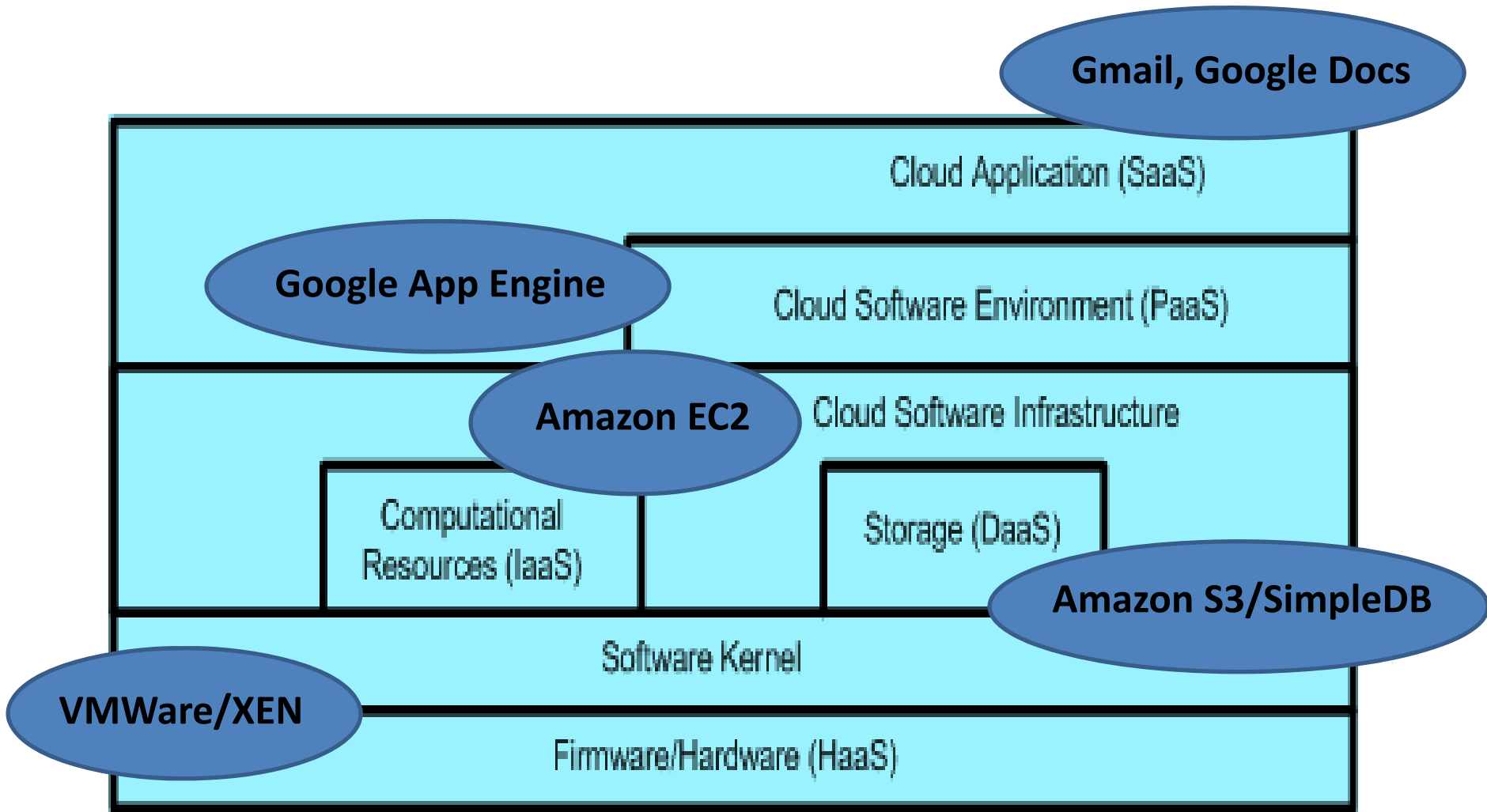


Security in the Clouds

Professor Sadie Creese
London Hopper 2010
May 2010

What is cloud computing?

