PRACTICAL EXPERIENCES OF BUILDING AN IPFIX BASED OPEN SOURCE BOTNET DETECTOR

Mark Graham

Anglia Ruskin University
Cambridge & Chelmsford

OUTLINE

- RESEARCH PROBLEM: Botnet detection in Cloud Providers
- FLOW: IPFIX and NetFlow
- CONCEPTUAL FRAMEWORK: Build environment & challenges
- RESULTS
- CONCLUSIONS: Why do the results matter?

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

ABOUT ME…

- PhD Student at Anglia Ruskin University, Cambridge, UK
- Just passed my 2nd Year Confirmation on Candidature
- Supervisors: Adrian Winckles, Dr Erika Sanchez-Velazquez

Working PhD title:

"A Botnet Needle in a Virtual Haystack(s)"

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

RESEARCH PROBLEM

"To create a botnet detection mechanism for cloud service provider networks."

Why a CSP environment?

- IOT - Ease of access for centralised data
- Attacks - From the cloud, on the cloud

Build Criteria:

- Privacy - Cannot site AV in tenant environment
- Isolation - A tenant cannot access another tenant
- IPv6 - must support this next gen protocol

RESEARCH PROBLEM… ATTACKS ON CSPS

1) HOST ESCAPE

CRISIS MALWARE (2012)

2) INTRA-VM ATTACKS

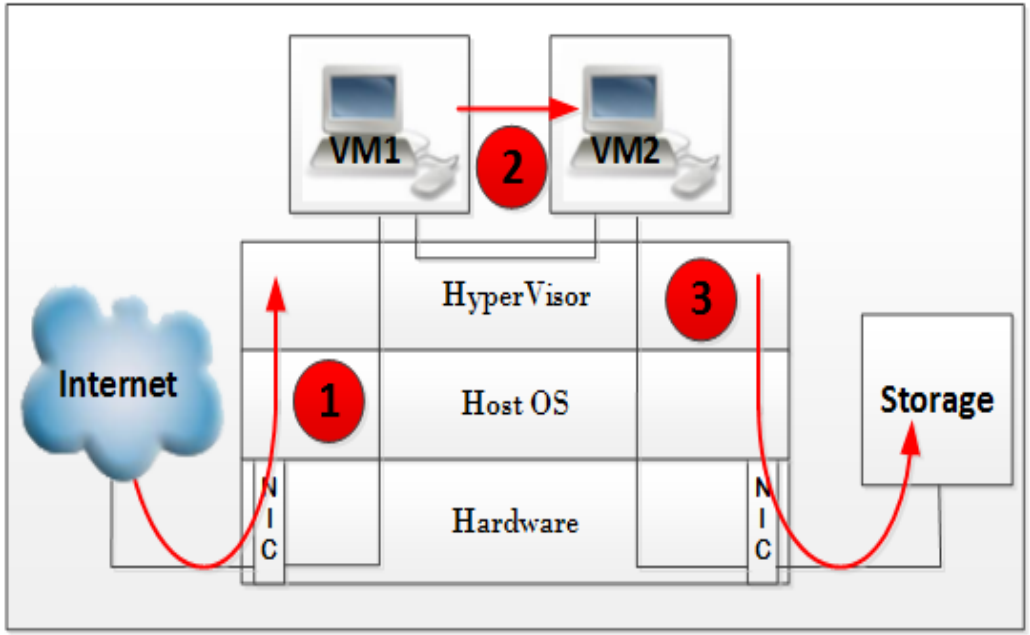
RISTENPART ET AL. (2006)

WANG & LEE (2006)

3) VM ESCAPE

CLOUDBURST MALWARE (2009)

VENOM (2015)



botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

A BRIEF HISTORY OF FLOW

- 1980 ‘s - SNMP
- 1990 ’s - Syslog
- 2002 - NetFlow v5 (Cisco)
- 2009 - NetFlow v9 (Cisco)
- 2013 - IPFIX (IETF Standard: RFC 7011- 7015)

botconf The botnet fighting conference 2015

Anglia Ruskin University
Cambridge & Chelmsford

WHY FLOW?

