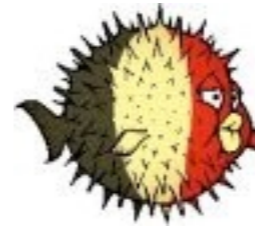


\$HOME Sweet \$HOME



\$ whoami

- Xavier Mertens (@xme)



- Consultant @ day



- Blogger, Hacker @ night

`/dev/random`

Can't sleep, hackers will eat me!



- BruCON co-organizer



\$ cat ~/.profile

- I like (your) data
- Playing “Active Defense”
- I prefer t-shirts than ties
- I like to play with gadgets!



\$ cat disclaimer.txt

“The opinions expressed in this presentation are those of the speaker and do not necessarily reflect those of past, present employers, partners or customers.”

Agenda

- **A Revolution Entered Our Homes**
- Internet of Nightmares
- Mitigations
- Conclusions

In
A Galaxy
No So Far
Away From Our
Modern World...

→ IN DE COMMUNICATION



RECHERCHE
PAR NOM
OU PAR RUBRIQUE



NOM: OFFICE DU TOURISME

OU
RUBRIQUE:

LOCALITE: DIJON.....

vous pouvez préciser
DEPARTEMENT: COTE D OR.....
ADRESSE:

PRENOM:

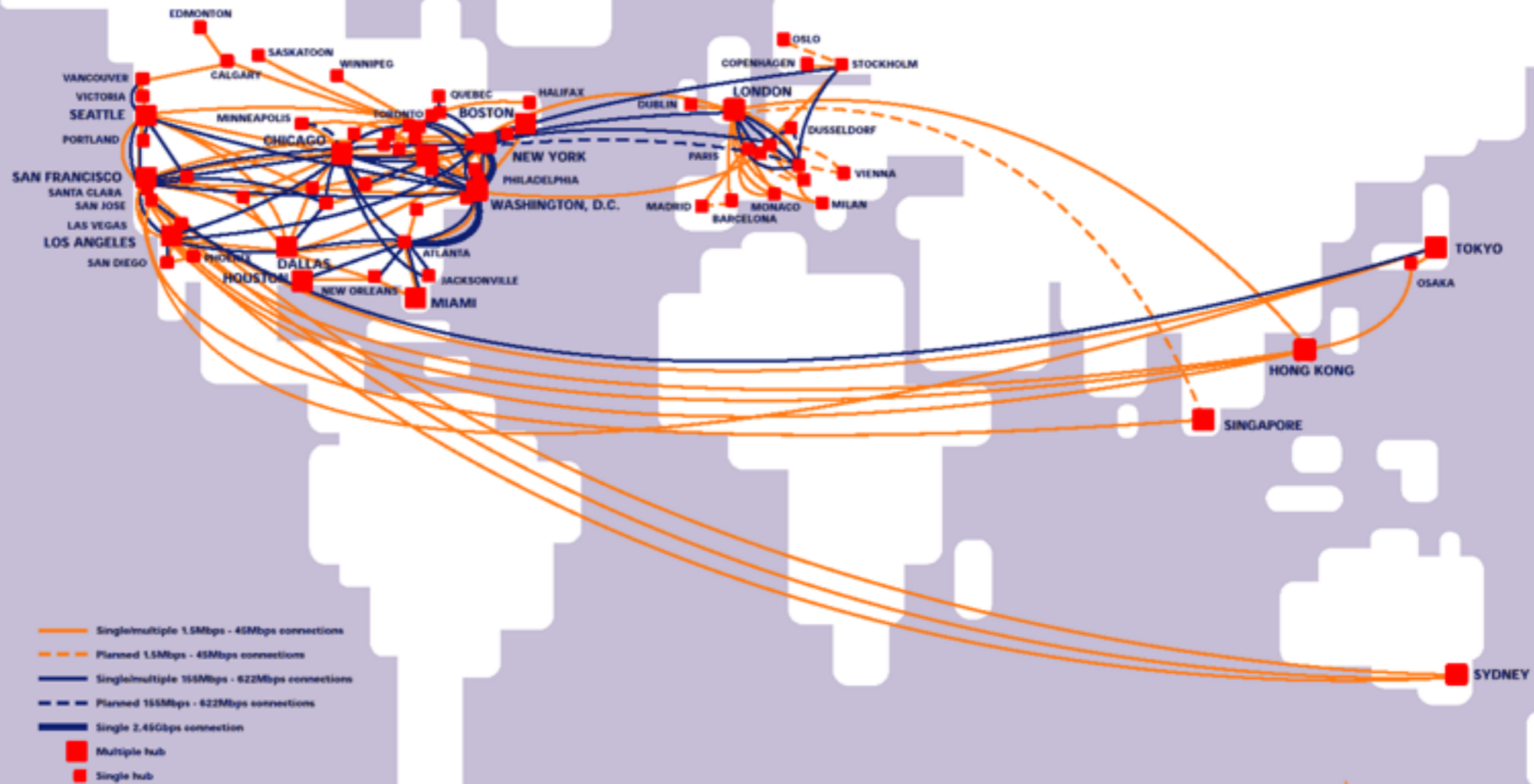
ligne suivante
ligne précédente
effacer
choisir dans une liste
obtenir la réponse

