D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures
Prof Bill Buchanan, Richard Macfarlane, Flavian Flandrin, Dr Jamie Graves, Dr Lu Fan, Dr Elias Ekonomou, Niladri Bose, Robert Ludwinia, Edinburgh Napier University
Scottish Centre of Excellence in Security and Cybercrime

- Vendors (EnCase CoE)
- Public sector: NHS, Social Care, etc
- Funders, Government
- Industry: Large (Dell SecureWorks) to SMEs
- Academia: Most of the universities in Scotland
- Law Enforcement: SCEDA, SIPR

The Scottish Institute for Policing Research

Engagement
Real Data Corpa (RDC)

Non-changing environment

Law enforcement training

Student training

Vendor tool analysis

Static capture

```
c:\forensics>bulk_extractor.0.1.0.exe images.bin -o test1
phase 1.
    Input file: images.bin
    Output directory: test1
    Reading raw file at offset 12576768/12582912... Done in
    00:00:00Phase 2. Report
    ng dir: test1

    c:\forensics>cd test1

    c:\forensics\test1>dir
    Volume in drive C is BOOTCAMP
    Volume Serial Number is BCC0-257A

    Directory of c:\forensics\test1

    01/09/2011  11:05                0  cons.txt
    01/09/2011  11:05                81  domains.txt
    01/09/2011  11:05               111  emails.txt
    01/09/2011  11:05                0  emails histogram.txt
    01/09/2011  11:05               21  rfc822.txt
    01/09/2011  11:05            337,898  wordlist.txt

      6 File(s)        338,111 bytes
     2 Dir(s)        1,620,799,488 bytes free

    c:\forensics\test1>head emails.txt
    10425618        per.ogren@sonyericsson.com
    10470675        per.ogren@sonyericsson.com
    10589305        per.ogren@sonyericsson.com
```
Training Issues:
- Lack of standardized images of training.
- Lack of engagement from industry/law enforcement.
- Environment is fairly static and not changing.
- Students not exposed to a wide range of tools and environments.
- Lack on training on real-life environments.
- Physical location can restrict training opportunities.
- And so on.

Validation Issues:
- Lack of validation for tools, especially for closed-source ones.
- No standardized framework for evaluation.
- Lack of repeatability.
- No standardization for the quality of digital forensics tools.
- Simulators suffer from not being realistic enough.
- And so on.
Community Cloud

- Overview for Cloud Computing.
- How Cloud Infrastructures could be used for teaching to enhanced skills.
- D-FET – A Community Cloud.
- Example used within teaching.
Community Cloud

D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> Overview in Cloud Computing

Author: Prof Bill Buchanan
Introduction

Changing trends

Mainframe

Computers connect to services (SoA)

Servers

Stand-alone computers

Computers connected to servers

Terminals
Private Cloud – owned and run by an organisation

Community Cloud – shared by several organisation, with a common policy, compliance, mission, etc

Public Cloud – owned by an organisation selling a cloud infrastructure

Hybrid Cloud – two or more clouds
**On-demand self-service.** Consumers get server CPU, memory, bandwidth and storage resources whenever required.

**Rapid elasticity.** Consumers can easily scale-up and scale-down, whenever required.

**Location independent resource pooling.** Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

**Pay per use.** All access to resources is monitored, and paid for either by advertising or usage. Payment methods: per users created, per hour usage (service), etc.
Audit/compliance
Can I be compliant with statutory and regulatory requirements?
- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

- Security: 74.8%
- Performance: 63.1%
- Availability: 63.1%
- Hard to integrate with in-house IT: 61.1%
- Not enough ability to customize: 55.8%
- Worried on-demand will cost more: 50.4%
- Bringing back in-house may be difficult: 50.0%
- Regulatory requirements prohibit cloud: 40.2%
- Not enough major suppliers yet: 44.3%
**Amazon CloudFront**
This allows content to be placed close to the places where it is to be consumed, the content thus gets moved to the edge of the cloud to support rapid delivery of content.

**Amazon SimpleDB**
This produces a mixture of structured data storage with the reliability of a traditional database.

**Amazon Elastic Cloud Compute (Amazon EC2)**
This is the core of the Amazon Cloud, and provides a Web services API to create, manage and delete virtual servers within the Amazon Cloud. This includes US, Asia (Japan and Singapore) and European data centres (Ireland), and uses the Xen hypervisor for the management of the servers.

**Amazon Simple Storage Service (Amazon S3)**
This provides data storage with web services through APIs. It differs from normal filesystems in that it does not have a hierarchical structure. Instead it uses buckets, which are unique namespaces across all of the Amazon customers. It is thus not a filesystem, and is a Web service, thus applications need to be written which specifically store data into the S3 Cloud.

**Amazon Virtual Private Cloud (VPC)**
This allows for complete network infrastructures to be built, which are isolated from other network infrastructures.
Amazon Machine Images (AMI)

$ ec2-describe-images -o AKIAIWUMTTAZYST2I2AA
$ ec2-describe-images
IMAGE ami-45c22e2c powerdns/image.manifest.xml 495219933132 available private
$ ec2-run-instances i-0d895566
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> How Cloud Computing could be used to enhance skills
Paravirtualisation. Guest OS communicates with a Hypervisor (KVM, Xen, etc). Bare Metal Virtualisation: VMware ESX/ESXi, Citrix XenServer, Microsoft Hyper-V
Downside: Guest OS requires modification, and makes them least compatible
Upside: Fastest of the methods
Public Sector
- Evaluation of systems.
- Training.

Government
- Define standards
- Evaluate products

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.

