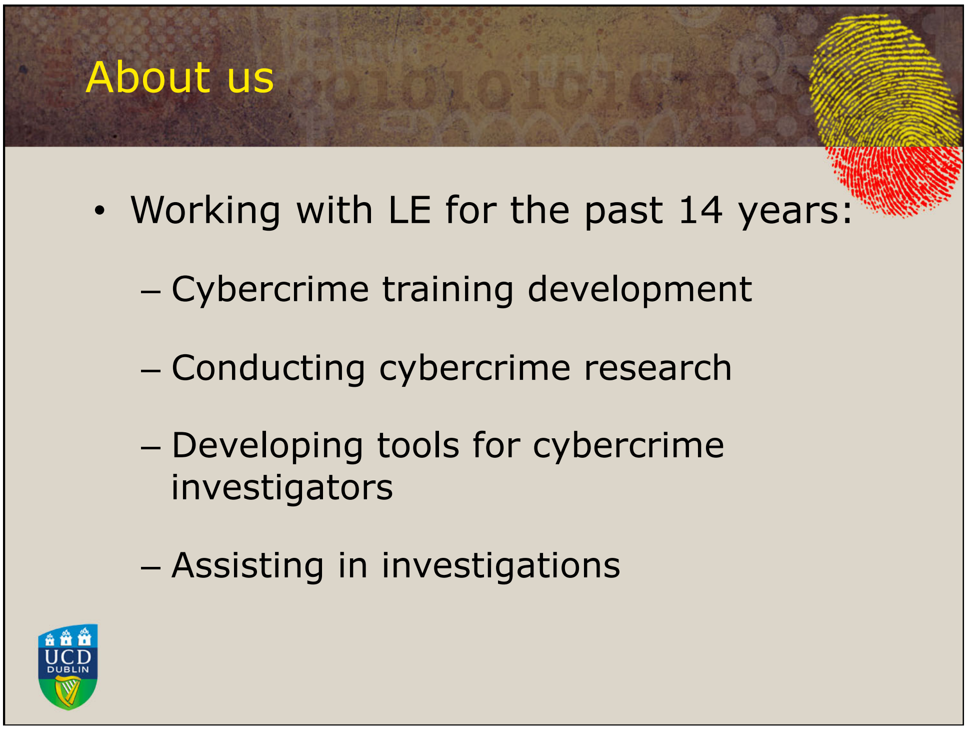
Digital Forensics Investigation Research Group

Digital Forensics, Cloud Computing, Future of Cybercrime Investigation

Pavel Gladyshev & Joshua James

University College Dublin

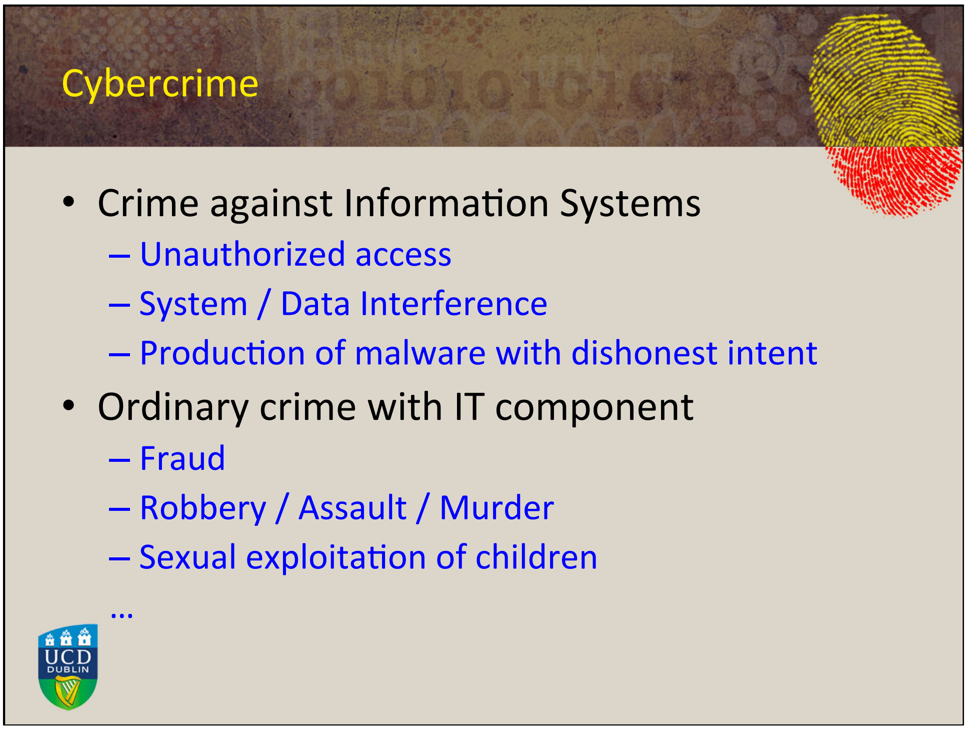


About us

- Working with LE for the past 14 years:
  - Cybercrime training development
  - Conducting cybercrime research
  - Developing tools for cybercrime investigators
  - Assisting in investigations

Partners

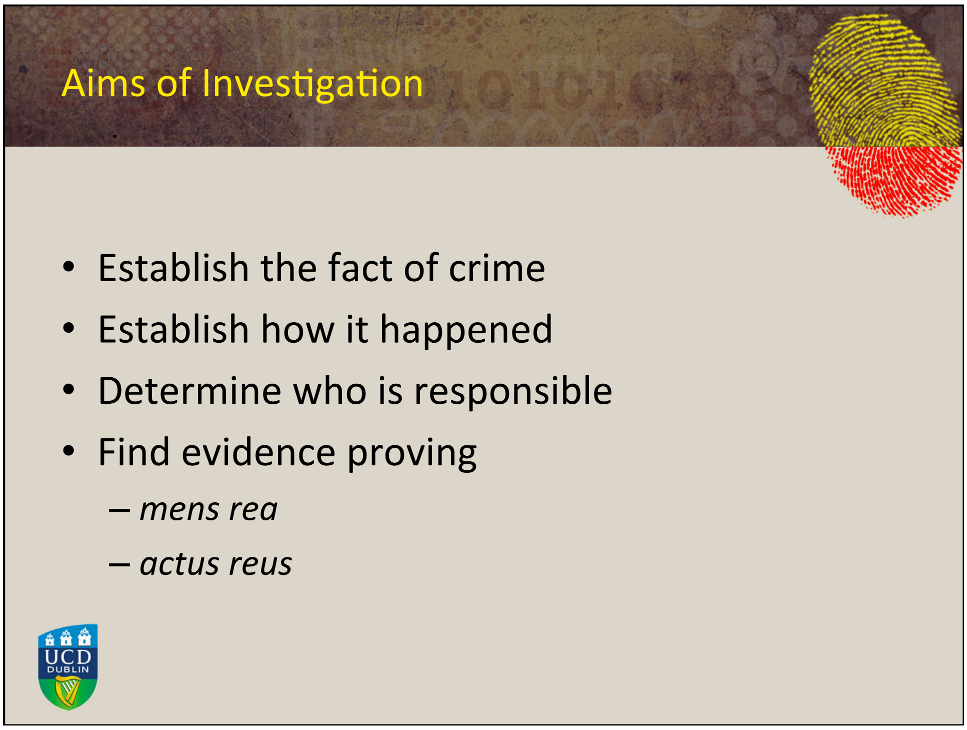
OIPC
ICPO
INTERPOL
EUROPOL
UCD
DUBLIN



Cybercrime

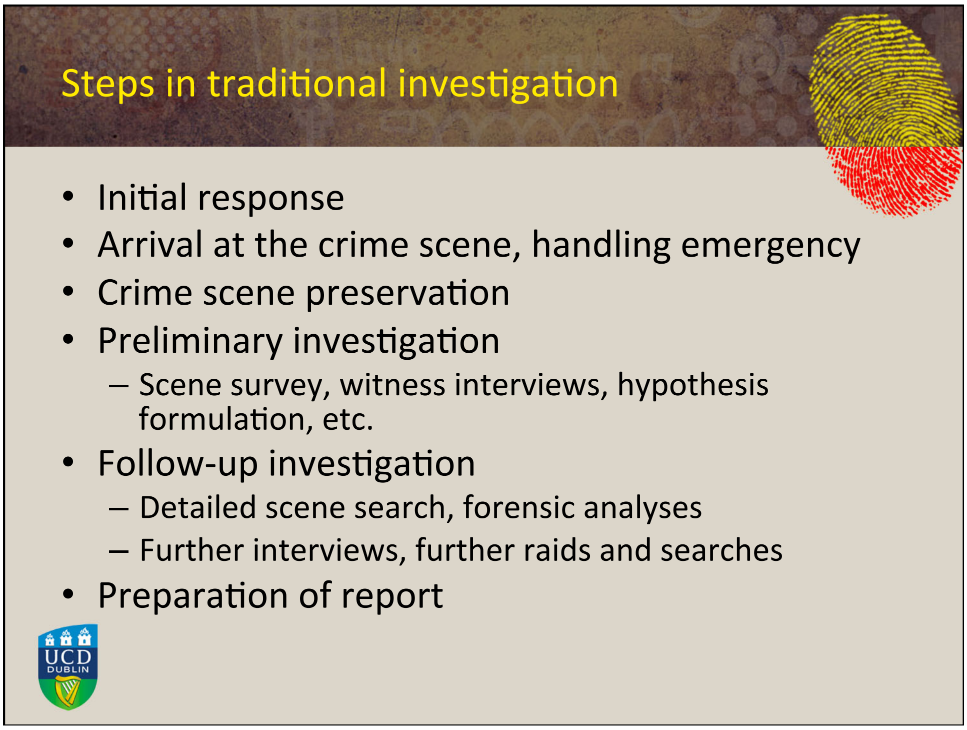
- Crime against Information Systems
  - Unauthorized access
  - System / Data Interference
  - Production of malware with dishonest intent
- Ordinary crime with IT component
  - Fraud
  - Robbery / Assault / Murder
  - Sexual exploitation of children

  …



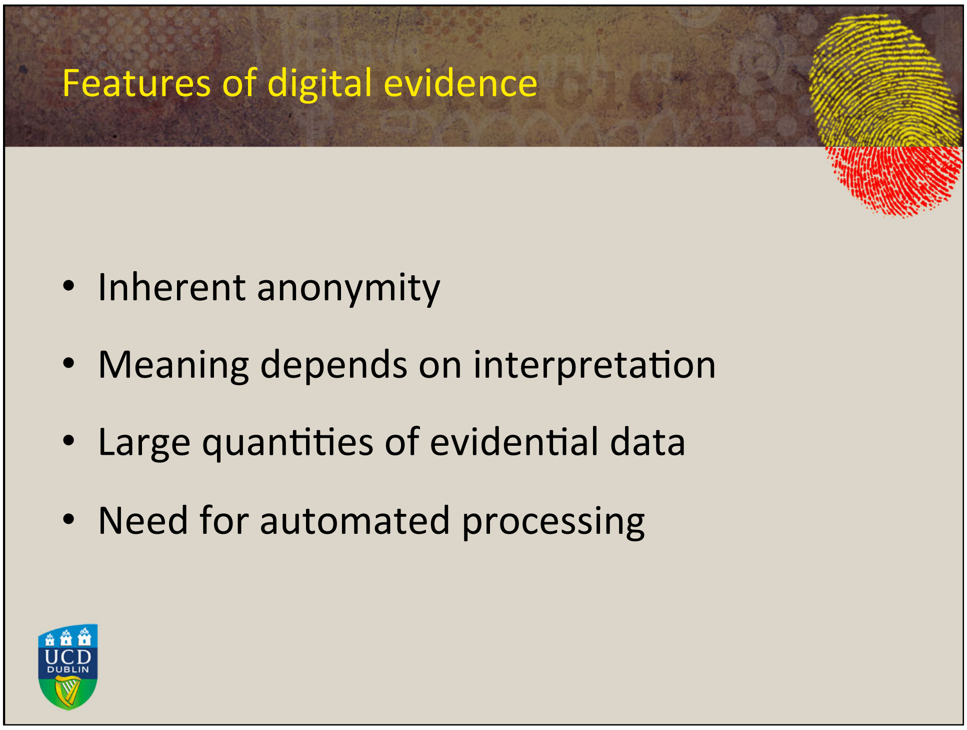
Aims of Investigation

- Establish the fact of crime
- Establish how it happened
- Determine who is responsible
- Find evidence proving
  - *mens rea*
  - *actus reus*