Suite
Retour
Correc.
Guide
Envoi





UUNET's Global Internet Backbone



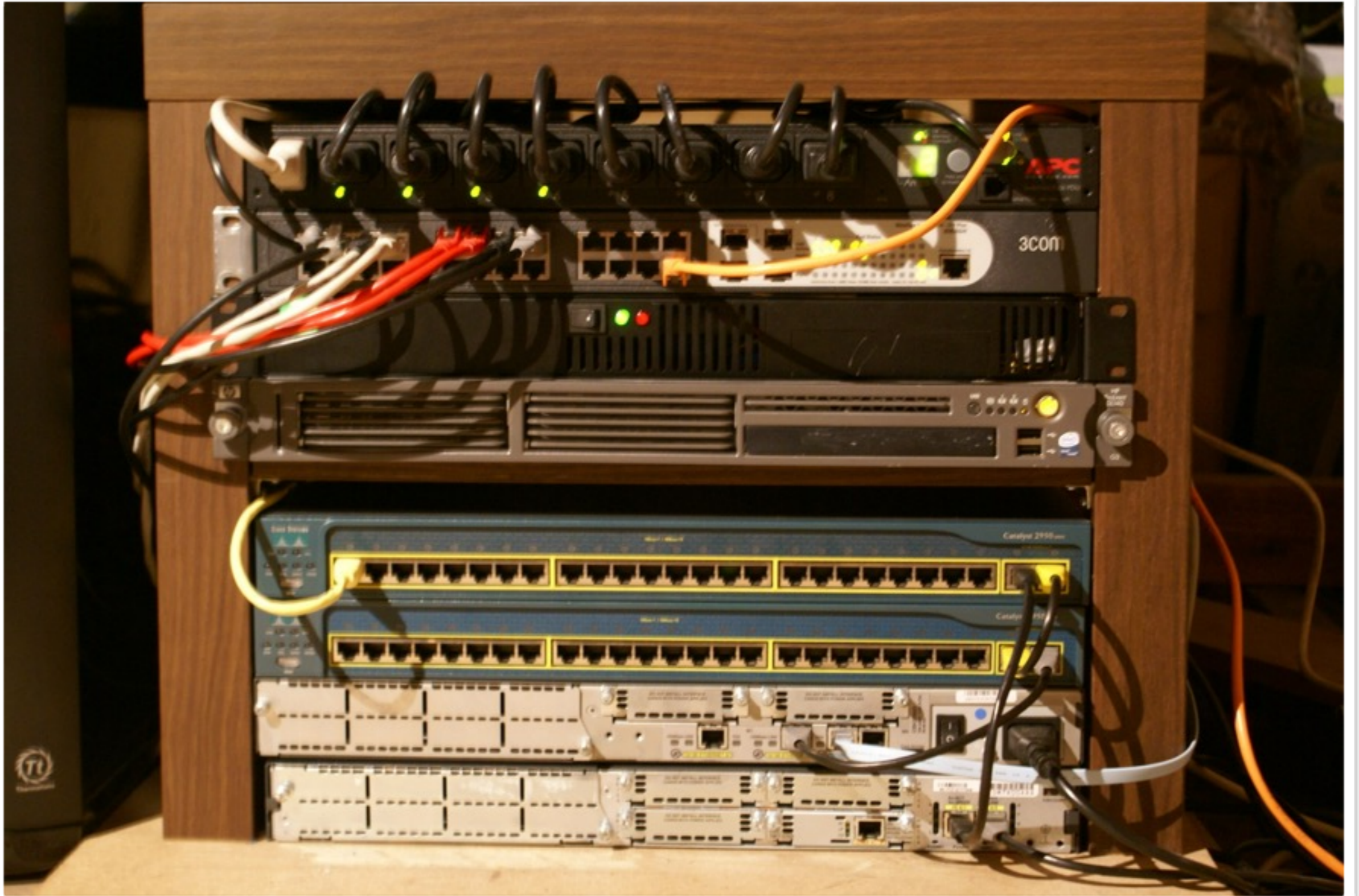
For more information visit www.uu.net

NB: With the exception of North America, Spain & Germany, all major 'in-country' links have been excluded from this map. 'In-state' links within the USA have also been excluded.

This does not constitute a solicitation of any former MCI customer whose dedicated Internet access service was transferred to Cable & Wireless unless the customer was also a WorldCom company Internet services customer as of the MCI/WorldCom merger.



Map/June 1999 2nd edition



CONNECT



ALL THE THINGS

memegenerator.net

#

i n i 1 5

BRILLO

foss **B**ytes

Agenda

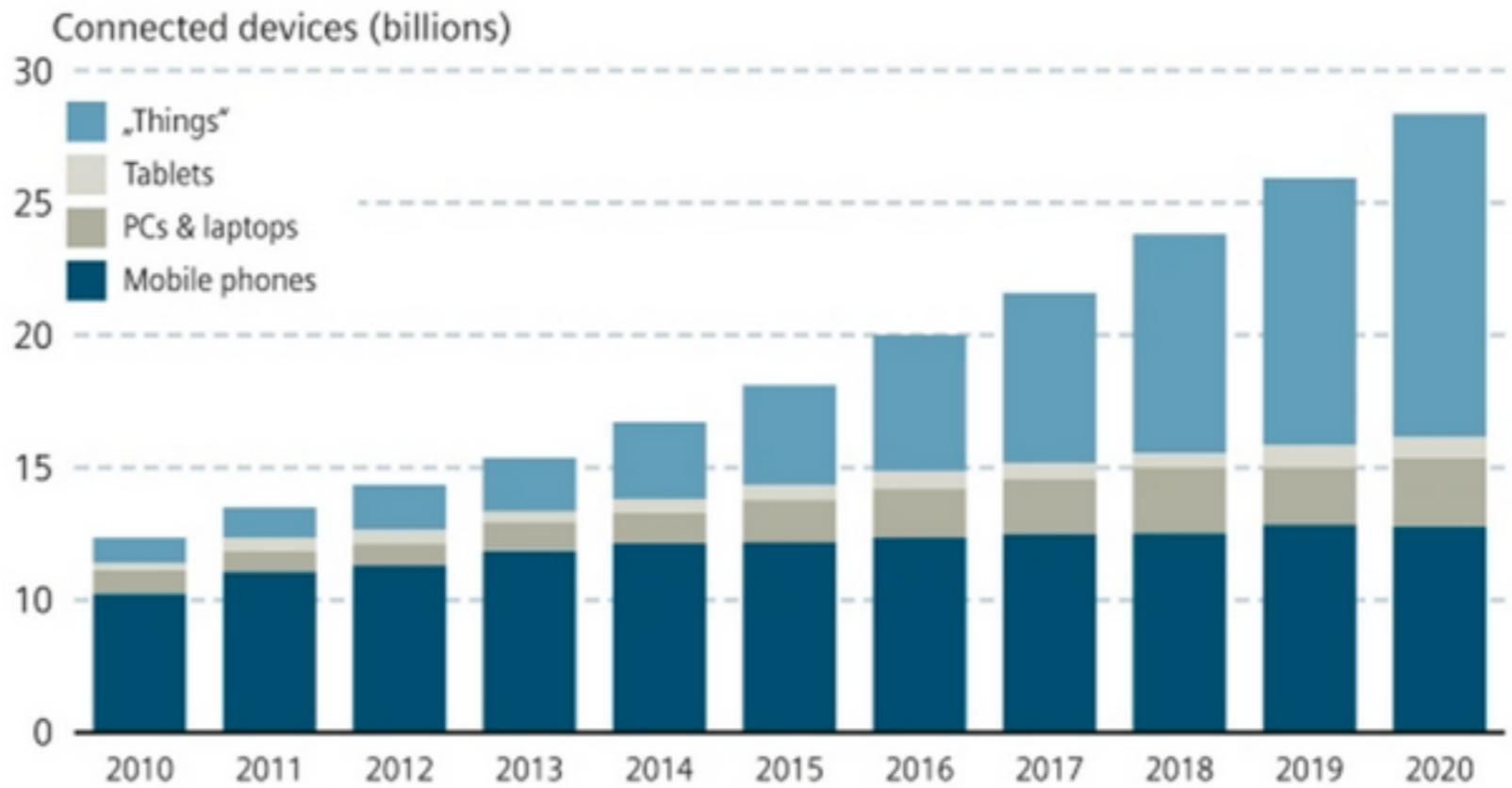
- A Revolution Entered Our Homes
- **Internet of Terrors**
- Mitigations
- Conclusions

Resistance is Futile!



Machines go Online

The number of everyday objects, or „things“, connecting to the Internet will exceed PCs and smartphones.