Industry
- Training/sharing materials.
- Professional certification

Academia
- Training/sharing materials
- Virtualised environments

Software Vendors:
- Test environments.
- Promoting products.
- Providing floating licences

Public clouds

Existing Academic Clouds
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> D-FET – A Community Cloud
Scottish Police
- Triage systems
- Training

Government
- Define standards
- Evaluate products

Industry
- Training/sharing materials.
- Professional certification

Academia
- Training/sharing materials
  - Virtualised environments

D-FET: e-Forensics Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

Digital Forensics Vendors
- Test environments.
- Promoting products.

Cloud@Napier
- links to existing Clouds
Distance learners
- Exact environments as face-to-face students.
- Blended learners have greater choice and flexibility.

Enhancing skills
- Supports a wide range of pre-built environments within a sandboxed infrastructure.

Working across institutions
- Cloud environments allow for working across traditional boundaries.

Project work
- Students can start from existing well-tested environments.

Engaging students
- State-of-the-art infrastructures

Group working
- Students can integrate their systems in an isolated environment.

Robust infrastructures
- No more 9-5pm, Mon-Friday environments.

Industry
- Adding evaluation infrastructures.
- Post project work/interesting areas of work.
- Ability to review materials presented to students.
- Ability to study within the workplace.

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

Continuation of work
- Students can carry their infrastructures throughout modules/years.

Snap-shots of work
- Student can create snap-shots, and move back and forward amongst them.
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> Example used in teaching
Difficult to use many of the techniques within a real-life space.

Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures.

Demands on professional certification.

Employers now require in-depth knowledge and a range of skills.
Virtualised and Cloud-based labs (AWS):
- Range of state-of-the-art operating systems and tools.
- Evaluation of Public Cloud resources.

Teaching of four modules in computer security, digital forensics and database systems for 2010/2011 (inc. Host-based Forensics, Security and Forensic Computing and Adv Security and Digital Forensics at BEng/BEng (Hons)/MSc level)

Virtualised and Cloud-based labs:
- Complex infrastructures for evaluation for students.
- Deep analysis of security and digital forensics in an isolated environment.
- Industry standard tools and methods.
INSTANCE LOAD [Image=WINDOWS2003]
MOUNT INSTANCE [Disk=STANDARD_DISK] AS [Partition="c"]
 ACTIVITY LOAD [Number=12] [Type=JPEG IMAGES; Class=DRUGS]
 INTO [Folder=USER FOLDER]
 AT [Period=1 MINUTE] [Interval=INTERVAL]
 FOR [User=Fred]

Virtualisation Cluster (VMWare ESXi)

Digital Forensics Instance Creator (DFIC)

Results Evaluator

Host Forensic Image (HFI)

HFI Library

Disk Instance (DI) Library

Forensic Media Library (FML)
Forensics Quality Evaluator
(Speed of response, CPU utilization, memory footprint, thread utilization, and so on)

Black-box Testing – completely unknown instances

Grey-box testing

White-box Testing – well known instances

Forensic Quality Metrics
- Presence of known illicit images
- Presence of known illicit movies
- Evidence of accessing/viewing/uploading/downloading illicit material
- Evidence of moving/copying/burning/printing illicit material to other locations
- User accounts – number and names
- Presence of files sharing software
- File sharing history vs known bad files
- Presence of counter-forensics software
- ...
- Hidden files (unallocated space) - recovery
- Deleted files - recovery
- String searches for ASCII strings
- String searches for UNICODE strings
Select labs:
- Lab 1.
- Instance A.
- Instance B.
- Lab 2.

REST services

Web Server

SOAP API

Flexiant
Cloud

Xen

vCenter
Cloud
(Supports files
to be mounted)

Sandboxed
environment

ESXi/ESXi

AWS

VNC link

Web interface

Current implementation
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> Some results
CPU Resources: 52GHz
Total memory: 75GB
Number of hosts: 3
Total processors: 24
Host: Dell PowerEdge R410, 2.4GHz, 2 Sockets, Xeon, 4 Processors per socket
Tool validation:
- Supports a wide range of tool validation.
- Ever changing environment for a range of testing.

Skills:
- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Different labs can be created for different situations (DF Tools/OSs/etc).
- Supports remote/distance learning.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.
- Extensive and complex infrastructures assessed within a sandboxed environments.

Drawbacks:
- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.

Other advantages:
- Easy for teaching team to update.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Produces repeatable labs.
- Not dependent on Napier/network infrastructure.
- Time windows of labs/tutorials can be carefully controlled.
Non-changing environment

Law enforcement training

Student training

Vendor tool analysis

Real Data Corpa (RDC)

```
c:\forensics>bulk_extractor.0.1.0.exe images.bin -o test1
phase 1.
Input file: images.bin
Output directory: test1
Reading raw file at offset 12576768/12582912... Done in
00:00:00Phase 2. Reporting dir: test1
c:\forensics>cd test1
c:\forensics\test1>dir
Volume in drive C is BOOTCAMP
Volume Serial Number is 8CCO-257A

Directory of c:\forensics\test1

01/09/2011 11:05 0  cons.txt
01/09/2011 11:05 81 domains.txt
01/09/2011 11:05 111 emails.txt
01/09/2011 11:05 0 emails histogram.txt
01/09/2011 11:05 21 rfc822.txt
01/09/2011 11:05 337,898 wordlist.txt
  6 File(s)  338,111 bytes
  2 Dir(s)  1,620,799,488 bytes free
c:\forensics\test1>head emails.txt
10425618  per.oan@sonyericsson.com
10470675  per.oan@sonyericsson.com
10589305  per.oan@sonyericsson.com
```
Community Cloud

- Overview for Cloud Computing.
- How Cloud Infrastructures could be used for teaching to enhanced skills.
- D-FET – A Community Cloud.
- Example used within teaching.

Author: Prof Bill Buchanan