Steps in traditional investigation

- Initial response
- Arrival at the crime scene, handling emergency
- Crime scene preservation
- Preliminary investigation
  - Scene survey, witness interviews, hypothesis formulation, etc.
- Follow-up investigation
  - Detailed scene search, forensic analyses
  - Further interviews, further raids and searches
- Preparation of report



Features of digital evidence

- Inherent anonymity
- Meaning depends on interpretation
- Large quantities of evidential data
- Need for automated processing

Digital Forensic Science (DFRWS)

- use of **scientifically** derived and proven **methods**

for

- preservation, validation, identification, analysis, interpretation, documentation and presentation

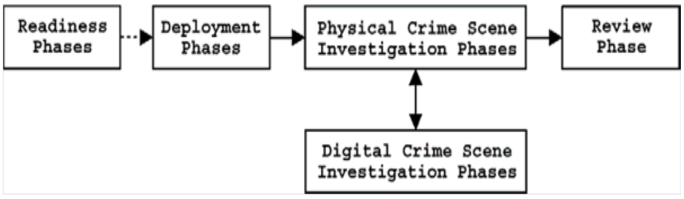
of

- **digital evidence** derived from **digital sources**

for

- reconstruction of criminal events
- helping to anticipate unauthorized actions

Enhanced Digital Investigation Process Model (Carrier & Spafford, 2003)



Readiness Phases

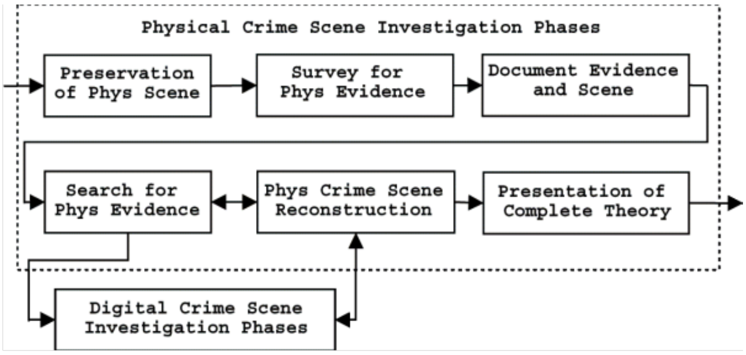
Deployment Phases

Physical Crime Scene Investigation Phases

Review Phase

Digital Crime Scene Investigation Phases

IDIP: Physical Phase



Physical Crime Scene Investigation Phases

Preservation of Phys Scene

Survey for Phys Evidence

Document Evidence and Scene

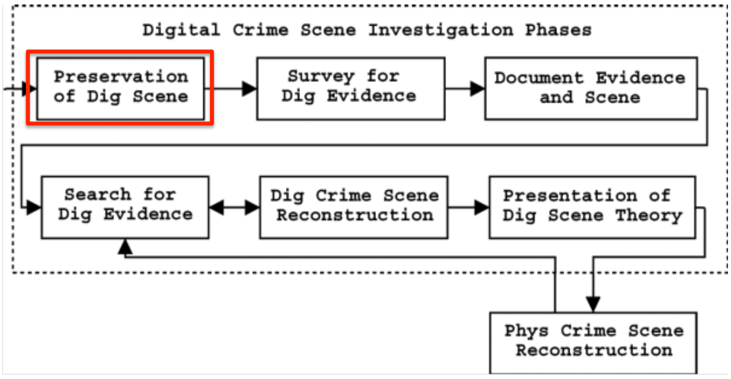
Search for Phys Evidence

Phys Crime Scene Reconstruction

Presentation of Complete Theory

Digital Crime Scene Investigation Phases

IDIP: Digital Phase



Digital Crime Scene Investigation Phases

Preservation of Dig Scene

Survey for Dig Evidence

Document Evidence and Scene

Search for Dig Evidence

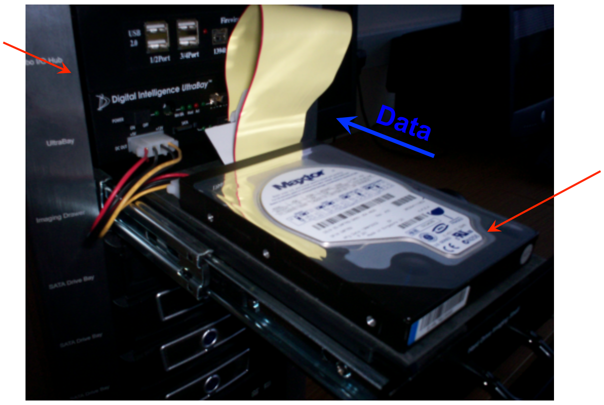
Dig Crime Scene Reconstruction

Presentation of Dig Scene Theory

Phys Crime Scene Reconstruction

Disk Imaging

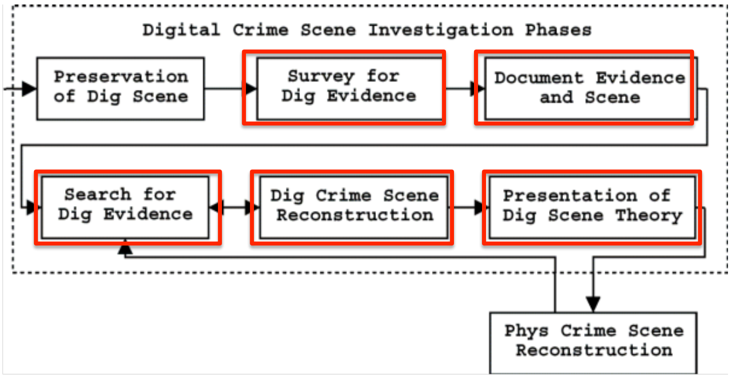
Forensic workstation



Evidential disk

- Evidential disk is extracted from its evidential computer and connected to forensic workstation. The data is copied out of it and into forensic workstation's internal data storage