Source: The Internet of Things, MIT Technology Review, Business Report



Aris Adamantiadis

@aris_ada



Following

When watching "Hackers" nearly 20 years ago, I thought "sprinklers connected to the phone/internet, sure...Never gonna happen".
And then #IoT



RETWEET

1



1:46 PM - 15 Jun 2015



SMALL DATA

@small_data



Follow

Syslog messages from Internet of Things:
Alert Toilet: Tank missing 22oz of water
Notice dog water bowl: Water level is 10 of 10



RETWEETS

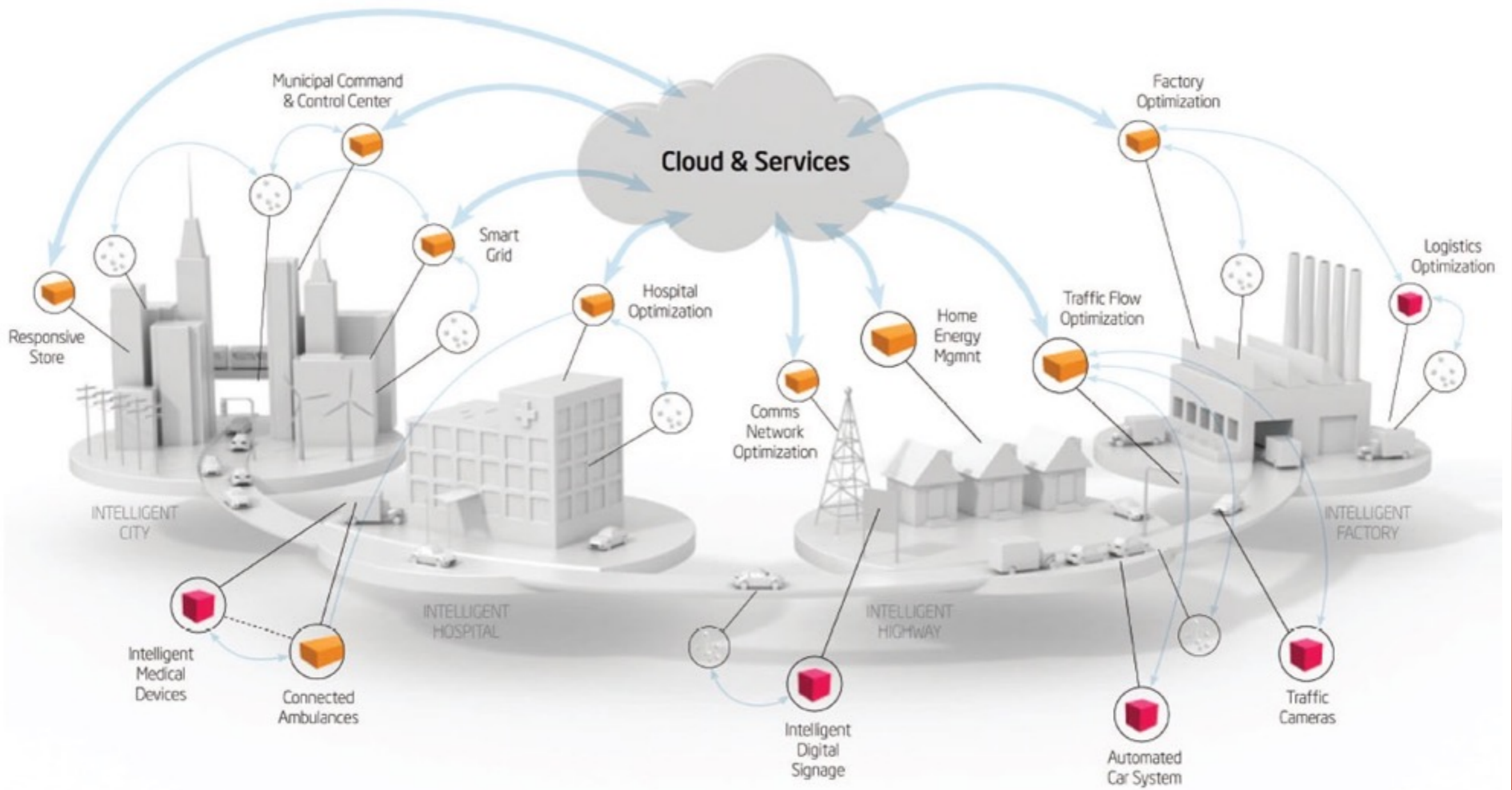
7

FAVORITES

8



10:36 PM - 27 Jun 2015



Source: Intel

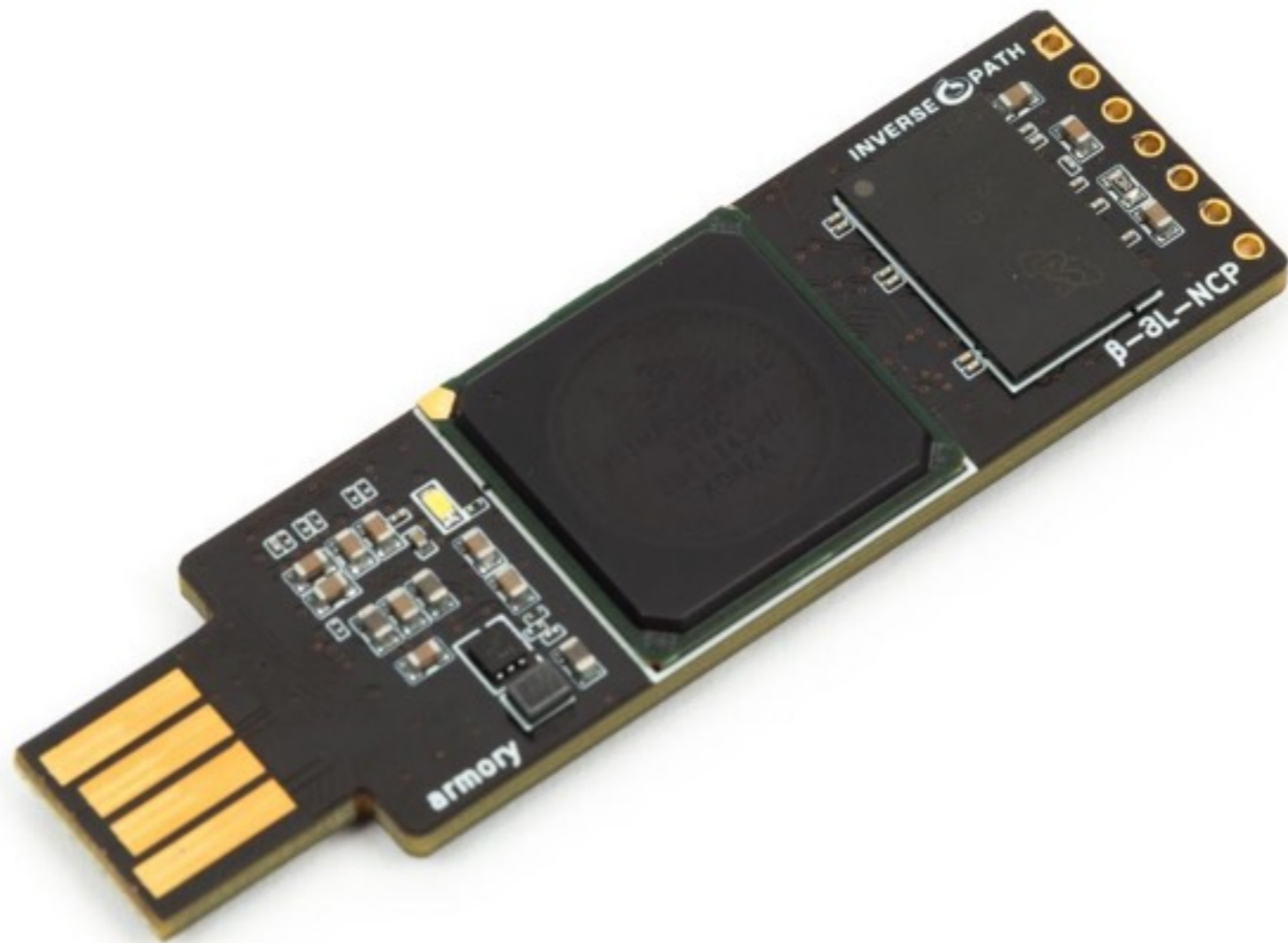
Table 1 - IoT Taxonomy

CATEGORY	TYPE
Personal Electronics	<ul style="list-style-type: none"> ● Fitness ● Toys ● Gadgets ● Other
Consumer Appliances	<ul style="list-style-type: none"> ● Large Appliances ● Small Appliances ● Entertainment ● Other
Home/Office Automation	<ul style="list-style-type: none"> ● External Home/Office ● Power Management ● HVAC ● Other
Security & Monitoring	<ul style="list-style-type: none"> ● Audio/Video ● Physical Locks ● Alarm System ● Environmental Monitors ● Other
Platform	<ul style="list-style-type: none"> ● IoT Management Platform ● Other