- Flows based on PDU header information

  1) Publically available metadata (v's PCAP does intrusive DPI)

  2) Data storage savings (3.1GB PCAP; 43KB in IPFIX)

  PCAP is a *phone call*; flow is the *phone bill* (who, when, how long)

- Traffic detection (v's forensic/signature detection)

  Botnet takedown requires locating C&C

- NFv5 + PCAP used in botnet detection research since 2007 as a data capture method to feed into detection algorithms:

  Bothunter, Botsniffer, Botcop, Botzilla, BLINC, etc.

IPFIX v NetFlow

IPFIX was developed to address the drawbacks of NetFlow:

- Standard: Vendor Neutrality
- Extensible: NFv5 – fixed template: 18 fields
  NFv9 - 79 fields (104 if Cisco)
  IPFIX - 433 fields (IANA)
- Protocol: NF is UDP; IPFIX supports UDP / TCP / SCTP (TLS)
- Security: IPFIX has C.I.A by design; including data obfuscation
- Next Gen: IPFIX supports IPv6, MPLS and multi-cast

Caveat: Cisco NFv9 support some of these, but proprietary

CRITERIA FOR "DATA CAPTURE" ELEMENT

- Cloud and IoT provider virtualised environments
- Respect cloud tenant data privacy (?)
- COTS & open source
- Feed into a neural network; which feeds into SDN / VM containment
- Ideally support NetFlow and IPFIX for experimental comparison

CONCEPTUAL DESIGN: VIRTUALISATION PLATFORM

1) Hypervisors:

- **Xen (Citrix)**, *Hyper-V (Microsoft), ESXi (VMWare)*

  Xen: Open Source

  Xen: Common in CSPs (AmazonAWS, OpenStack, Apache CloudStack)

  Xen: Full Para-virtualisation

2) Software Switches:

- **OVS (Open vSwitch)**, *Hyper-V, Nexus (Cisco), vSwitch (VMWare)*

  OVS: Open Source

  OVS: Exports IPFIX, NetFlow v5/v9 and sFlow

  OVS: Sits well with Xen Hypervisor

EXPERIENCE OF BUILDING THE SYSTEM #1

Citrix XenServer 6.2.0:

- OS: Linux Centos v5.5 i386
- Hypervisor: Xen v4.1.5
- Hypervisor Mgmt: XenCentre (GUI)
- Virtual Switch: Open vSwitch v1.4.6

This worked fine for NetFlow v5, but…

EXPERIENCE OF BUILDING THE SYSTEM #1

1. XenCentre GUI does not support IPFIX

   OK - we could use command Line XAPI Toolstack

2. Open vSwitch only supports IPFIX on v1.10+

   We have OVS v1.4.6

3. Open vSwitch v1.10 requires Centos 5.5 i686

   We have Centos 5.5 i386 - ok, lets upgrade

   XenServer partitions DOM0 into 4GB, of which 3.8GB is used by Xen.

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

EXPERIENCE OF BUILDING THE SYSTEM #1

1. XenCentre GUI does not support IPFIX

   OK - we could use command Line XAPI Toolstack

2. Open vSwitch only supports IPFIX on v1.10+

   We have OVS v1.4.6

3. Open vSwitch v1.10 requires Centos 5.5 i686

   We have Centos 5.5 i386 - ok, lets upgrade

   XenServer partitions DOM0 into 4GB, of which 3.8GB is used by Xen.

I am not a Citrix expert…

Centos refused to be upgraded

EXPERIENCE OF BUILDING THE SYSTEM #2

Citrix XenServer Creedence v6.5:

- OS: Linux Centos v5.10 i686 ✔
- Hypervisor: Xen v4.4 (64 bit) ✔
- Virtual Switch: Open vSwitch v2.1.2 ✔

  Supports IPFIX

  But, IPFIX would not export timestamps

  And IPFIX would not aggregate

EXPERIENCE OF BUILDING THE SYSTEM #2

Citrix XenServer Creedence v6.5:

- OS: Linux Centos v5.10 i686 ✔
- Hypervisor: Xen v4.4 (64 bit) ✔
- Virtual Switch: Open vSwitch v2.1.2 ✔
  - Supports IPFIX
  - But, IPFIX would not export timestamps
  - And IPFIX would not aggregate

I am not an OVS expert…

OVS refused to work with IPFIX

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

EXPERIENCE OF BUILDING THE SYSTEM #3

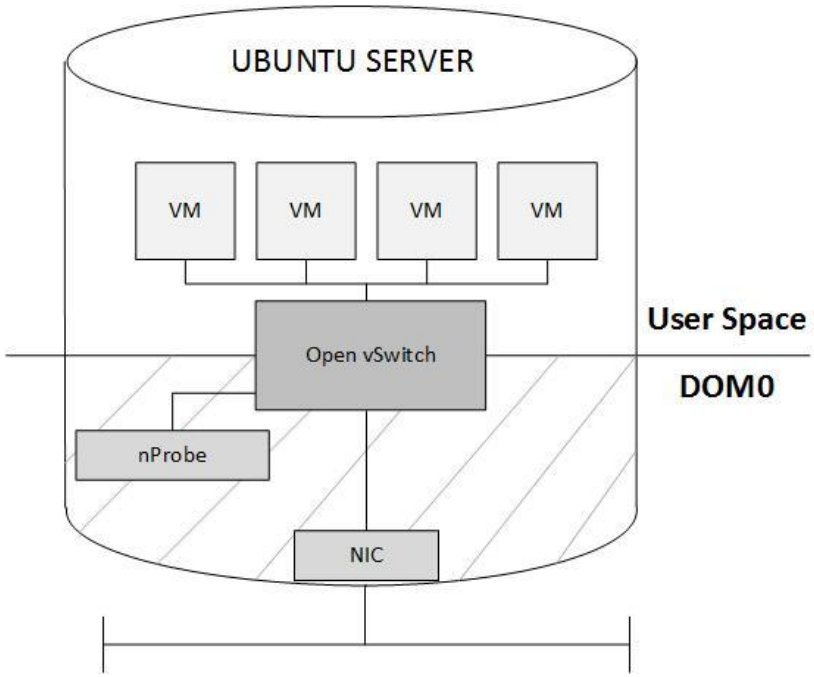
Mark's Bespoke Build v1.0:

- OS: Ubuntu 14.04 ←***NEW OS***
- Hypervisor: Xen Project v4.4 (64 bit) ←***STANDALONE***
- Hypervisor API: XAPI Toolstack ←***ADDITION***
- Virtual Switch: Open vSwitch v2.0.2 ←***DOWNGRADED***
- IPFIX Exporter/Collector: nProbe v6.15 ←***ADDITION***