IDIP: Digital Phase



Digital Crime Scene Investigation Phases

Preservation of Dig Scene

Survey for Dig Evidence

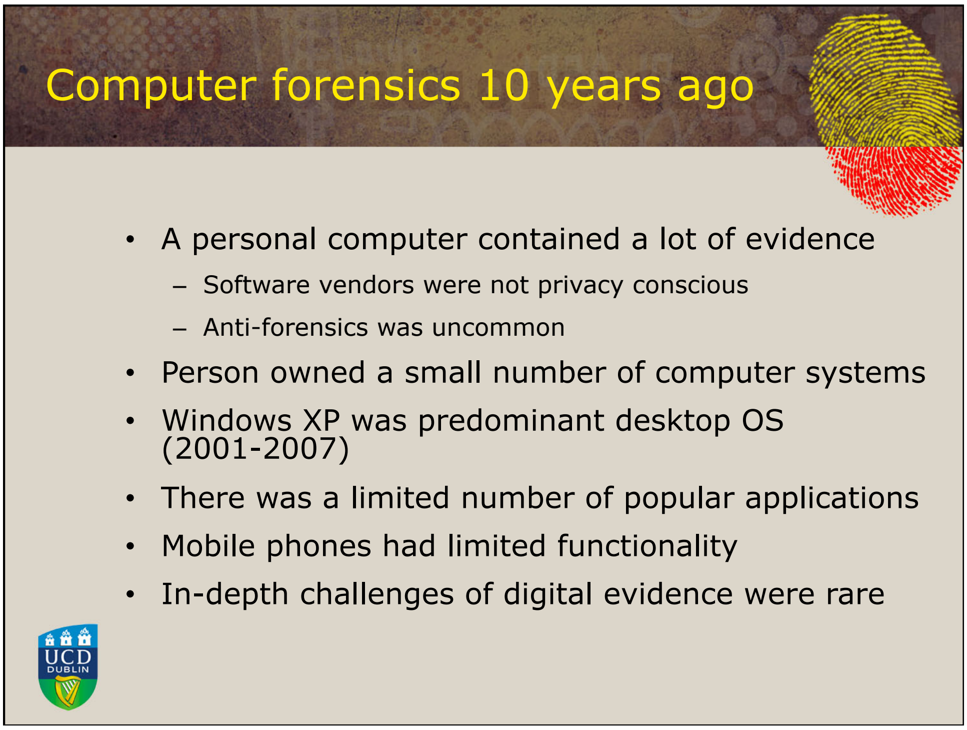
Document Evidence and Scene

Search for Dig Evidence

Dig Crime Scene Reconstruction

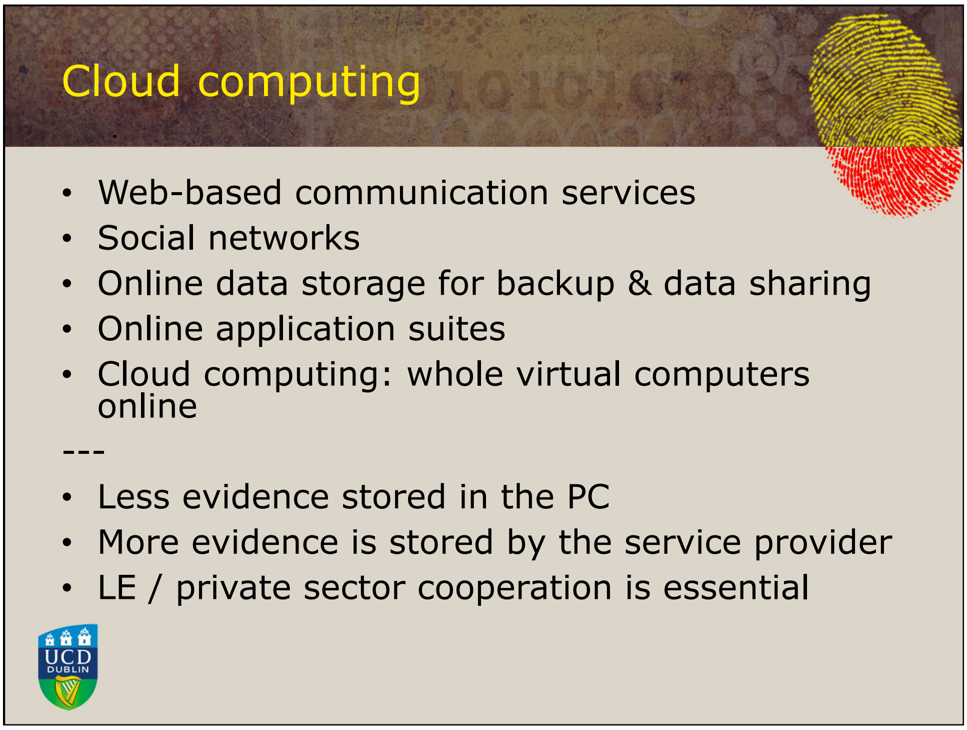
Presentation of Dig Scene Theory

Phys Crime Scene Reconstruction



Computer forensics 10 years ago

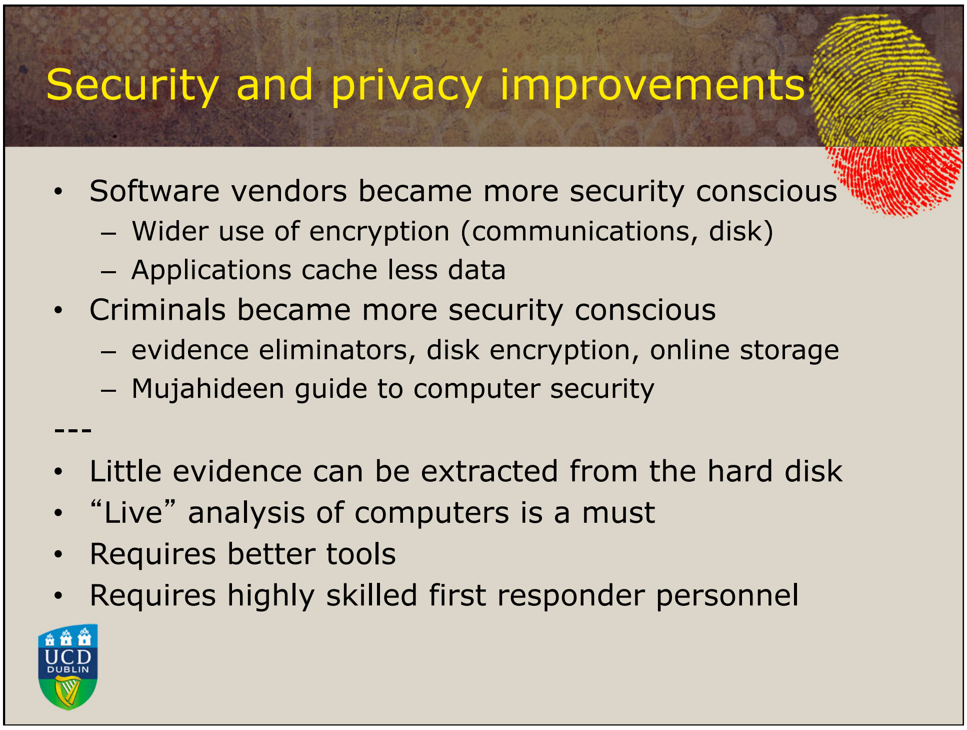
- A personal computer contained a lot of evidence
  - Software vendors were not privacy conscious
  - Anti-forensics was uncommon
- Person owned a small number of computer systems
- Windows XP was predominant desktop OS (2001-2007)
- There was a limited number of popular applications
- Mobile phones had limited functionality
- In-depth challenges of digital evidence were rare



Cloud computing

- Web-based communication services
- Social networks
- Online data storage for backup & data sharing
- Online application suites
- Cloud computing: whole virtual computers online

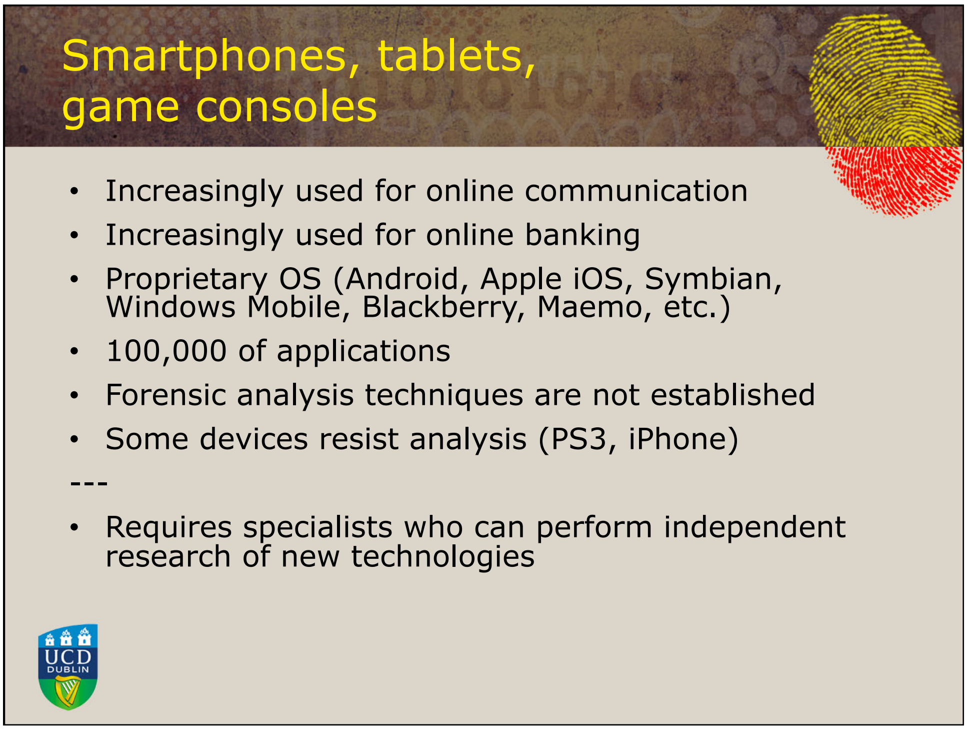
- Less evidence stored in the PC
- More evidence is stored by the service provider
- LE / private sector cooperation is essential



Security and privacy improvements

- Software vendors became more security conscious
  - Wider use of encryption (communications, disk)
  - Applications cache less data
- Criminals became more security conscious
  - evidence eliminators, disk encryption, online storage
  - Mujahideen guide to computer security

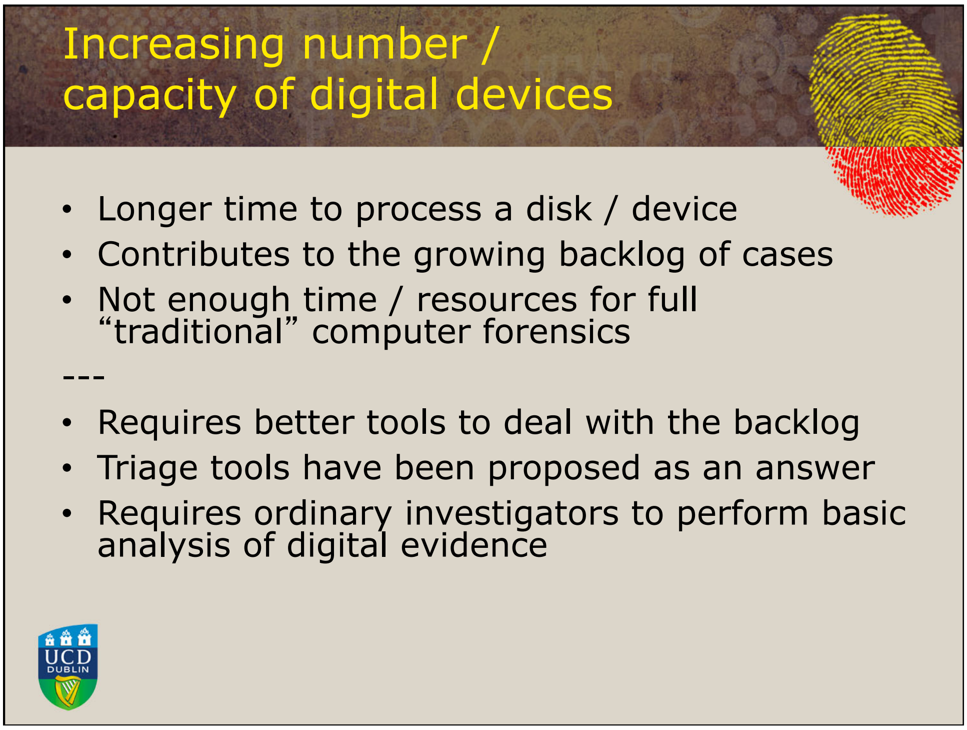
- Little evidence can be extracted from the hard disk
- “Live” analysis of computers is a must
- Requires better tools
- Requires highly skilled first responder personnel



Smartphones, tablets, game consoles

- Increasingly used for online communication
- Increasingly used for online banking
- Proprietary OS (Android, Apple iOS, Symbian, Windows Mobile, Blackberry, Maemo, etc.)
- 100,000 of applications
- Forensic analysis techniques are not established
- Some devices resist analysis (PS3, iPhone)

- Requires specialists who can perform independent research of new technologies

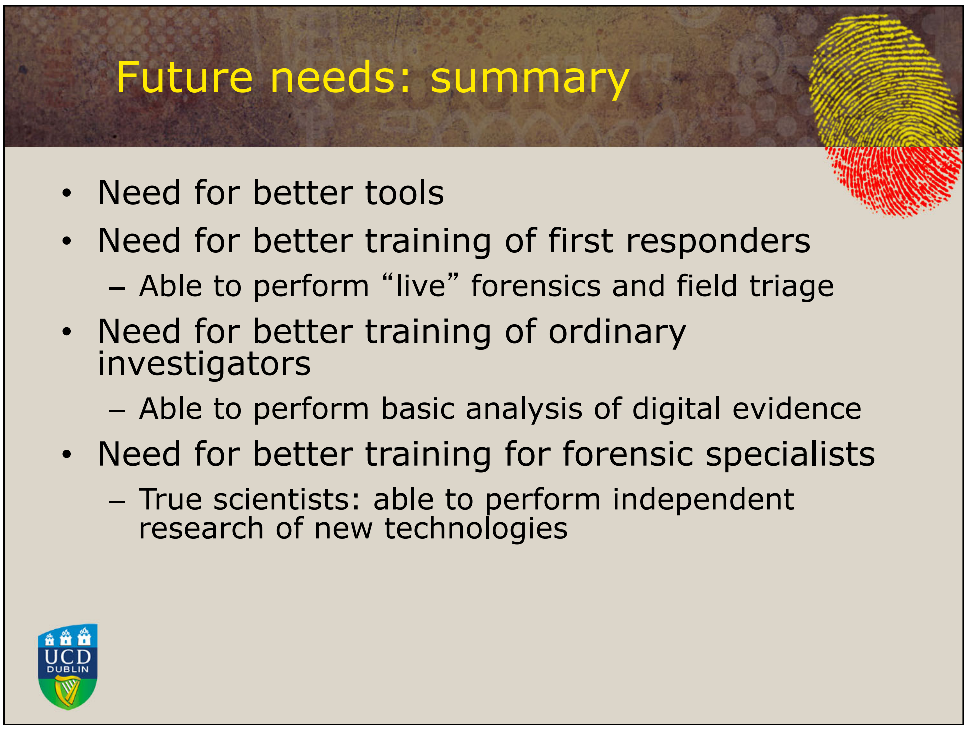


Increasing number / capacity of digital devices

- Longer time to process a disk / device
- Contributes to the growing backlog of cases
- Not enough time / resources for full "traditional" computer forensics