Service Model



Cloud Market Drivers

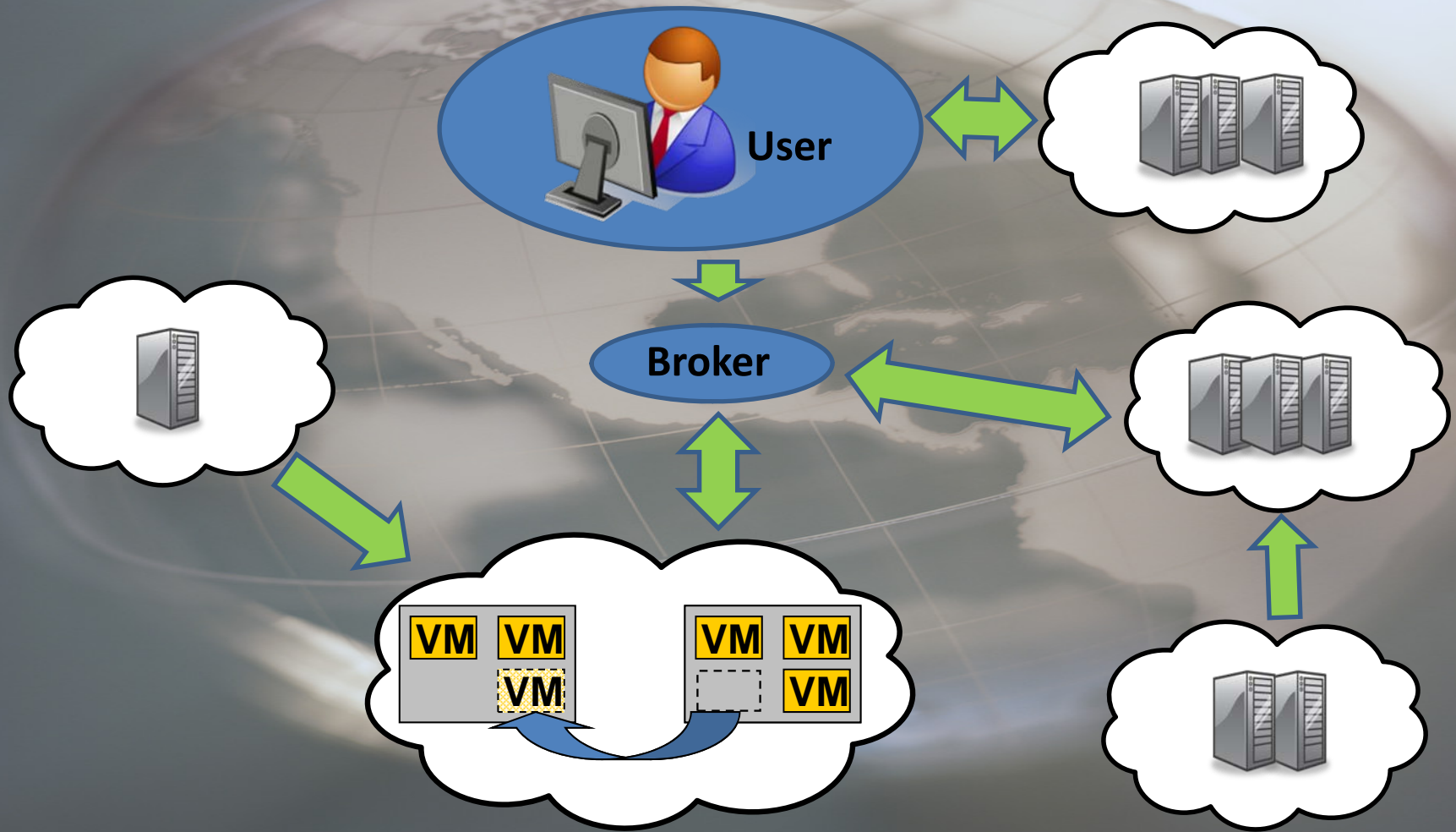
- **Enterprise Drivers**

- Compression of deployment cycles
- Instant upgrade and try-it-out
- Elasticity
- Cost alignment
- Reduction of IT team costs
- Accessibility and sharing
- Dependability
- Waste reduction and carbon footprint