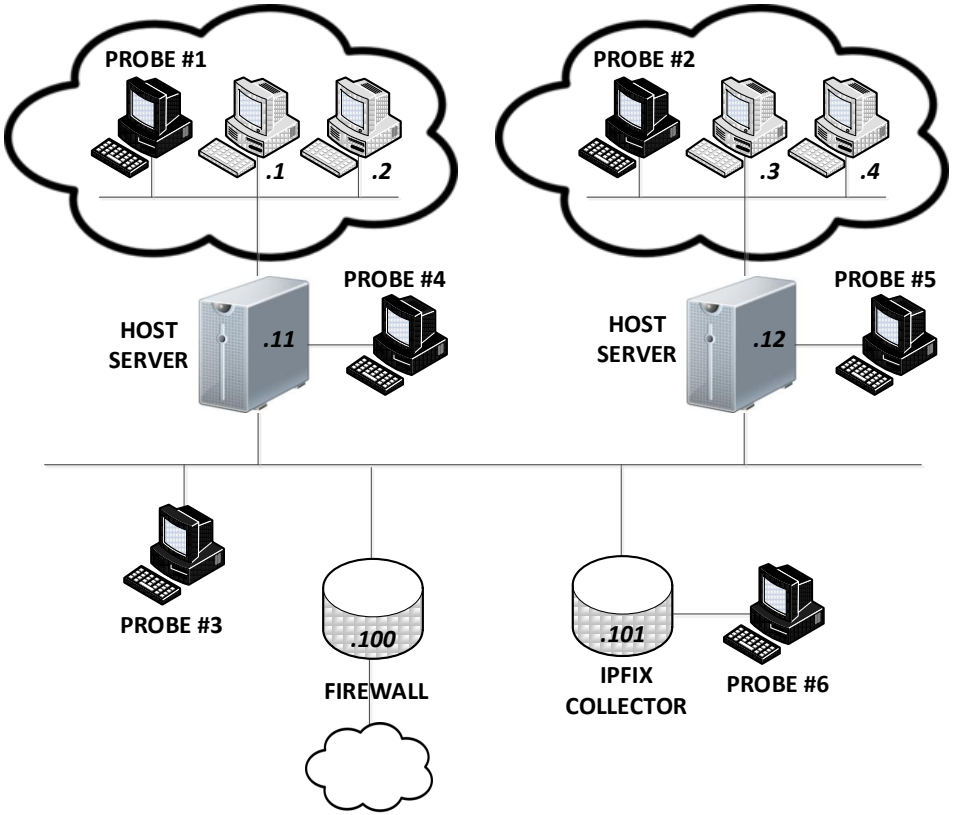
3 HOUR TOTAL INSTALL

CLOUD STACK:

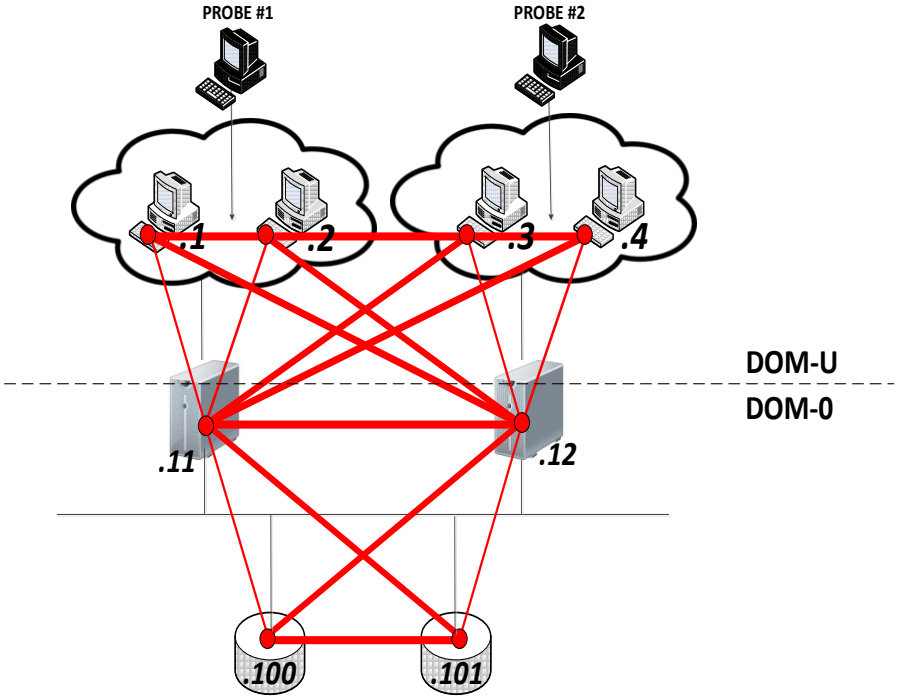
DOM-0 OS	Ubuntu 14.04
Hypervisor	Xen 4.4 (64 bit)
Hypervisor API	XAPI Toolstack
Virtual Switch	Open vSwitch v2.0.2
Flow Exporter	nProbe v6.15
Flow Collector	nProbe v6.15
VM Management	XenCentre v6.5
Flow Protocol Support	NetFlow v5 NetFlow v9 IPFIX
Flow Traffic Presentation	Neo4J