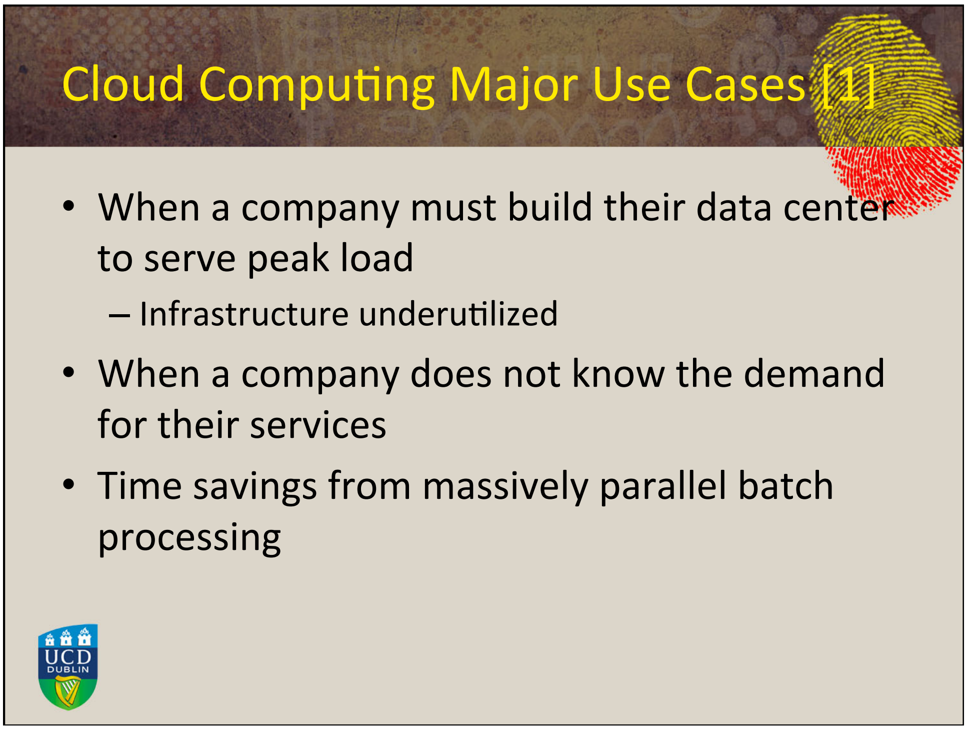
---

- Requires better tools to deal with the backlog
- Triage tools have been proposed as an answer
- Requires ordinary investigators to perform basic analysis of digital evidence



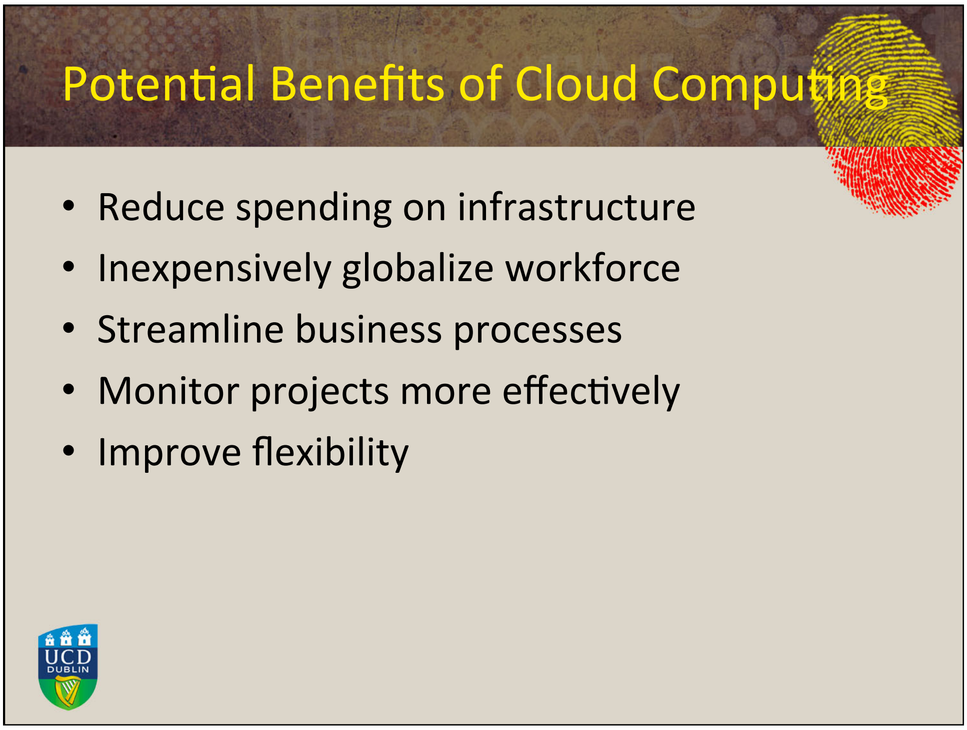
Future needs: summary

- Need for better tools
- Need for better training of first responders
  - Able to perform "live" forensics and field triage
- Need for better training of ordinary investigators
  - Able to perform basic analysis of digital evidence
- Need for better training for forensic specialists
  - True scientists: able to perform independent research of new technologies



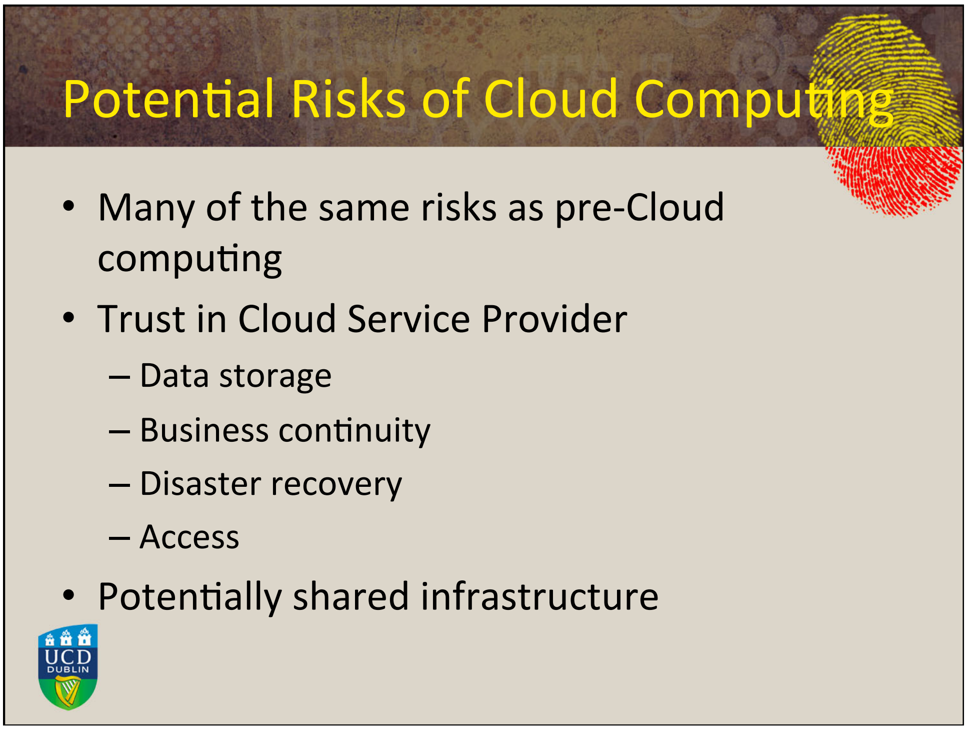
Cloud Computing Major Use Cases [1]

- When a company must build their data center to serve peak load
  - Infrastructure underutilized
- When a company does not know the demand for their services
- Time savings from massively parallel batch processing



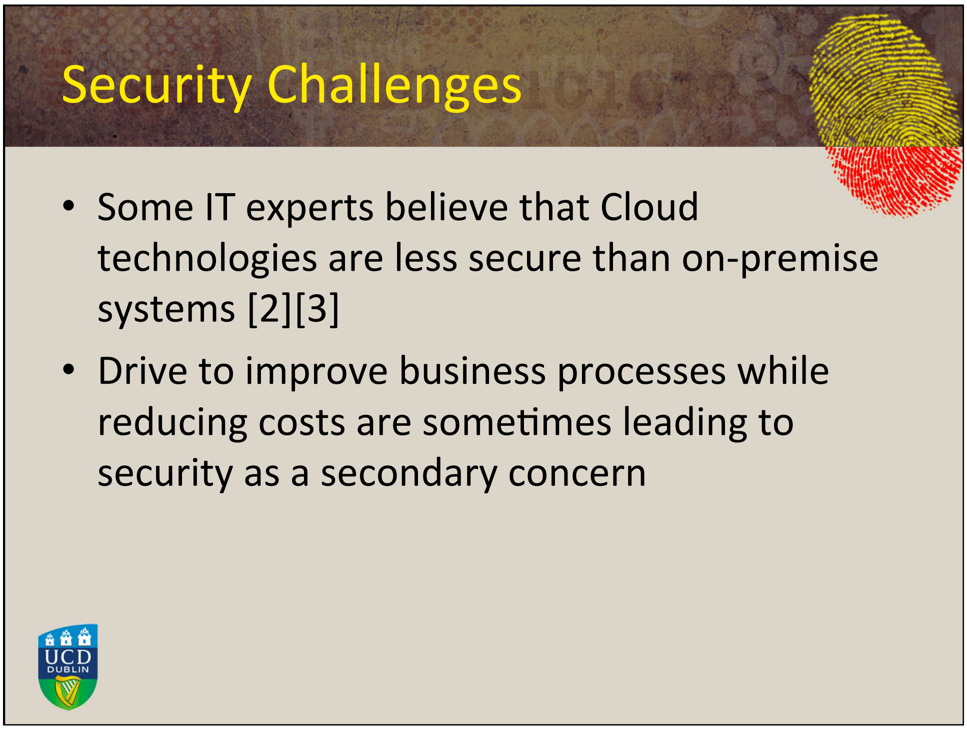
Potential Benefits of Cloud Computing

- Reduce spending on infrastructure
- Inexpensively globalize workforce
- Streamline business processes
- Monitor projects more effectively
- Improve flexibility



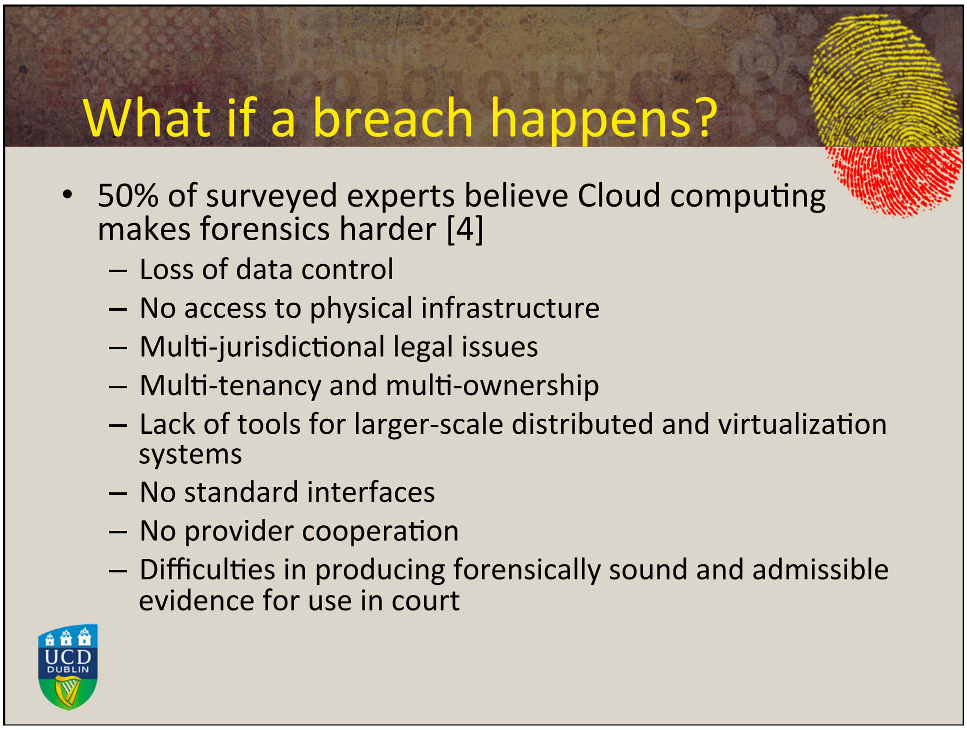
Potential Risks of Cloud Computing

- Many of the same risks as pre-Cloud computing
- Trust in Cloud Service Provider
  - Data storage
  - Business continuity
  - Disaster recovery
  - Access
- Potentially shared infrastructure



