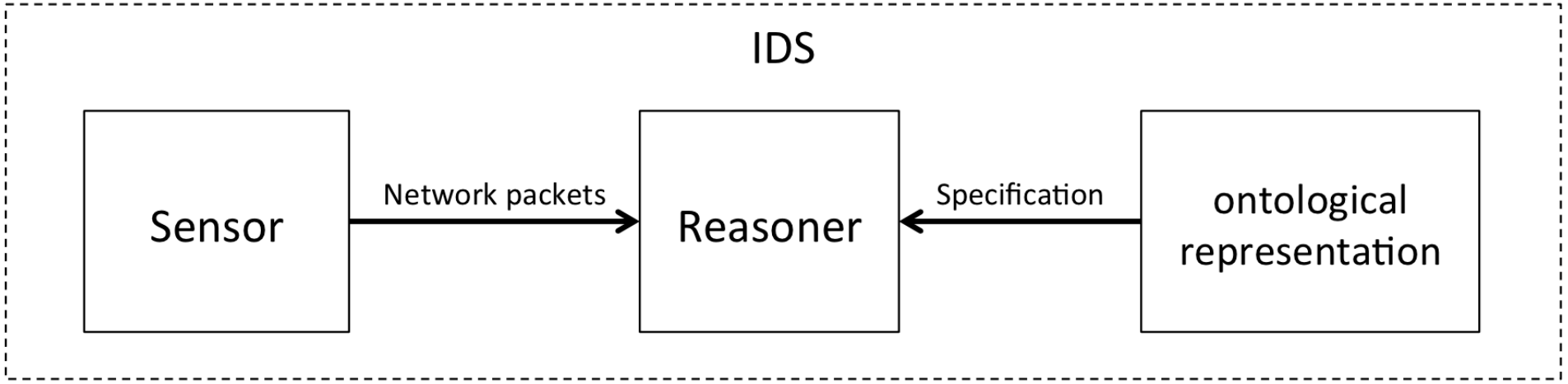
Specification

- Lowest rate of type II errors
- Does not require continuous support and development of signature databases
- Allows to detect unknown types of attacks and intrusions