Source: OpenDNS The 2015 Internet of Things in the Enterprise Report

**What is the difference
between...**







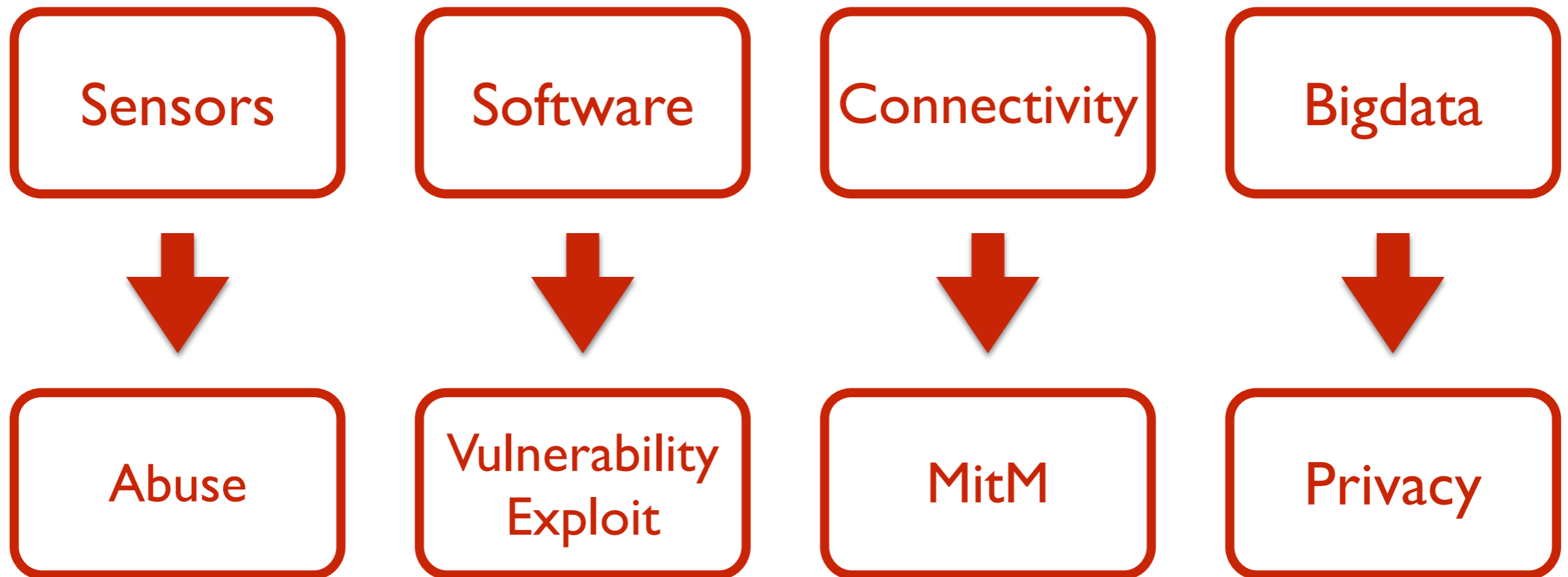
The **Internet of Things** (IoT, sometimes **Internet** of Everything) is the network of physical objects or "**things**" embedded with electronics, **software**, **sensors** and **connectivity** to enable it to achieve greater value and service by exchanging **data** with the manufacturer, operator and/or other connected devices based on the ...



[Internet of Things - Wikipedia, the free encyclopedia](https://en.wikipedia.org/wiki/Internet_of_Things)
https://en.wikipedia.org/wiki/Internet_of_Things