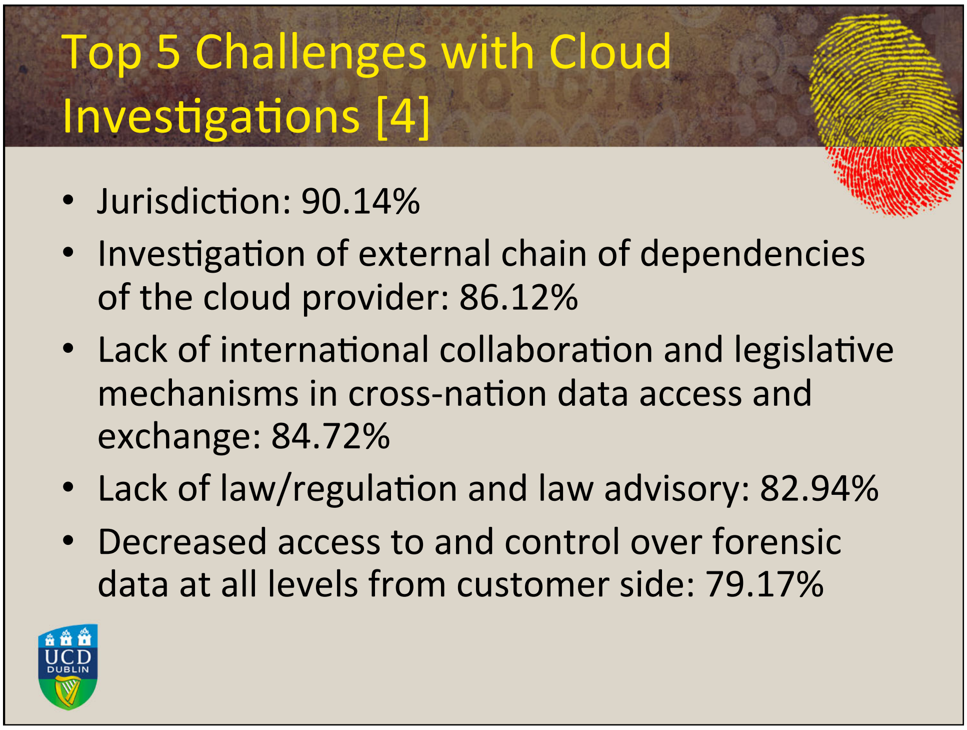
Security Challenges

- Some IT experts believe that Cloud technologies are less secure than on-premise systems [2][3]
- Drive to improve business processes while reducing costs are sometimes leading to security as a secondary concern



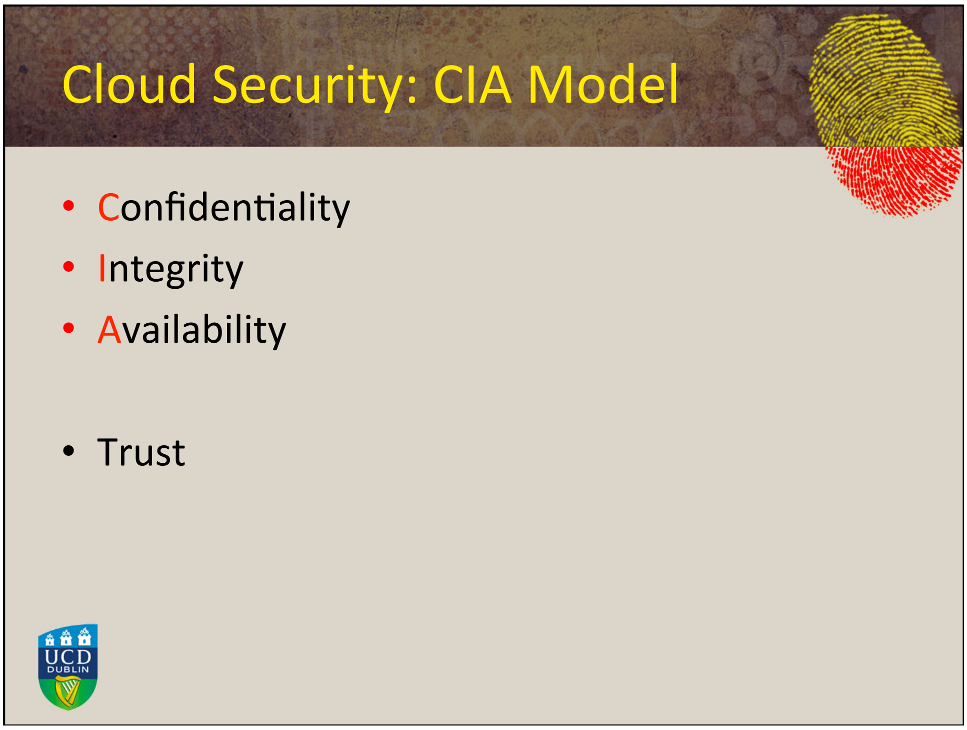
What if a breach happens?

- 50% of surveyed experts believe Cloud computing makes forensics harder [4]
  - Loss of data control
  - No access to physical infrastructure
  - Multi-jurisdictional legal issues
  - Multi-tenancy and multi-ownership
  - Lack of tools for larger-scale distributed and virtualization systems
  - No standard interfaces
  - No provider cooperation
  - Difficulties in producing forensically sound and admissible evidence for use in court



Top 5 Challenges with Cloud Investigations [4]

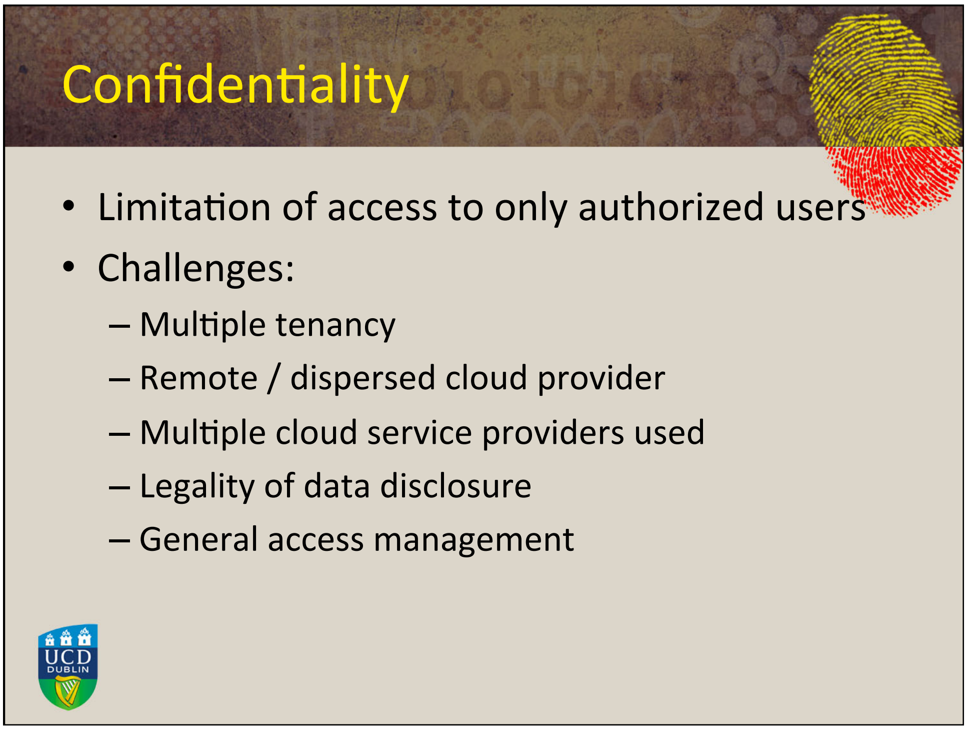
- Jurisdiction: 90.14%
- Investigation of external chain of dependencies of the cloud provider: 86.12%
- Lack of international collaboration and legislative mechanisms in cross-nation data access and exchange: 84.72%
- Lack of law/regulation and law advisory: 82.94%
- Decreased access to and control over forensic data at all levels from customer side: 79.17%



Cloud Security: CIA Model

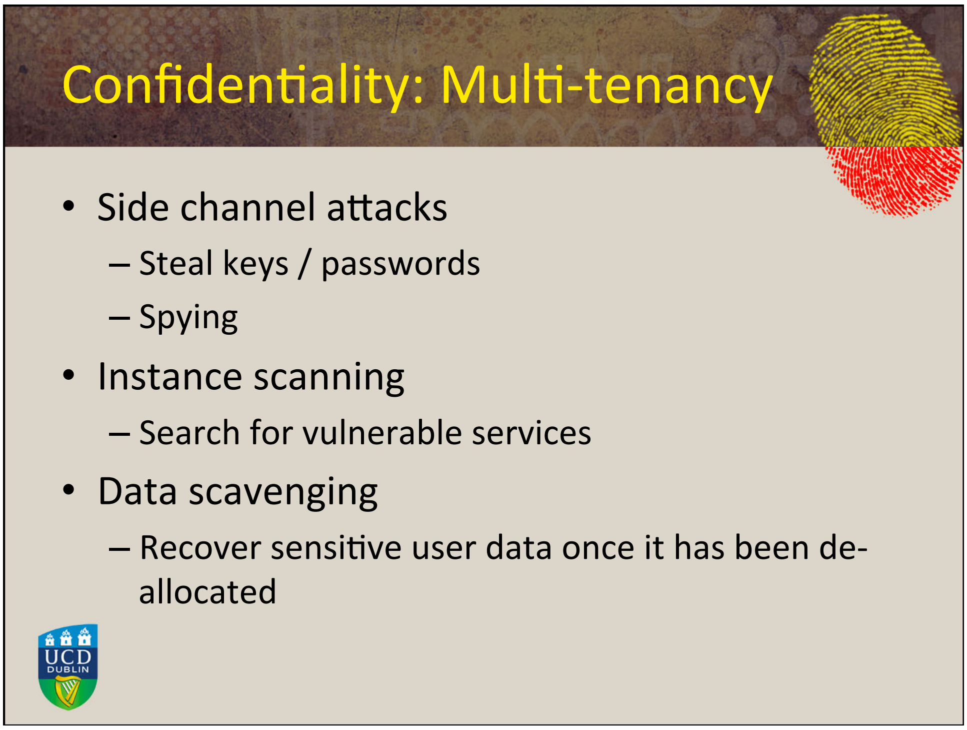
- Confidentiality
- Integrity
- Availability

- Trust



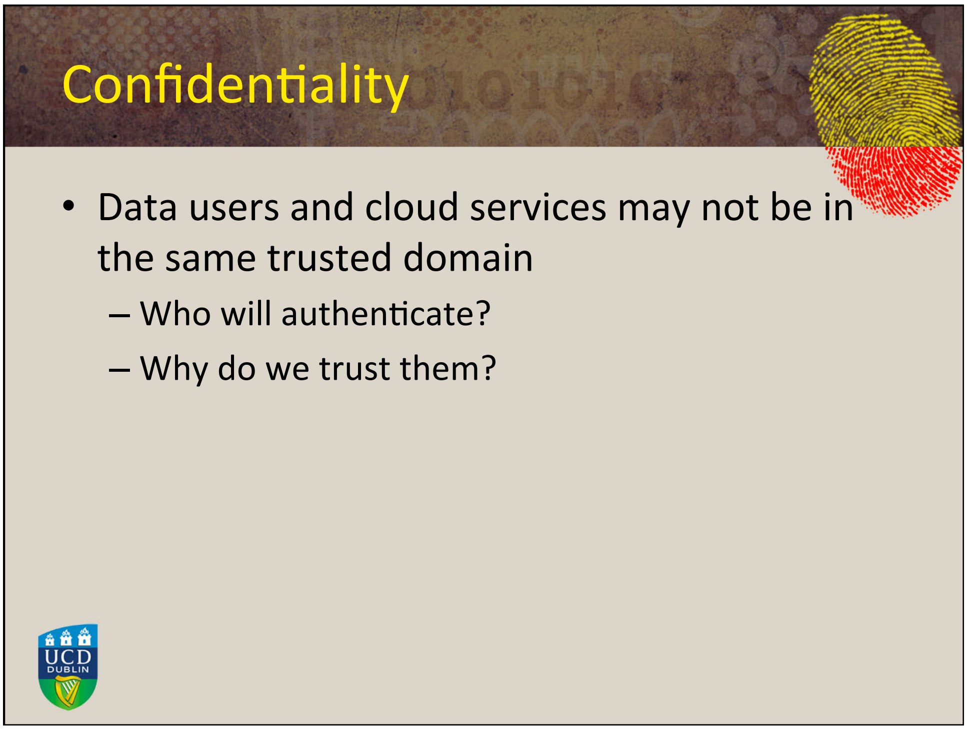
Confidentiality

- Limitation of access to only authorized users
- Challenges:
  - Multiple tenancy
  - Remote / dispersed cloud provider
  - Multiple cloud service providers used
  - Legality of data disclosure
  - General access management