Architecture



Architecture

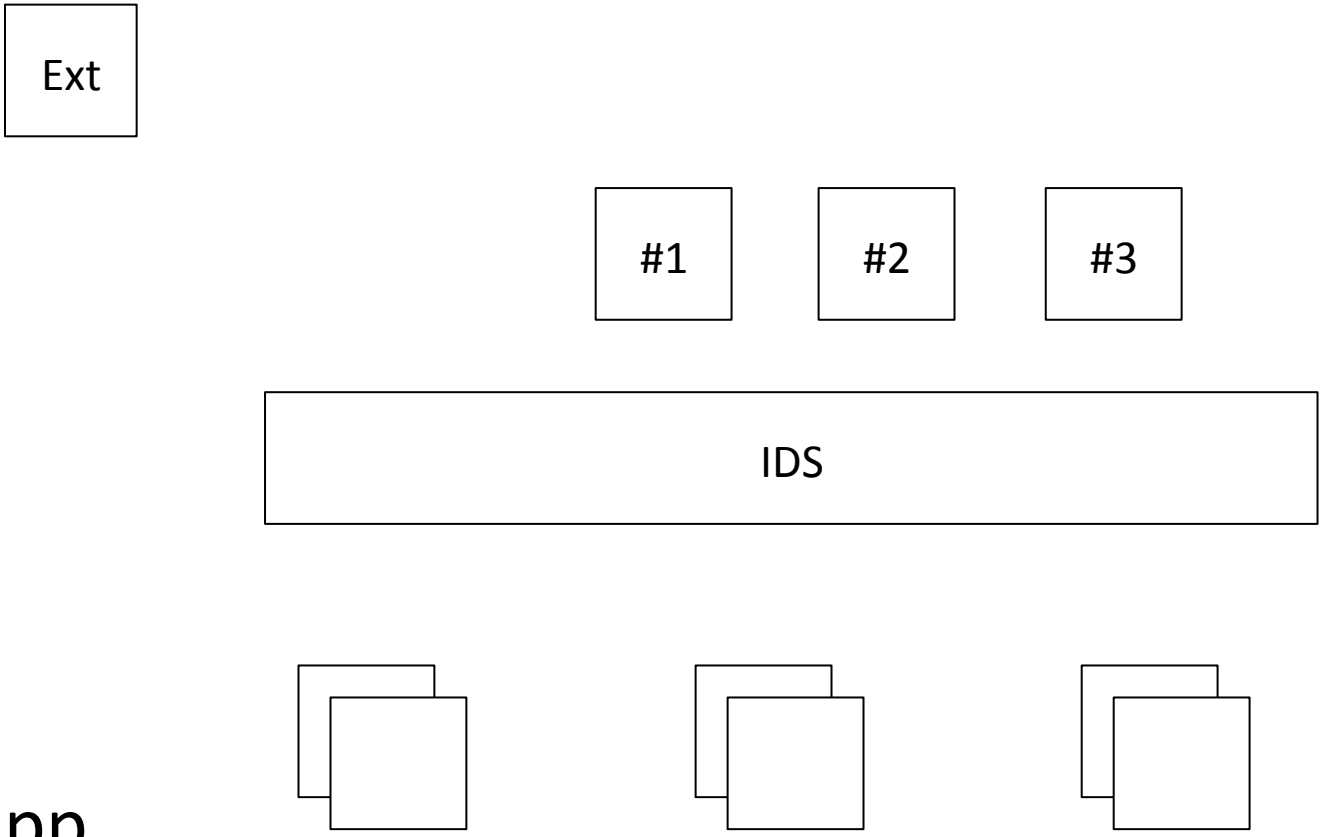


Suricata/Snort Rule

```
action proto src_ip src_port -> dst_ip dst_port
    (msg:"Message";content:"body")

alert ip [3.1.1.1] any -> any any
    (msg:" Wrong hw addr";
            eth_src:00-00-03-01-01-01;)
```

Example



- 1 External
- 3 Clients
- 3 servers + Replication
- 2-3 server app.
- 42+ connections

Cyber-Physics Systems

- Complexity
- How to control/debug?
- Visualization
- Hardware?

Ontology

- Ontology is a formal, clear, precise definition of conceptualization.
- Conceptualization is an abstract, simplified view of the world formed for specific purposes
- Combination of Logic and Physical entities
- RDF n3 (subject-predicate-object)

Ontology

- Rack (Physical)
- Unit (Physical)
- Server (physical, logical)
- Model (Physical)
- NetDev (Physical)
- Switch (Physical)
- Port (Physical)
- Subnet (logical)
- Program
- relationships

Representations

- Physical
  - Servers: Location, voltage, etc
  - Connections: physical ports
- Logical
  - Programs: Client <-> Server
  - Subnets
  - Modificator: Replication

- Physical <-> Logical
  - IP/MAC/Device
  - Server (physical, component of the network)

Representations

```
@forSome <#rack1> .
<#rack1>                a <Rack> .
<#rack1>                <name>                  "rack" .
<#rack1>                <sn>                    "555-55-45" .