More about Internet of Things

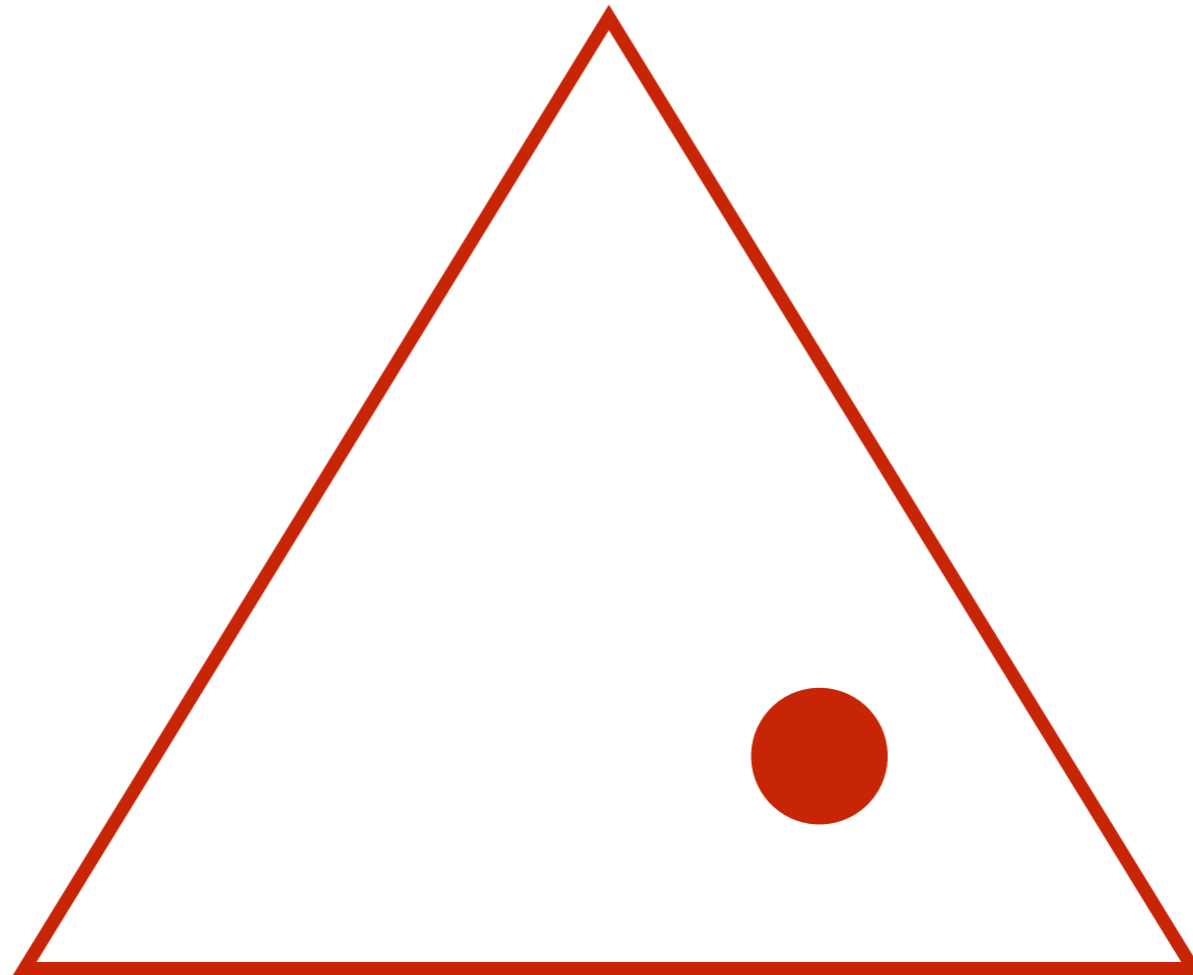


OWASP

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Ease of Use

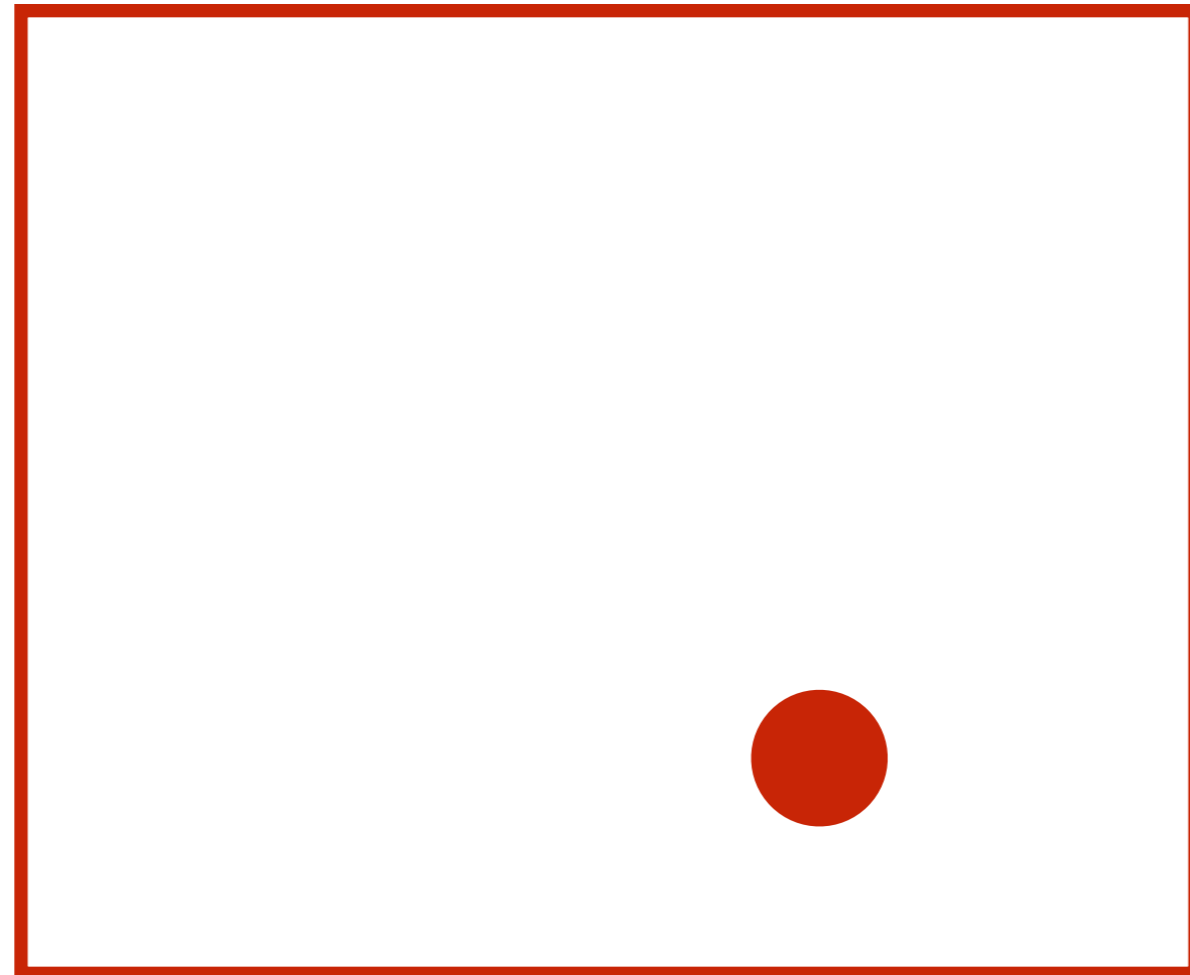


Features

Security

Business

Ease of Use



Features

Security

Smart Devices? Really?

In February 2015, the press discovered that if Samsung's Smart TV voice recognition system is activated, the television sends voice commands to Samsung and then to a third-party provider for processing. Any other conversations that are overheard are also sent. The company's user manual explains:¹

If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you.



TARGET

<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

Agenda

- A Revolution Entered Our Homes
- Internet of Terrors
- **Mitigations**
- Conclusions



<warning>

This section focuses on devices connected
to your IP home network

</warning>

Rule #1

- Implement an egress filter
- Any:Any to Any:Any, Drop & Log

Rule #2

- Assign a fixed DHCP lease to known devices

```
host myflattv {  
    hardware ethernet aa:bb:cc:dd:ee:ff;  
    fixed-address 192.168.1.100;  
    option routers 192.168.1.1;  
    default-lease-time 3600;  
}
```

Rule #3

- Use a local resolvers (DNS queries) and log

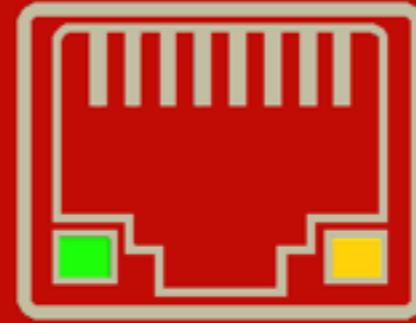
Rule #4

- Capture the traffic from unknown devices (<http://blog.rootshell.be/2015/03/17/the-lack-of-network-documentation/>)

Rule #5



- What is the MAC address of the device?
- What are the network requirements?
(DNS, NTP, SNMP, Syslog)
- What are the open ports required? To which IP address(es)?
- Can the device be upgraded?
- Are firmwares signed?
- Can we backup/restore the config?