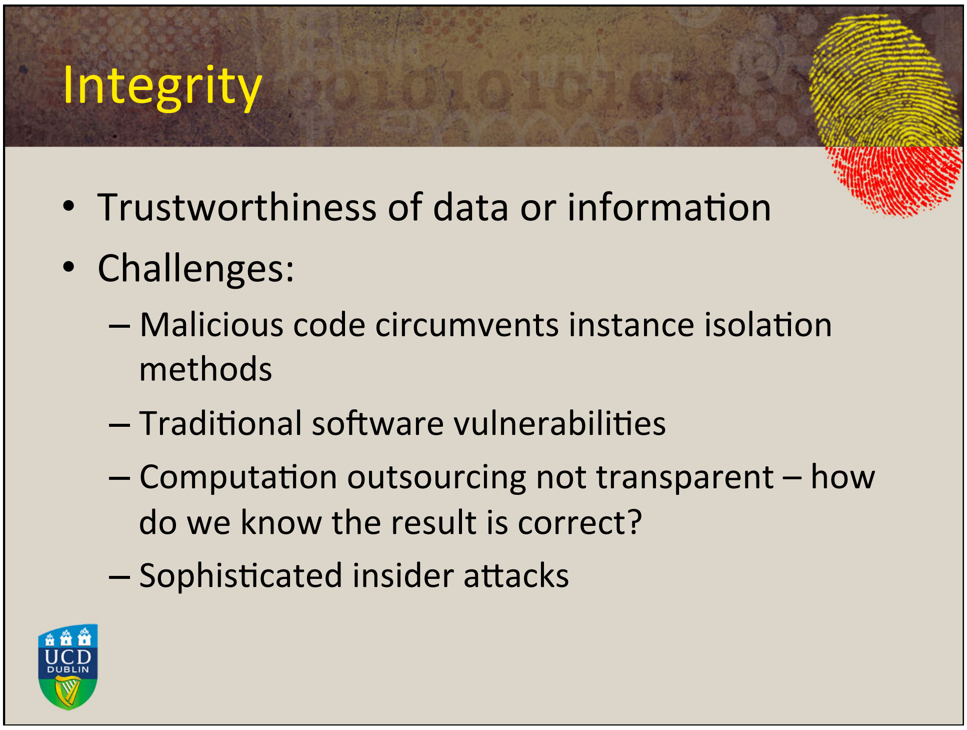
Confidentiality: Multi-tenancy

- Side channel attacks
  - Steal keys / passwords
  - Spying
- Instance scanning
  - Search for vulnerable services
- Data scavenging
  - Recover sensitive user data once it has been de-allocated



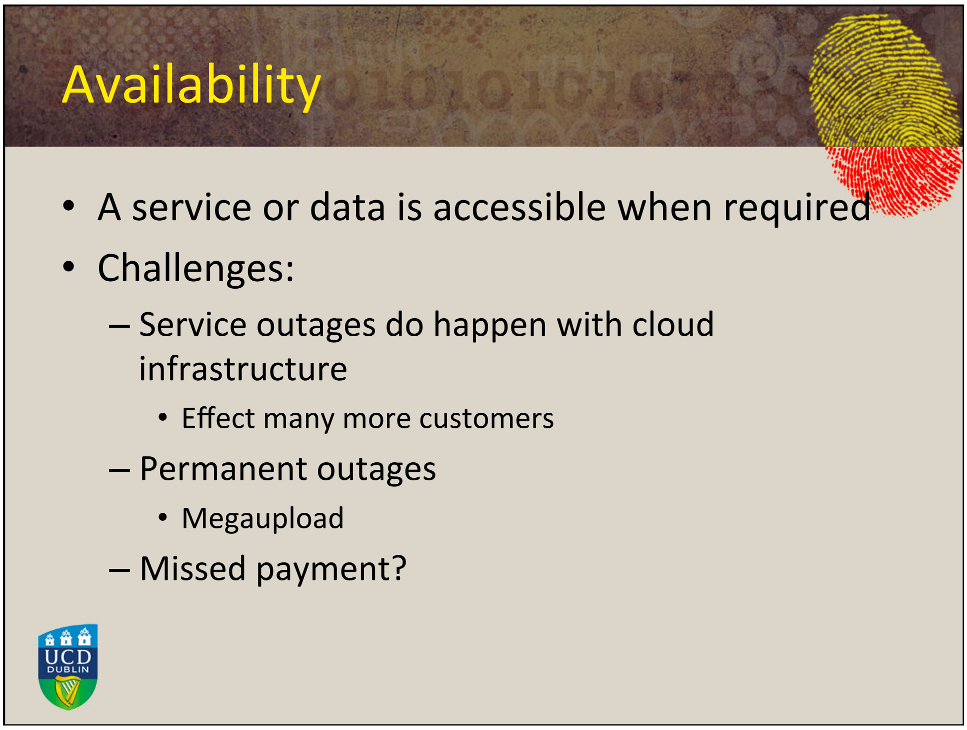
Confidentiality

- Data users and cloud services may not be in the same trusted domain
  - Who will authenticate?
  - Why do we trust them?



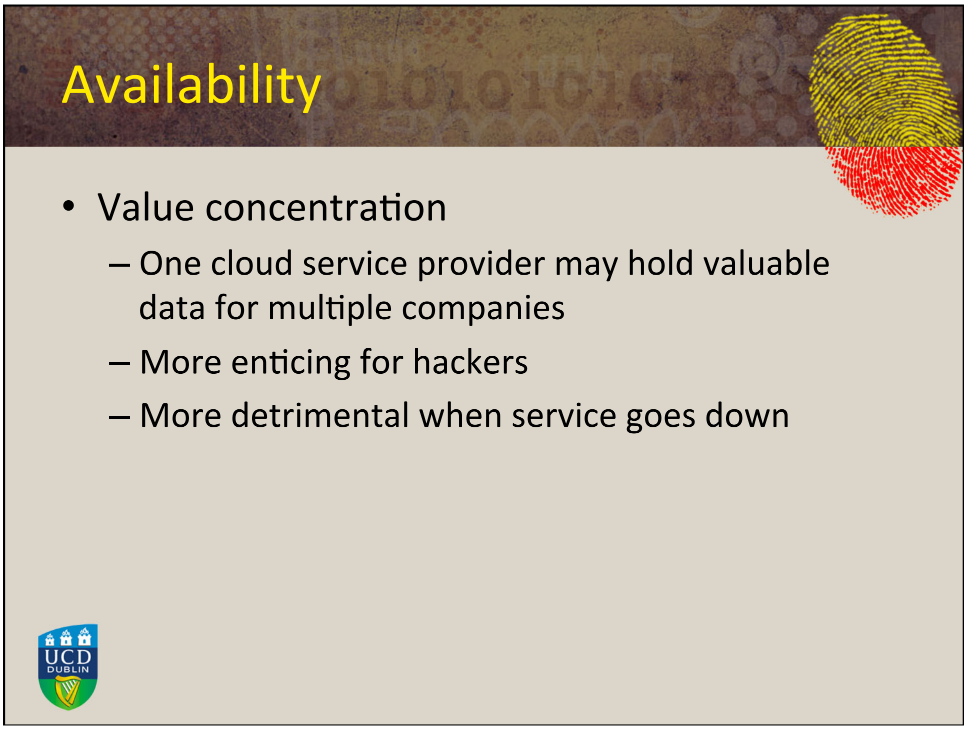
Integrity

- Trustworthiness of data or information
- Challenges:
  - Malicious code circumvents instance isolation methods
  - Traditional software vulnerabilities
  - Computation outsourcing not transparent – how do we know the result is correct?
  - Sophisticated insider attacks



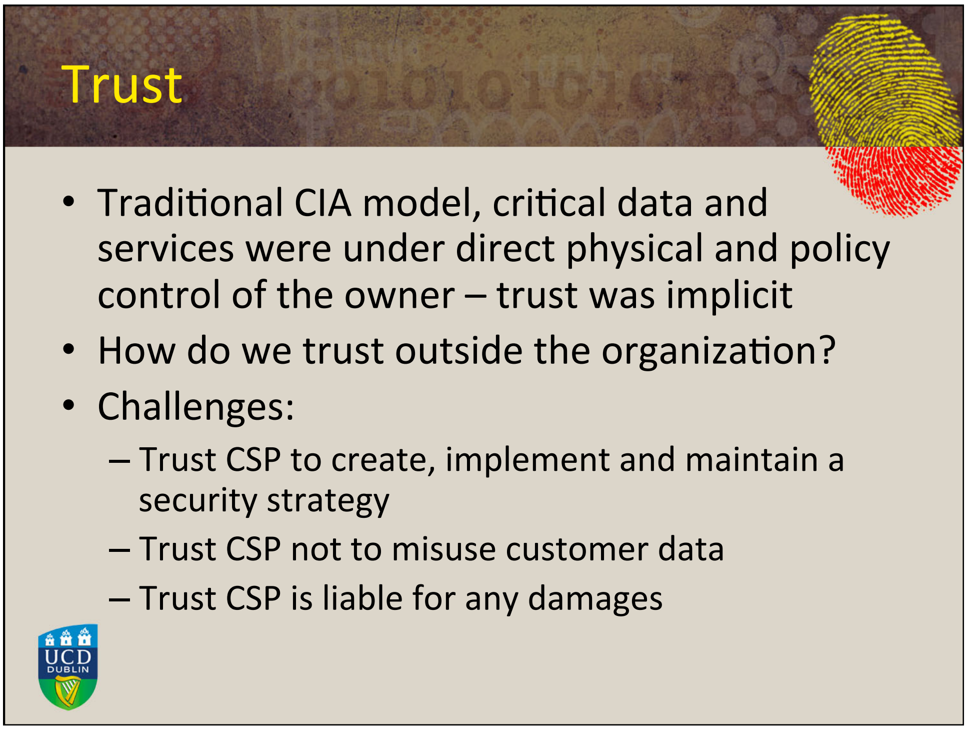
Availability

- A service or data is accessible when required
- Challenges:
  - Service outages do happen with cloud infrastructure
    - Effect many more customers
  - Permanent outages
    - Megaupload
  - Missed payment?