<#rack1>                <maxUnits>              "25" .
<#rack1>                <hasUnit>               <#r1_u0> .
...
<#rack1>                <hasUnit>               <#r1_u24> .
```

```
@forSome <#r1_u11> .
<#r1_u11>                a                      <Unit> .
<#r1_u11>                <number>               "11" .
<#r1_u11>                <occupiedBy>           <#Switch2> .

@forSome <#r1_u12> .
<#r1_u12>                a                      <Unit> .
<#r1_u12>                <number>               "12" .
<#r1_u12>                <occupiedBy>           <#APMS> .
```

```
@forSome <#CISCO2950> .
<#CISCO2950>            a               <Model> .
<#CISCO2950>            <name>          "Cisco Catalyst 2950-24" .
<#CISCO2950>            <size>          "1U" .
<#CISCO2950>            <power>         "30" .
<#CISCO2950>            <cooling>       "nan" .
<#CISCO2950>            <weight>        "3" .
```

```
@forSome <#Switch2> .
<#Switch2>              a                       <Switch> .
<#Switch2>              <name>                  "Switch2" .
<#Switch2>              <sn>                    "111-456" .
<#Switch2>              <model>                 <#CISCO2950> .
<#Switch2>              <mngPort>               "0" .
<#Switch2>              <port>                  <#sw2_p1> .
<#Switch2>              <port>                  <#sw2_p2> .
```