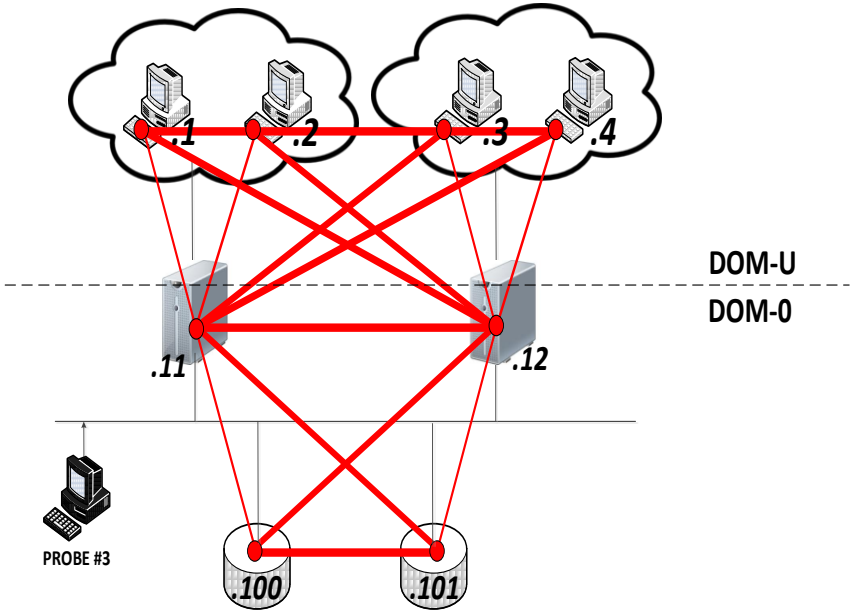


PROBE LOCATION



PROBE LOCATION

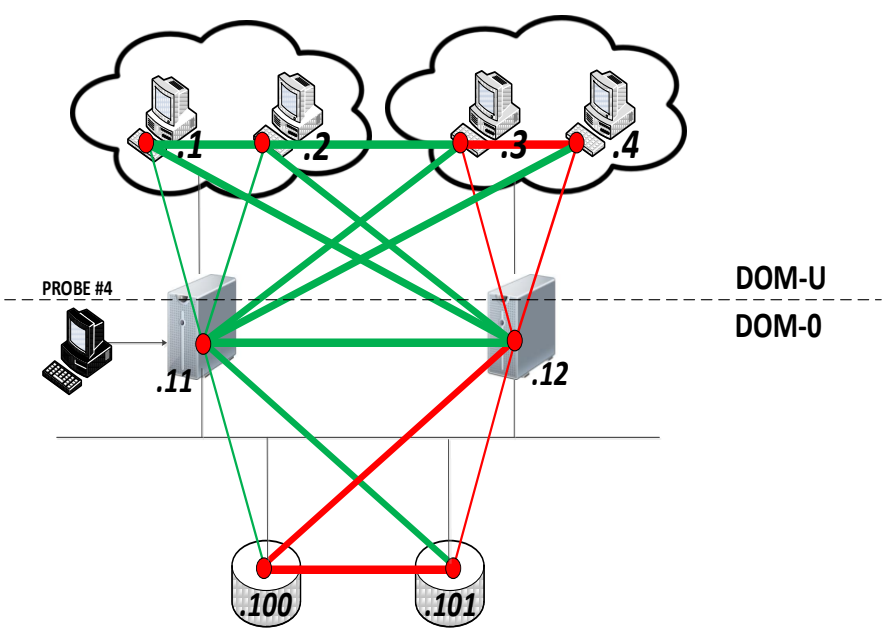


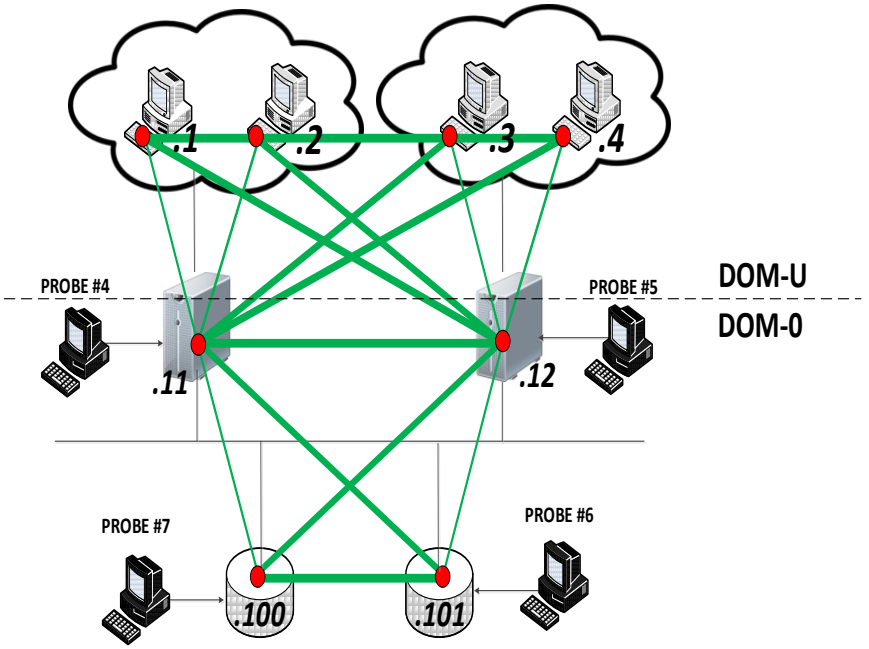


botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

PROBE LOCATION





botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

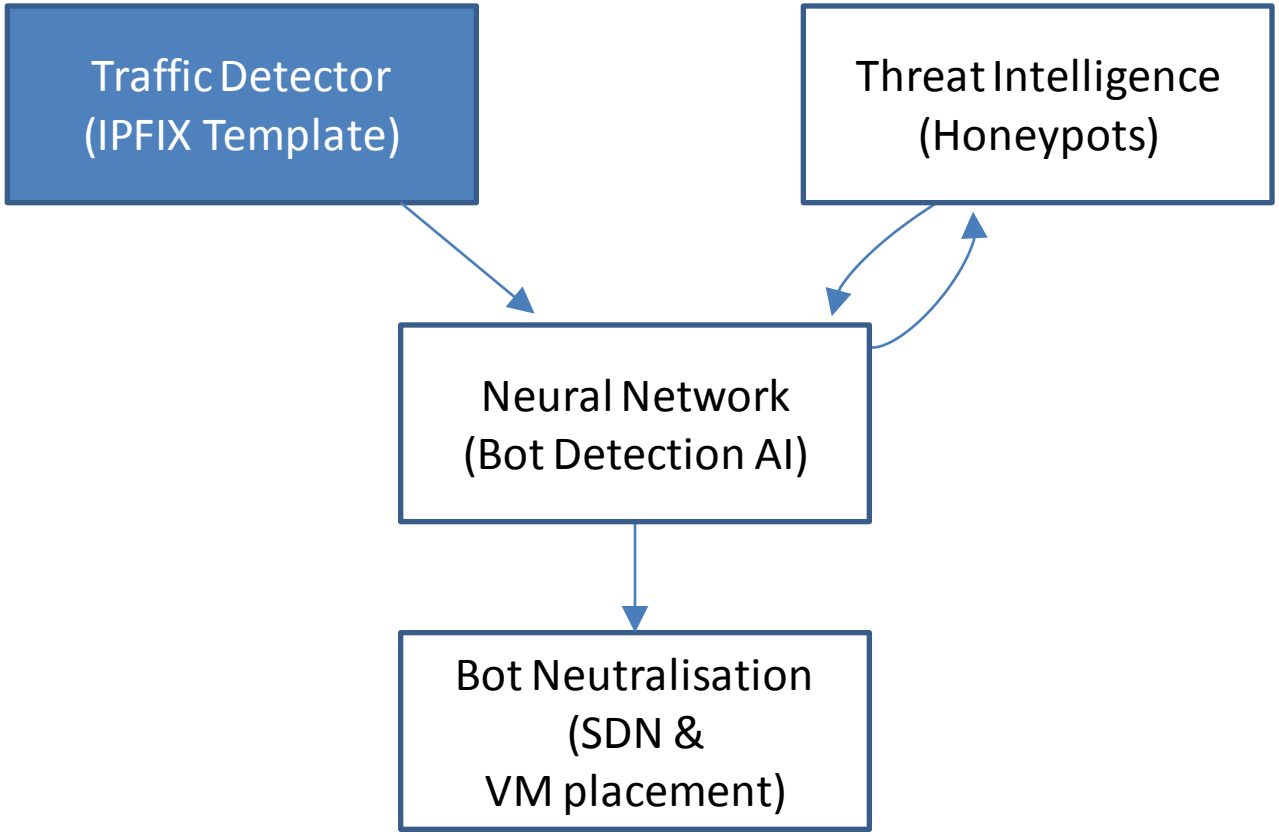