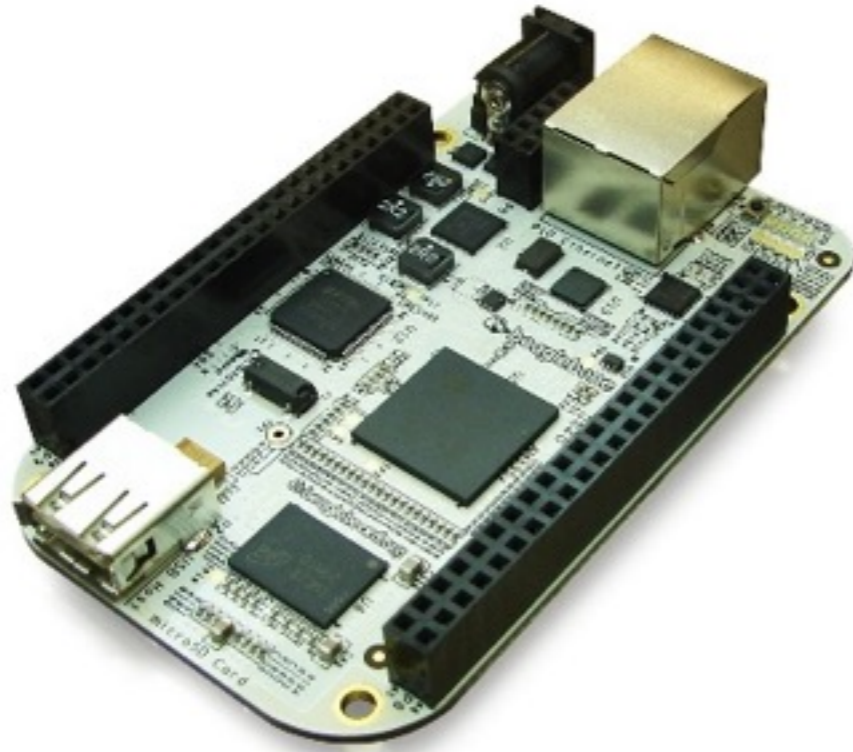


**KEEP
CALM
AND
SNIFF
PACKETS**

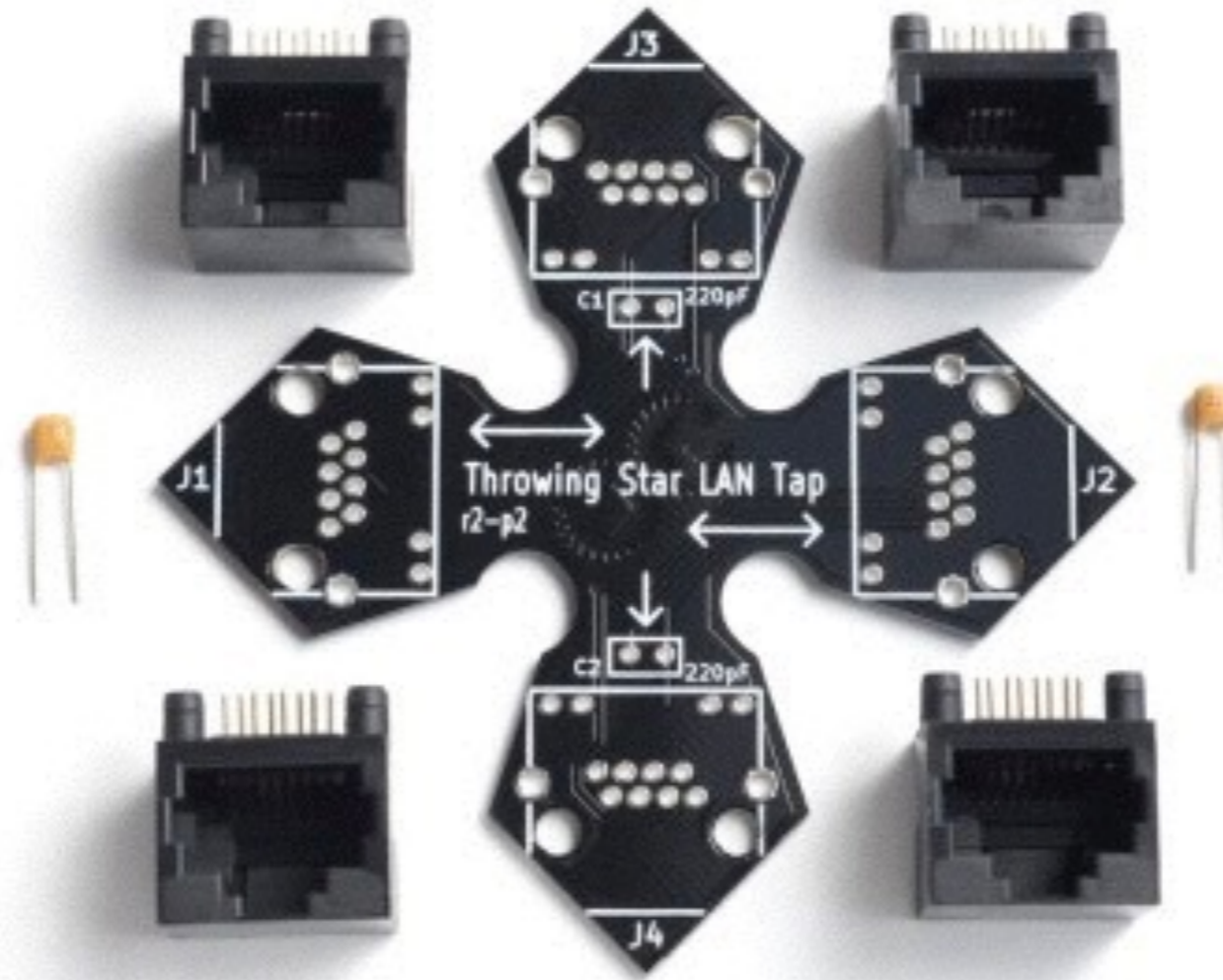
Hardware



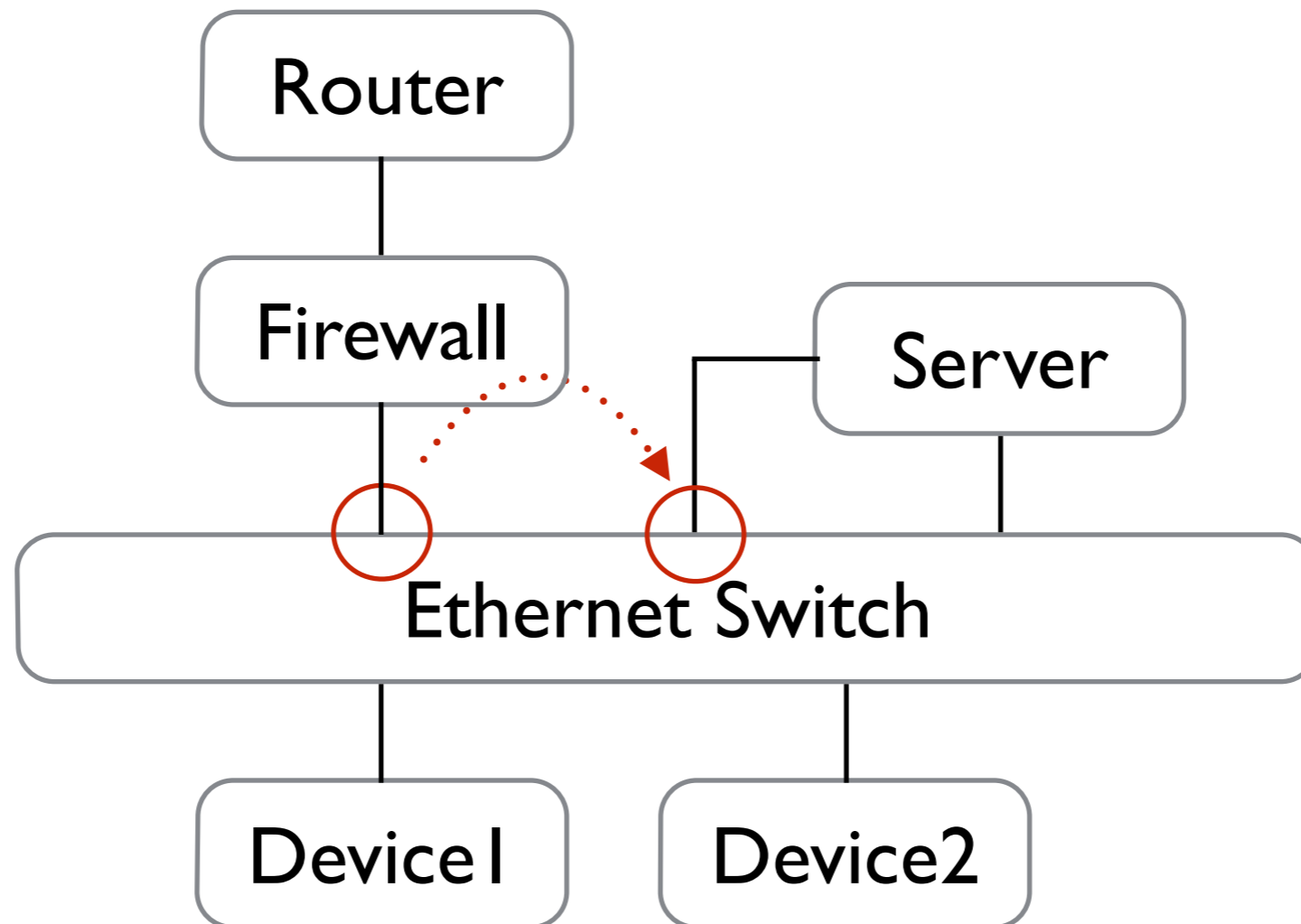
Hardware



Hardware

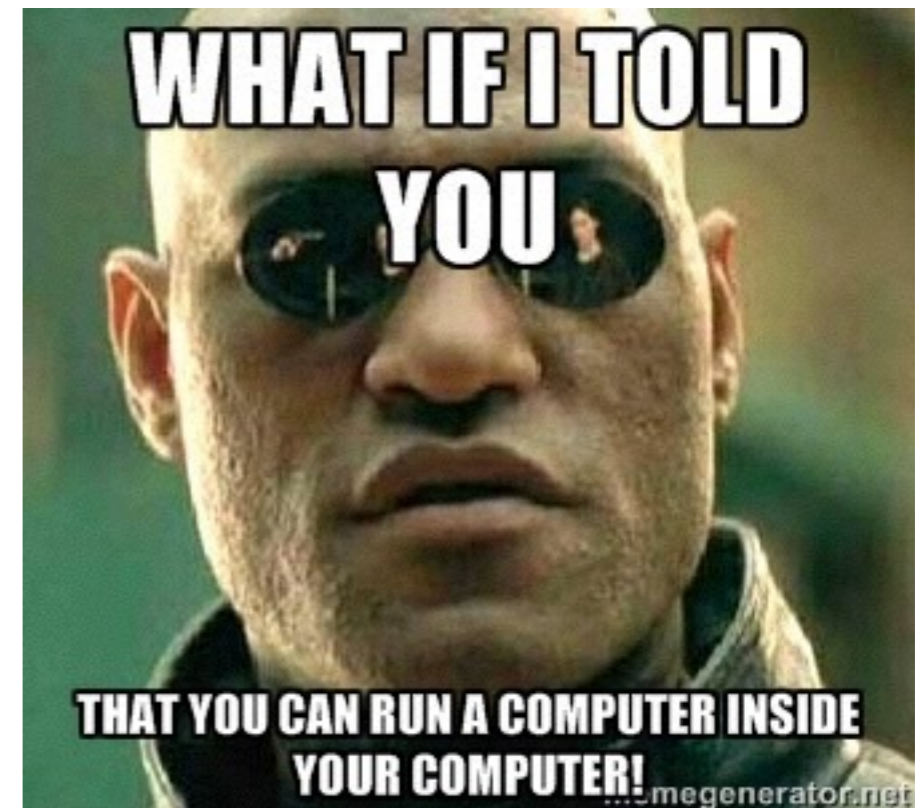


Topology



Virtualize!


KVM (“Kernel-based Virtual Machine”) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module that provides the core virtualization infrastructure and a processor specific module.



Security Onion

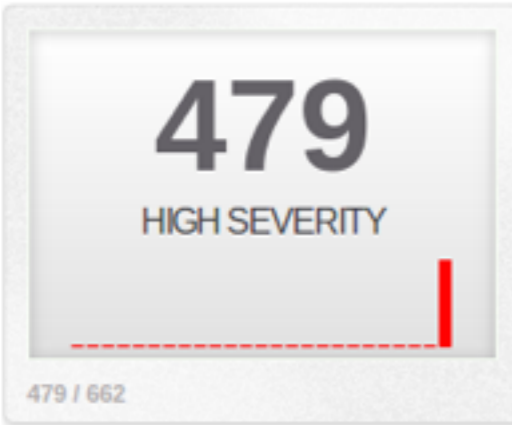
Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. Core components are: Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools.

