Securing the Cloud

Digital Investigations for the Cloud

Emma Webb Hobson
Senior Digital Forensic Investigator
ejwhobson@qinetiq.com
Client side analysis – post mortem

Machine is seized (power is cut) and sent to the lab for analysis

Two major questions to answer:
• How do you know if a user has been using cloud services?
• If they have – what fragments or traces remain?

Some previous experience:
• Internet analysis
• Internet history
• Browser artefacts
• Temporary internet files
• Cookies
• Favourites
Client side analysis – live

Live forensics – examination while computer is still turned on

• Can capture running services and processes
• Network traffic
• RAM capture
• Mounted encrypted volumes and files
• Instant messenger sessions
And now….  
• Cloud computing services and connections?
• Encrypted cloud data?

Live forensics – disadvantages

• Only a snapshot – single point in time
• Integrity is preserved from point of capture but cannot be reproduced
• Installation of tools modifies data
• Requires technical specialists on site
Server (CSP) side analysis

Request data from cloud service provider (CSP)
• Users files
• Users access logs

Problems
• Immature procedure
• International jurisdictions
• Bureaucracy, paperwork, time delays and cost
• Reluctance from CSP
  – Reputational damage
  – Client privacy
  – Genuine difficulty and cost of responding
Network traffic analysis

Capture data travelling between CSP and cloud service user

**Law enforcement monitoring**
Interception of communications?
⇒ Warrant from Home Office
⇒ Serious and organised crime only?

**Business monitoring**
Private telecommunications?
⇒ Acceptable Use Policy
⇒ RIPA s1(6)
⇒ Telecommunications Regulations 2000
⇒ Data Protection Act 1998

What data can be captured?

How can it be interpreted?

Probably encrypted…
Application Programming Interface (API)

• Set of commands used by client to interact with cloud service

• Currently, each CSP has developed their own

• Capture and interpretation of commands could identify actions of user and applications, data acted on, and date and time information
http://www.linkedin.com/e/vgh/2934495/
Any Questions?

http://uk.linkedin.com/in/emmawebbhobson

Emma Webb Hobson
Proposition Development Manager at QinetiQ
Guildford, United Kingdom

- Contact Emma Webb Hobson
- Add Emma Webb Hobson to your network

Emma Webb Hobson
Senior Digital Forensic Investigator
ejwhobson@qinetiq.com