CURRENT WORK: IPFIX TEMPLATE

Version: 10 (2)	Length (2)
Export Time Stamp = 2015-01-01 12:59:59 (4)	
Sequence Number = 0 (4)	
Observation Domain ID = 123456 (4)	
Set ID = 1 (2)	Set Length (2)
Template ID = 456	Field Count = 8
Flow_Start_MilliSeconds = 152	Field Length (4)
Flow_End_MilliSeconds = 153	Field Length (4)
IN_Bytes = 1	Field Length (4)
IPv4_DST_Addr = 12	Field Length (4)
L4_SRC_Port = 7	Field Length (2)
L4_DST_Port = 11	Field Length (2)
Protocol = 4	Field Length (1)
BiFlow_Direction = 239	Field Length (1)

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

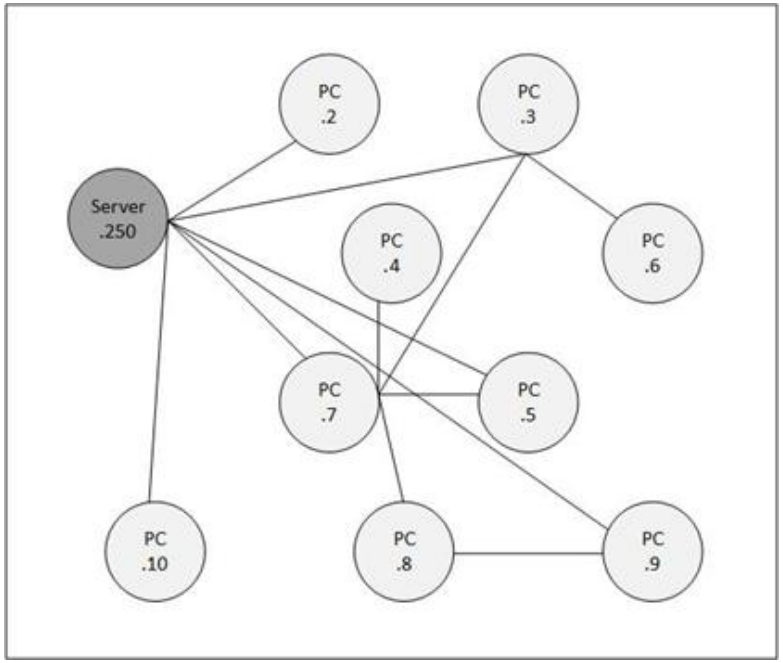
FUTURE WORK: CSP NEUTRALISATION ECO-SYSTEM