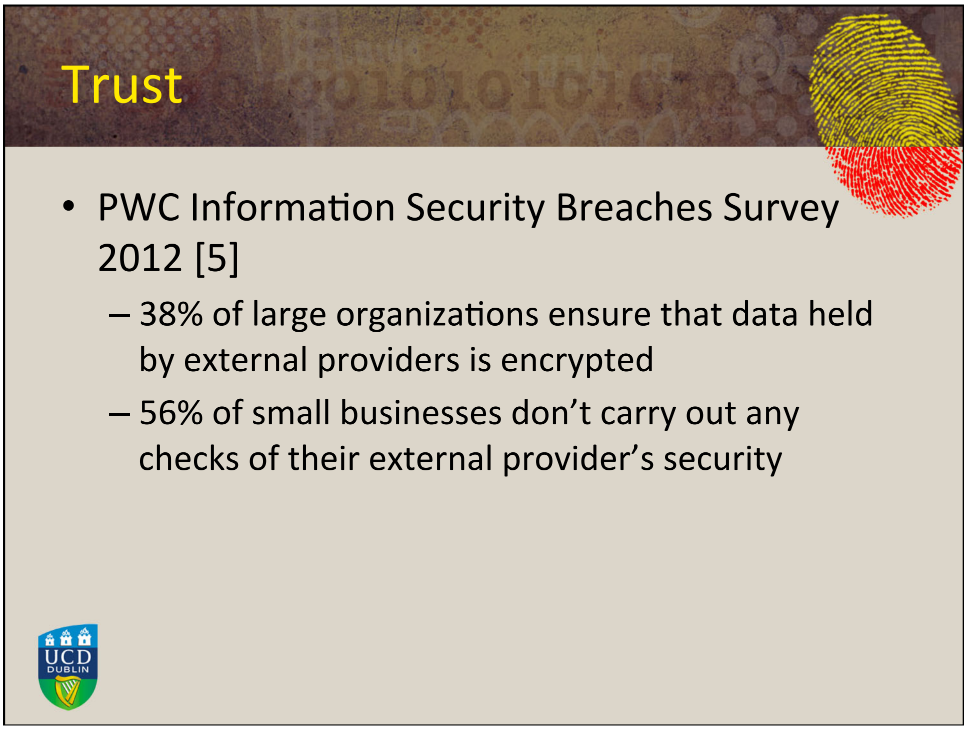
Availability

- Value concentration
  - One cloud service provider may hold valuable data for multiple companies
  - More enticing for hackers
  - More detrimental when service goes down



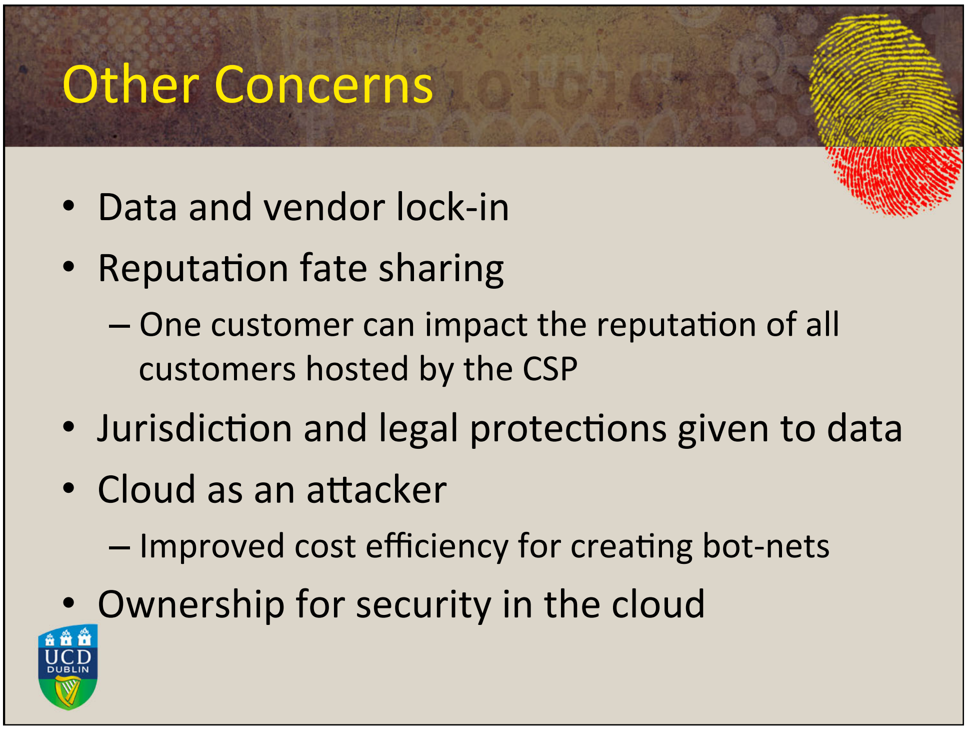
Trust

- Traditional CIA model, critical data and services were under direct physical and policy control of the owner – trust was implicit
- How do we trust outside the organization?
- Challenges:
  - Trust CSP to create, implement and maintain a security strategy
  - Trust CSP not to misuse customer data
  - Trust CSP is liable for any damages



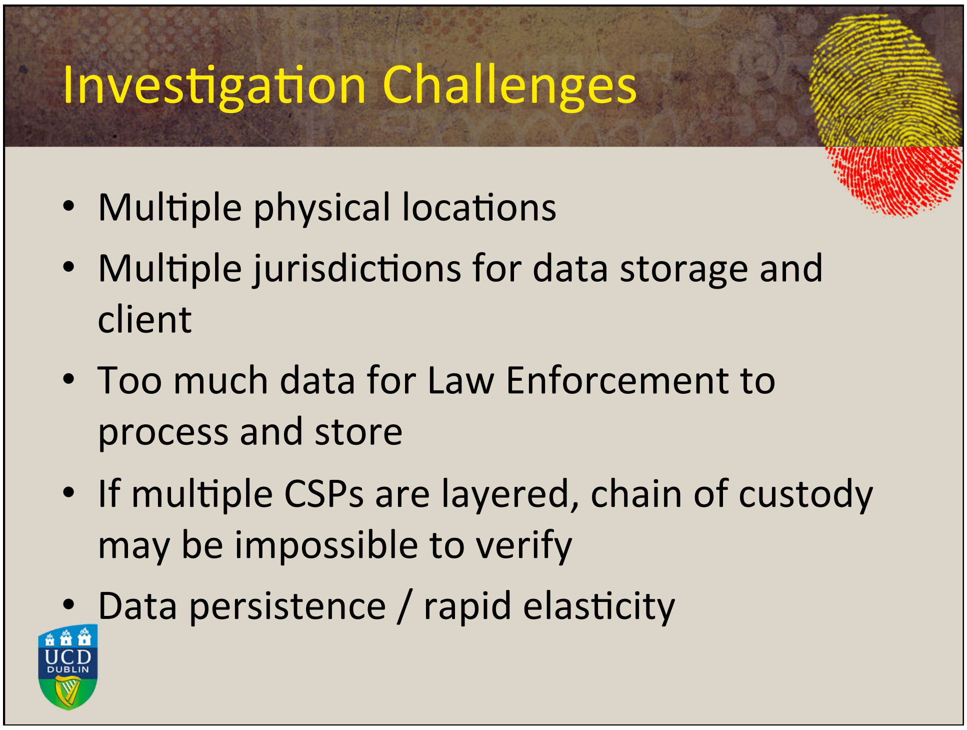
Trust

- PWC Information Security Breaches Survey 2012 [5]
  - 38% of large organizations ensure that data held by external providers is encrypted
  - 56% of small businesses don't carry out any checks of their external provider's security



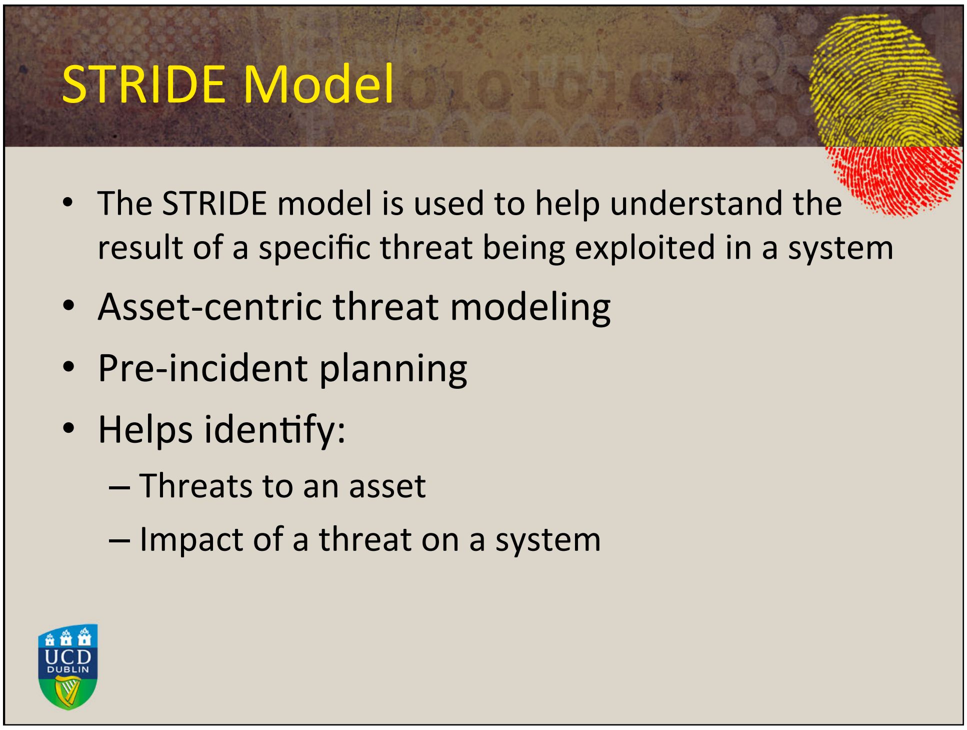
Other Concerns

- Data and vendor lock-in
- Reputation fate sharing
  - One customer can impact the reputation of all customers hosted by the CSP
- Jurisdiction and legal protections given to data
- Cloud as an attacker
  - Improved cost efficiency for creating bot-nets
- Ownership for security in the cloud



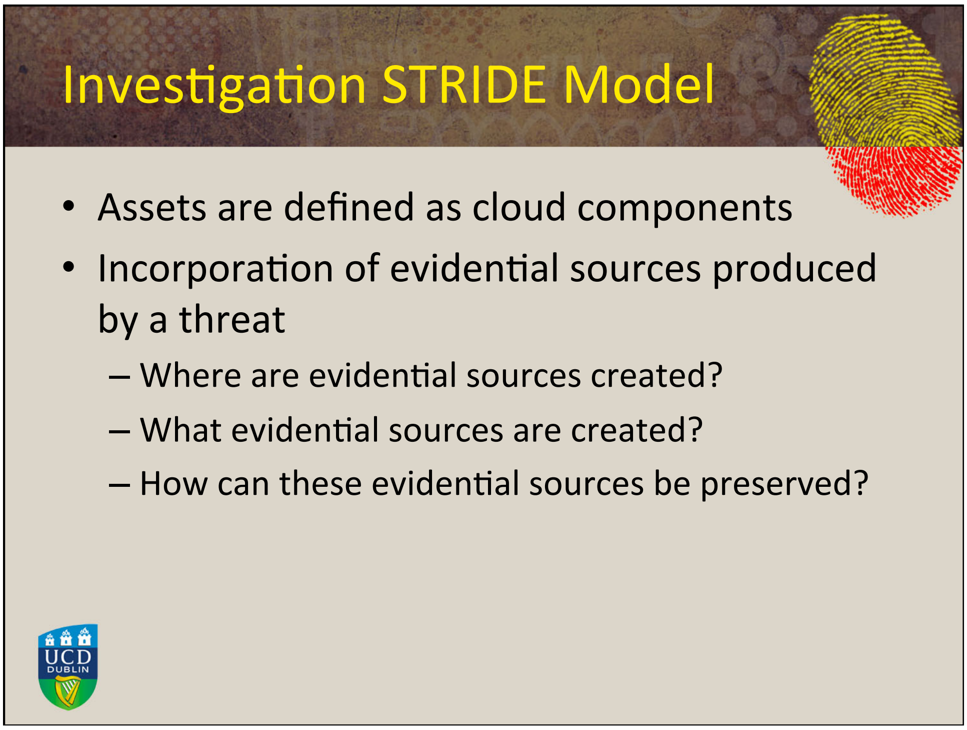
Investigation Challenges

- Multiple physical locations
- Multiple jurisdictions for data storage and client
- Too much data for Law Enforcement to process and store
- If multiple CSPs are layered, chain of custody may be impossible to verify
- Data persistence / rapid elasticity