Representations

```
@forSome <#net1> .
<#net1>          a                <Subnet> .
<#net1>          <name>           "NET1" .
<#net1>          <hasServer>      <#SPS> .
<#net1>          <hasServer>      <#APMS> .
```

```
@forSome <#SS> .
<#SS>            a                <Server> .
<#SS>            <name>           "SS" .
<#SS>            <hasDevice>      <#SS_eth0> .
<#SS>            <model>          <#simple1U> .
<#SS>            <hasProgram>     <#ss_sps_1414> .
```

```
@forSome <#sps_mysql_3306> .
<#sps_mysql_3306>       a                        <Program> .
<#sps_mysql_3306>       <name>                   "mysql" .
<#sps_mysql_3306>       <listenPort>             "3306" .
<#sps_mysql_3306>       <communicateWith>        <#sps_mysql_3306> .
```

Representations

```
@forSome <#S3_eth0> .
<#S3_eth0>      a <NetDev> .
<#S3_eth0>      <name>           "eth0" .
<#S3_eth0>      <ip>             "2.4.1.1" .
<#S3_eth0>      <hwAddr>         "00-00-02-04-01-01" .
<#S3_eth0>      <speed>          "1Gb" .
<#S3_eth0>      <type>           "UTP" .
<#S3_eth0>      <connectedWith> <#sw1_p2> .
```

```
@forSome <#sw1_p2> .
<#sw1_p2>               a                       <Port> .
<#sw1_p2>               <number>                "2" .
<#sw1_p2>               <speed>                 "1Gb" .
<#sw1_p2>               <type>                  "UTP" .
<#sw1_p2>               <connectedWith>         <#S3_eth0> .
```

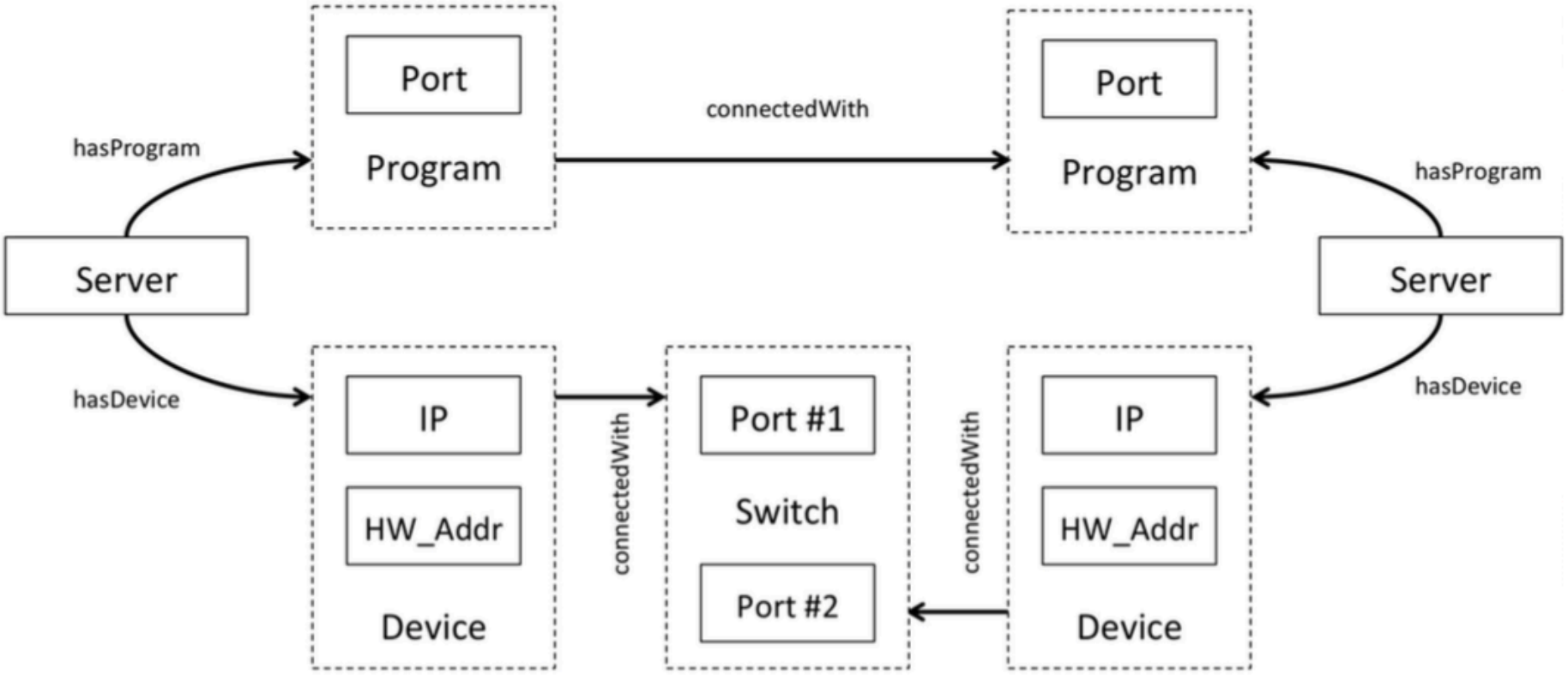
Client-Server

```
@forSome <#sps_mysql_3306> .
<#sps_mysql_3306>       a                       <Program> .
<#sps_mysql_3306>       <name>                  "mysql" .
<#sps_mysql_3306>       <listenPort>            "3306" .
<#sps_mysql_3306>       <communicateWith>       <#sps_mysql_3306> .

@forSome <#sps_crypto_80> .
<#sps_crypto_80>        a <Program> .
<#sps_crypto_80>        <name>          "crypto_server1" .
<#sps_crypto_80>        <listenPort>    "80" .

@forSome <#apms_sps_80> .
<#apms_sps_80>  a                       <Program> .
<#apms_sps_80>  <name>                  "crypto_client" .
<#apms_sps_80>  <communicateWith>       <#sps_crypto_80> .
```