Dashboard

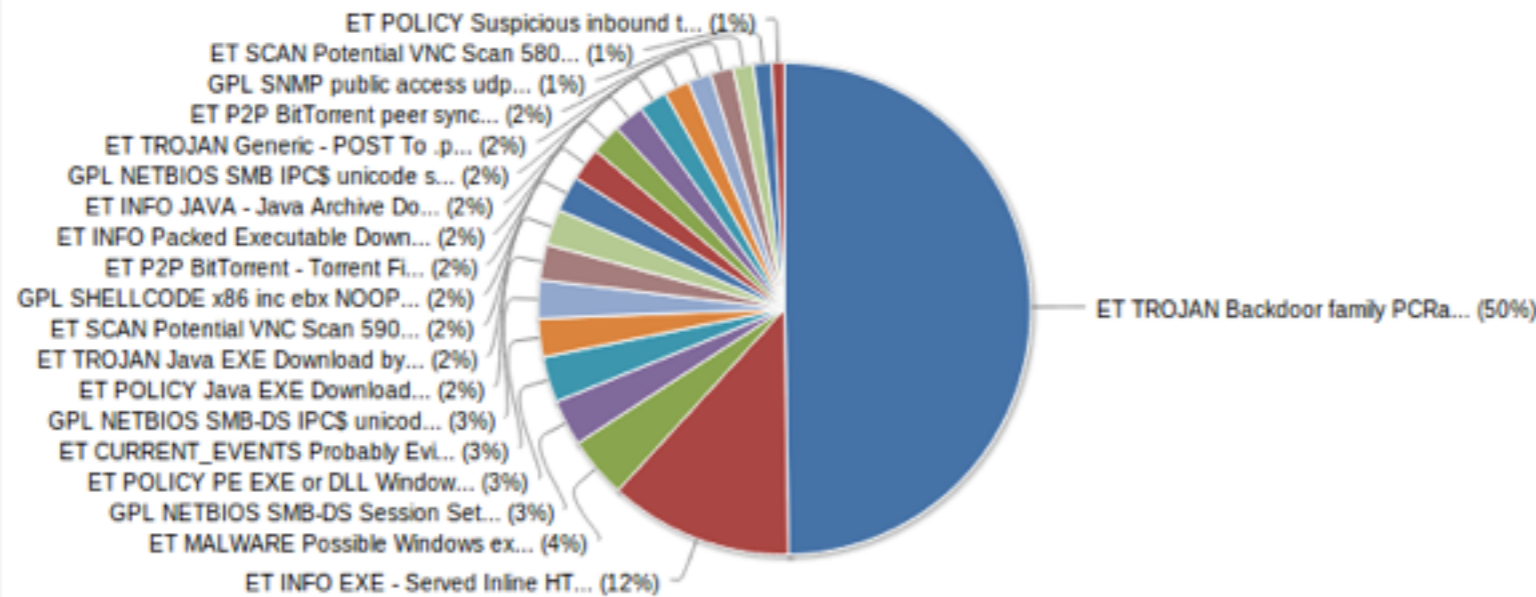
 More Options

LAST 24 TODAY YESTERDAY LAST WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 11/11/13 03:12 PM UTC



Sensors Severities Protocols Signatures Sources Destinations



TOP 5 SENSOR

doug-virtual-machine-eth1:1 1,200

TOP 5 ACTIVE USERS

Administrator 0

LAST 5 UNIQUE EVENTS

ET POLICY SUSPICIOUS *.do... 2

ET POLICY PE EXE or DLL W... 29

ET SHELLCODE Possible Cal... 6

ET INFO Exectuable Downlo... 2

GPL SHELLCODE x86 inc ebx... 23

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access 0

Unauthorized User Access 0

Attempted Unauthorized... 0

Denial of Service Attack 0

Policy Violation 0

Reconnaissance 0

Virus Infection 0

False Positive 0

Events Welcome doug | [Logout](#) [comments](#) [sensors](#) [filters](#)

< 2012 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2014 >

Timeline: 2013-11-06 00:00:00 until 2013-11-06 23:59:59 (+00:00) Filtered by Object: NO Filtered by Sensor: NO Status: Synchronized

Toggle

Event Grouping: on

Event Queue Only: on

Map: off

Event Summary

Queued Events: 518

Total Events: 900

Total Signatures: 32

Total Sources: -

Total Destinations: -

Event Count by Priority

High: 379 (73.2%)

Medium: 46 (8.9%)

Low: 72 (13.9%)

Other: 20 (3.9%)

Event Count by Classification

- Admin Access: -
- User Access: -
- Attempted Access: -
- Denial of Service: -
- Policy Violation: -
- Reconnaissance: -
- Malware: -
- No Action Req'd: 382 (42.4%)
- Escalated Event: -

History ^{u?}

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow.to_server,established; content:".doc.exe"; http_uri; nocase; classtype:bad-unknown; sid:2013475; rev:1;)

file: downloaded.rules:10836

categorize 0 event(s)

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
1		2013-11-06 13:05:54	172.16.150.20	RFC1918 (.b)	66.32.119.38	-unknown (-)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE	
RT	2013-11-06 13:05:54	3.5305	TX	172.16.150.20	1294	66.32.119.38	80	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL

Sensor Name: doug-virtual-machine-eth1-1

Timestamp: 2013-11-06 13:05:54

Connection ID: CLI

Src IP: 172.16.150.20 (Unknown)

Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)

Src Port: 1294

Dst Port: 80

OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)

OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)

OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /igers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1

SRC: Accept: image/gif, image/x-bitmap, image/png, image/jpeg, application/x-shockwave-flash, *

SRC: Accept-Language: en-us

SRC: Accept-Encoding: gzip, deflate

SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

SRC: Host: 66.32.119.38

SRC: Connection: Keep-Alive

SRC:

SRC:

DST: HTTP/1.1 200 OK

DST: Date: Fri, 27 Apr 2012 17:40:31 GMT

DST: Server: Apache/2.2.16 (Ubuntu)

DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT

DST: ETag: "42d3b-2000-4bda04a8ed053"

DST: Accept-Ranges: bytes

update

pfSense

The pfSense project is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality.

pfSense software, with the help of the package system, is able to provide the same functionality or more of common commercial firewalls



System Information

Name	fw1.
Version	2.1-RELEASE (386) built on Wed Sep 11 18:16:50 EDT 2013 FreeBSD 8.3-RELEASE-p11 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5310 @ 1.60GHz
Uptime	95 Days 18 Hours 37 Minutes 37 Seconds
Current date/time	Mon Dec 16 19:31:17 EST 2013
DNS server(s)	127.0.0.1 8.8.8.8 8.8.4.4
Last config change	Mon Dec 16 19:07:55 EST 2013
State table size	0% (364/100000) Show states
MBUF Usage	9% (2286/25600)
Load average	0.04, 0.06, 0.07
CPU usage	4%
Memory usage	22% of 1003 MB
SWAP usage	0% of 1024 MB
Disk usage	43% of 2.9G

Interfaces

WAN	↑ 1000baseT <full-duplex> 66.1 261
HOSTINGNET1	↑ 1000baseT <full-duplex> 172. 261
DEVNET1	↑ 1000baseT <full-duplex> 172 261
SYNC	↑ 1000baseT <full-duplex> 172
MGMT	↑ 1000baseT <full-duplex> 172 261

Traffic Graphs

Current WAN Traffic

In 77 Kbps 12/16/2013 19:31:20 [Switch to interface's AutoScale \(off\)](#) wan

Out 3.32 Mbps

Graph shows last 1200 seconds

Current HOSTINGNET1 Traffic

In 3.33 Mbps 12/16/2013 19:31:17 [Switch to interface's AutoScale \(off\)](#) lan

Out 74 Kbps

Graph shows last 1200 seconds

Keep an eye on ARP

- arpwatch is a nice tool to track new/ changing MAC addresses

```
Apr 17 11:36:03 shiva arpwatch: new station 10.90.14.85 34:a3:95:c5:d2:e5 eth0
```


OSSEC HIDS

To: ossec@rootshell.be

OSSEC Notification - (shiva) 192.168.254.8 - Alert level 7

OSSEC HIDS Notification.
2015 Jun 30 12:09:28

Received From: (shiva) 192.168.254.8->/var/log/syslog
Rule: 7209 fired (level 7) -> "Possible arpspoofing attempt."
Portion of the log(s):

Jun 30 12:09:27 shiva arpwatch: ethernet mismatch 192.168.254.217 7c:d1:c3:0a:67:f7 (34:51:c9:a8:a0:9a) eth0

--END OF NOTIFICATION

Next Level...

Detecting Suspicious Devices On-The-Fly!

(<https://isc.sans.edu/forums/diary/Guest+diary+Detecting+Suspicious+Devices+OnTheFly/18993>)

Agenda

- A Revolution Entered Our Homes
- Internet of Terrors
- Mitigations
- **Conclusions**

Five tips to keep in mind

- IoT is there and will(is) invade(ing) our homes
- Think “IoT” == “Computers” (same issues)
- Smart != Safe
- Tools exists to control them
- Ask yourself: “Do I need it?”

Thank you!

@xme

xavier@truesec.be

<http://blog.rootshell.be>

<https://www.truesec.be>