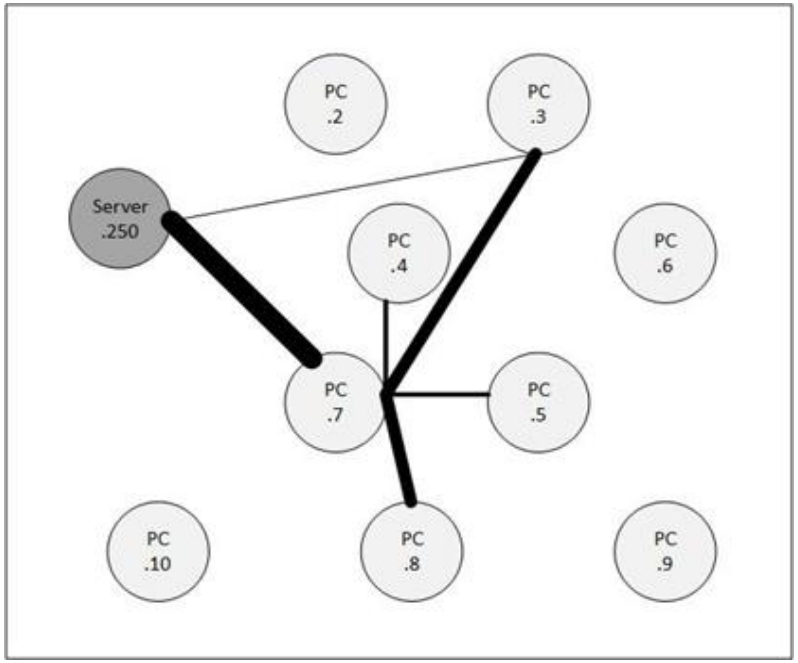
botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

FUTURE WORK: VISUALISATION



All Protocols



HTTP Only

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

LIMITATIONS OF THE SYSTEM

- **Deep Packet Inspection**

  Discarding the payload for privacy comes at a cost:
  - Can you detect botnets without DPI information? … (Probably not)
  - IPFIX allows customisable Information Elements to capture DPI information

    We have developed a DPI template: HTTP, DNS, SMTP & IRC.
  - Where is the cross-over with tenant privacy? … (Need to measure to detect)

- **Encryption / VPN Traffic**
  - Payload encryption wont impact traffic communication graphs
  - But encrypted PDU headers within a VPN will impact collection

CURRENT WORK: EXTENDED IPFIX TEMPLATE

Version: 10 (2)	Length (2)
Export Time Stamp = 2015-01-01 12:59:59 (4)	
Sequence Number = 0 (4)	
Observation Domain ID = 123456 (4)	
Set ID = 1 (2)	Set Length (2)
Template ID = 457	Field Count = 11
DNS ID	...
DNS TTL	...
DNS Query Name	...
DNS IP Address	...
HTTP GET	...
HTTP Referer	...
HTTP Location	...
HTTP Age	...
HTTP Cookie	...
HTTP Set Cookie	...
HTTP Via	...

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

CONCLUSION

Using COTS technology we created a botnet traffic capture mechanism:

- 80%+ CSPs already collect flow traffic for network management
- Probe must be located on the hypervisor
- IPFIX template for botnet detection

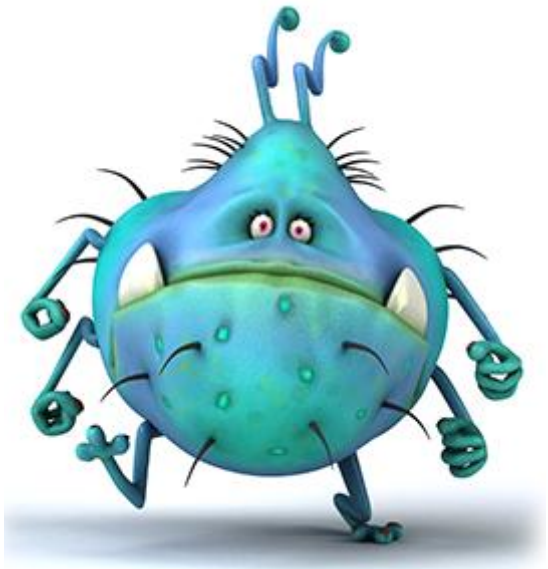
Clouds will host IoT and Smart Cities:

- Cloud is an attack platform (ideal breeding ground of botnets)
- Cloud is an attack target (storage, other tenants, VE malware)
- Traditional AV is not suited for botnets

botconf 2015
The botnet fighting conference

Anglia Ruskin University
Cambridge & Chelmsford

THANK YOU



mark.graham@anglia.ac.uk