Architecture



FDNet

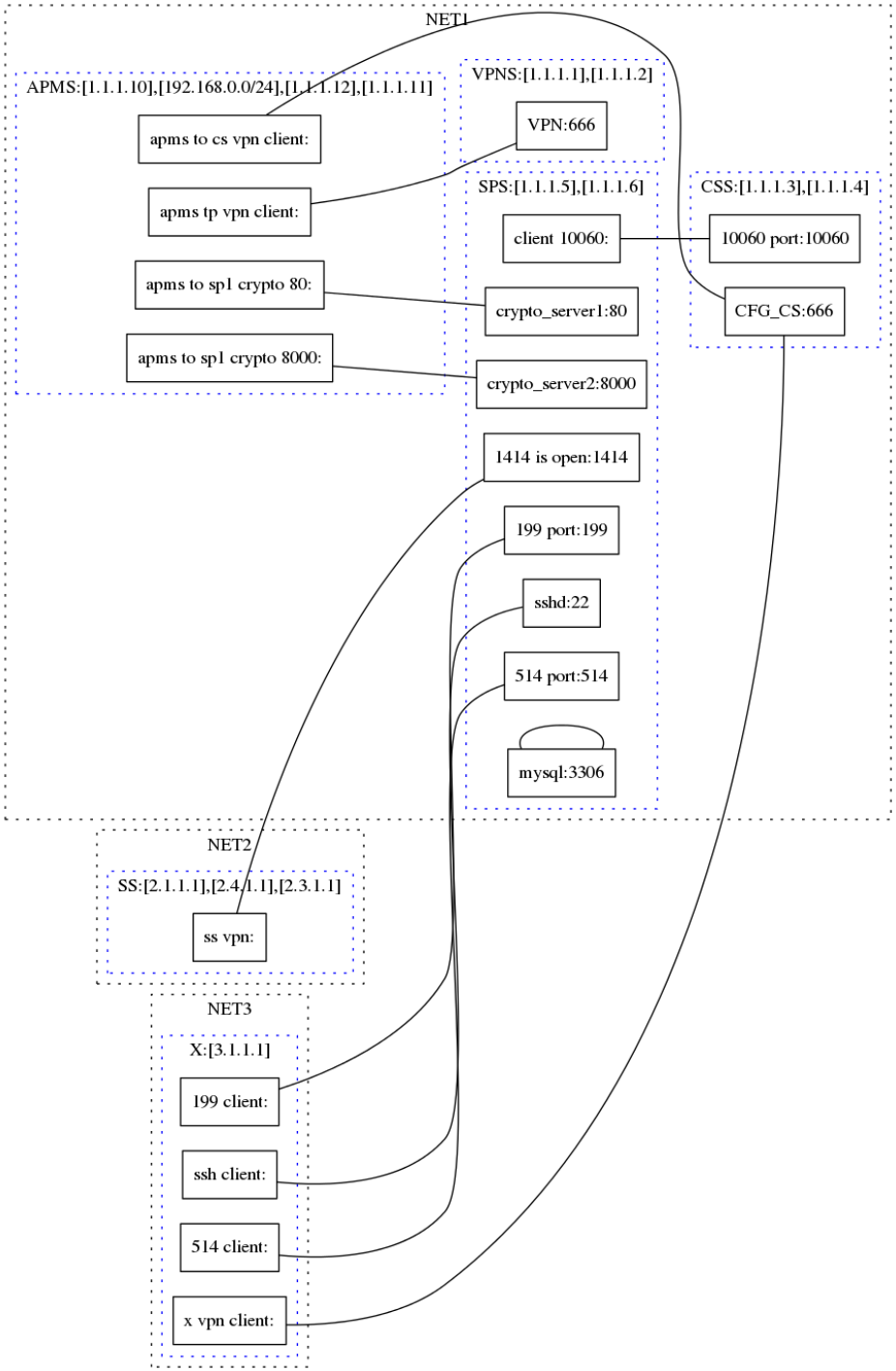
- Python
- RDF N3
- Output
  - sid-msg.map
  - net.dot & net.png
  - net.rules
  - net_ip-plan.xlsx, net_phys.xlsx, net_place.xlsx
- Decrease complexity
  - Replicas
  - Virtual networks
  - Subnets (weak)
- http://github.com/Ksys-labs/fdnet

Replication

```
@forSome <#SS> .
<#SS>           a               <Server> .
<#SS>           <name>          "SS" .
<#SS>           <hasDevice>     <#SS_eth0> .
<#SS>           <model>         <#simple1U> .
<#SS>           <hasProgram>    <#ss_sps_1414> .

@forSome <#S2> .
<#S2>           a               <Server> .
<#S2>           <name>          "S2" .
<#S2>           <hasDevice>     <#S2_eth0> .
<#S2>           <model>         <#simple1U> .
<#S2>           <replica>       <#SS> .

@forSome <#APM4> .
<#APM4>         a <Server> .
<#APM4>         <name>          "APM4" .
<#APM4>         <replica>       <#APMS> .
<#APM4>         <ip>            "192.168.0.0/24" .
```


NET1
APMS:[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]
apms to cs vpn client:
apms tp vpn client:
apms to sp1 crypto 80:
apms to sp1 crypto 8000:
VPNS:[1.1.1.1],[1.1.1.2]
VPN:666
SPS:[1.1.1.5],[1.1.1.6]
client 10060:
crypto_server1:80
crypto_server2:8000
1414 is open:1414
199 port:199
sshd:22
514 port:514
mysql:3306
CSS:[1.1.1.3],[1.1.1.4]
10060 port:10060
CFG_CS:666
NET2
SS:[2.1.1.1],[2.4.1.1],[2.3.1.1]
ss vpn:
NET3
X:[3.1.1.1]
199 client:
ssh client:
514 client:
x vpn client:

Example

- 86 Entities
- 30 Rules(!!)
  - 8+8
  - 14 HW_ADDR
  - Subnets, undefined components, replications, etc.

Anti-conclusion

- DARPA Cyber Gran Challenge

Thank you

Vasily A. Sartakov

Sartakov@ksyslabs.org