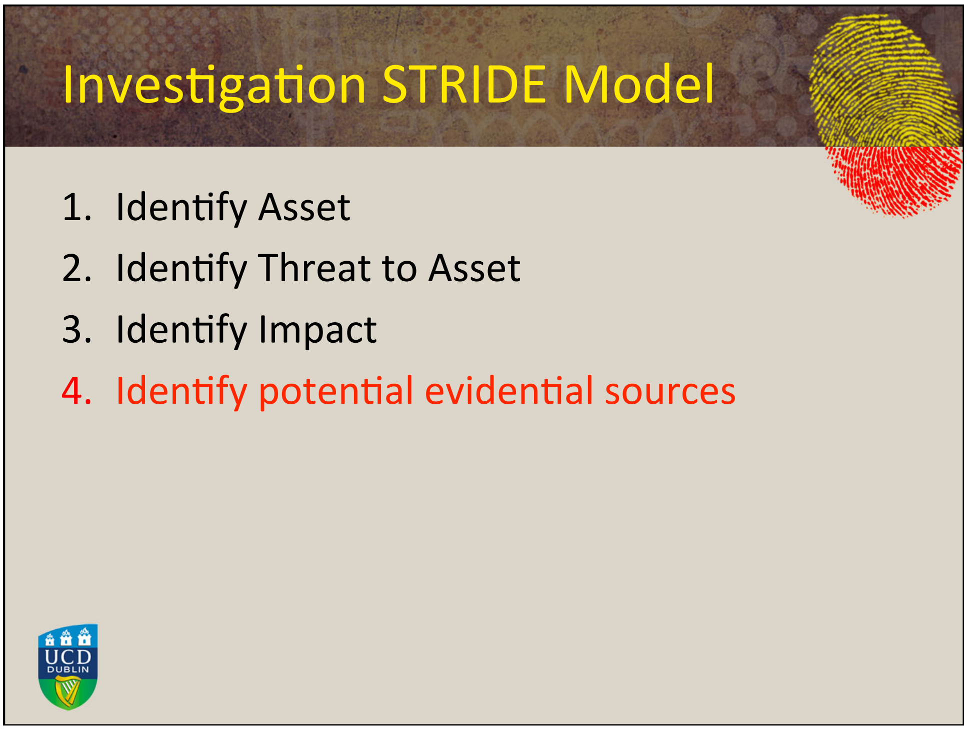
STRIDE Model

- The STRIDE model is used to help understand the result of a specific threat being exploited in a system
- Asset-centric threat modeling
- Pre-incident planning
- Helps identify:
  - Threats to an asset
  - Impact of a threat on a system



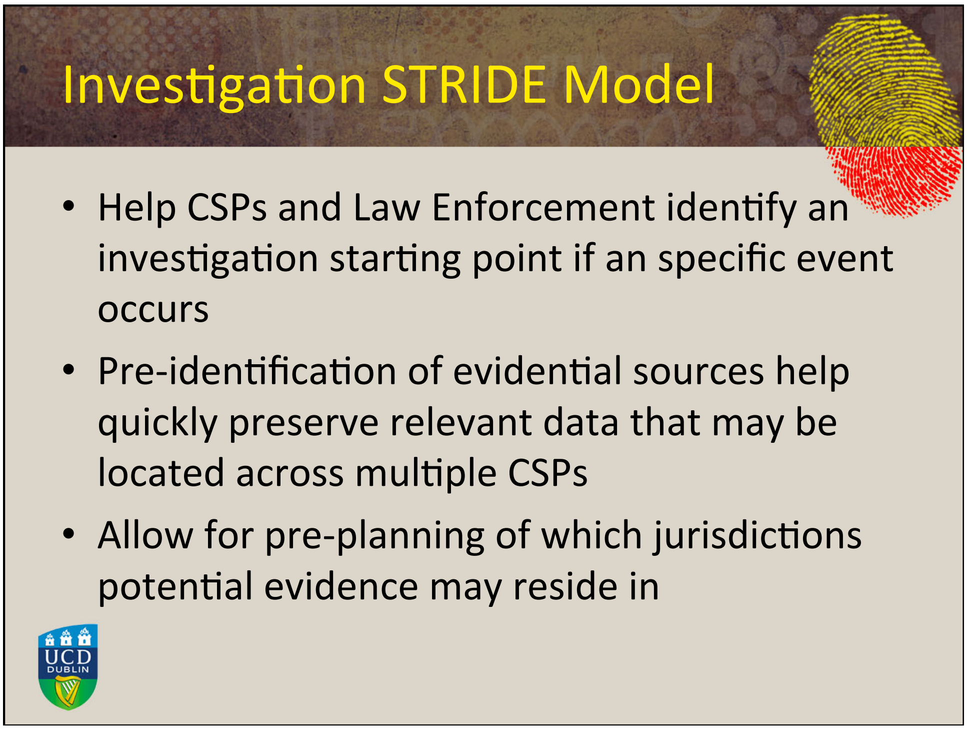
Investigation STRIDE Model

- Assets are defined as cloud components
- Incorporation of evidential sources produced by a threat
  - Where are evidential sources created?
  - What evidential sources are created?
  - How can these evidential sources be preserved?



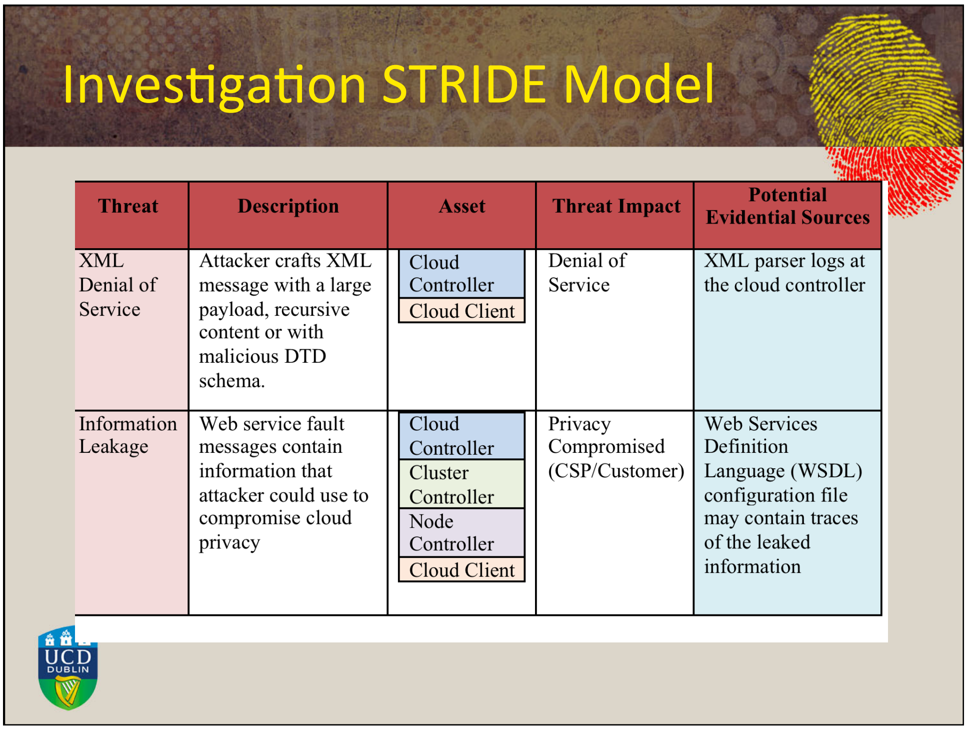
Investigation STRIDE Model

1. Identify Asset
2. Identify Threat to Asset
3. Identify Impact
4. Identify potential evidential sources



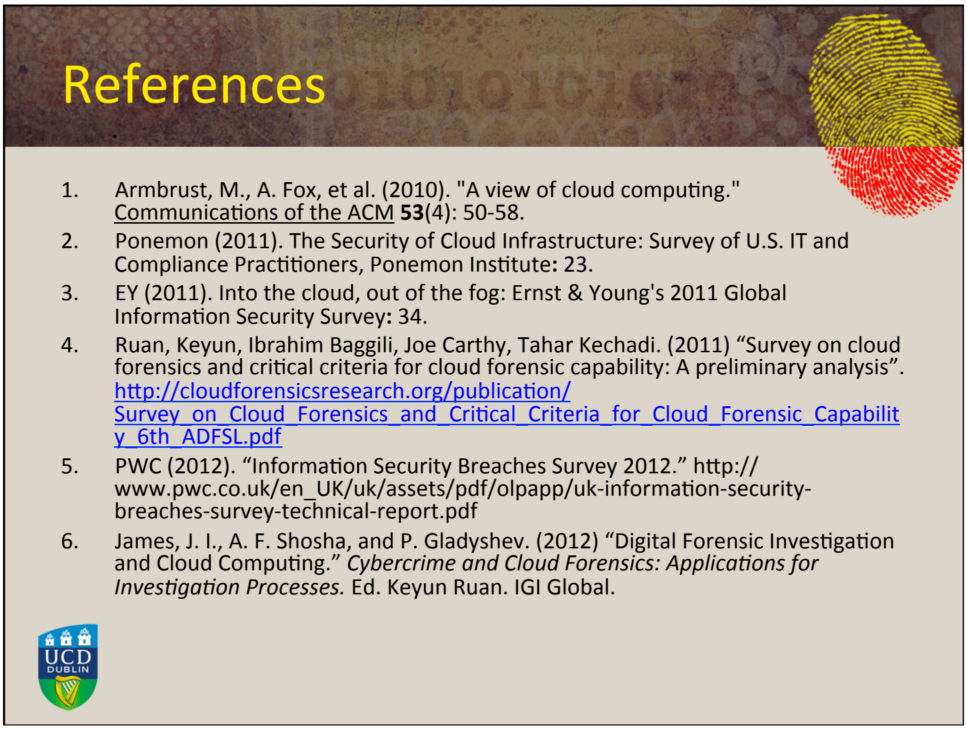
Investigation STRIDE Model

- Help CSPs and Law Enforcement identify an investigation starting point if an specific event occurs
- Pre-identification of evidential sources help quickly preserve relevant data that may be located across multiple CSPs
- Allow for pre-planning of which jurisdictions potential evidence may reside in



Investigation STRIDE Model

Threat	Description	Asset	Threat Impact	Potential Evidential Sources
XML Denial of Service	Attacker crafts XML message with a large payload, recursive content or with malicious DTD schema.	Cloud Controller Cloud Client	Denial of Service	XML parser logs at the cloud controller
Information Leakage	Web service fault messages contain information that attacker could use to compromise cloud privacy	Cloud Controller Cluster Controller Node Controller Cloud Client	Privacy Compromised (CSP/Customer)	Web Services Definition Language (WSDL) configuration file may contain traces of the leaked information



References

1. Armbrust, M., A. Fox, et al. (2010). "A view of cloud computing." Communications of the ACM **53**(4): 50-58.
2. Ponemon (2011). The Security of Cloud Infrastructure: Survey of U.S. IT and Compliance Practitioners, Ponemon Institute**:** 23.
3. EY (2011). Into the cloud, out of the fog: Ernst & Young's 2011 Global Information Security Survey**:** 34.
4. Ruan, Keyun, Ibrahim Baggili, Joe Carthy, Tahar Kechadi. (2011) "Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis". http://cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf
5. PWC (2012). "Information Security Breaches Survey 2012." http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf
6. James, J. I., A. F. Shosha, and P. Gladyshev. (2012) "Digital Forensic Investigation and Cloud Computing." *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* Ed. Keyun Ruan. IGI Global.