- **Consumer drivers**

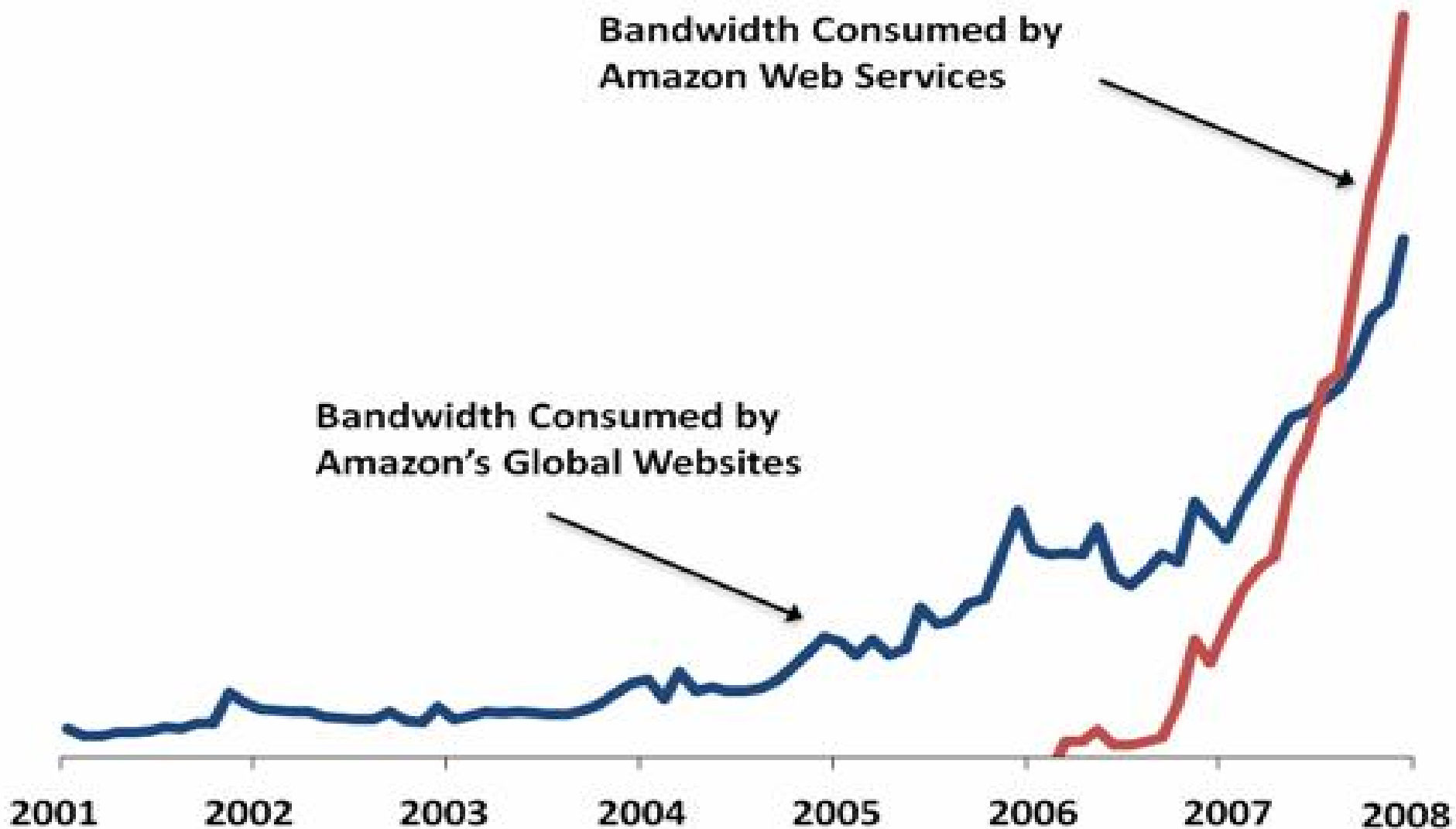
- Up to speed with latest apps
- Pay-as-you-use
- Accessibility and sharing
- Dependability

Cloud Ecosystems



Why are we concerned?

Significant investment



Large Cloud Application Service Provider Space



Extract from slides : "Prophet a Path out of the cloud", Best Practical, Presented at O'Reilly Open Source Conf, 2008

People Are Worried

Key barriers to uptake, as recognised in the community:

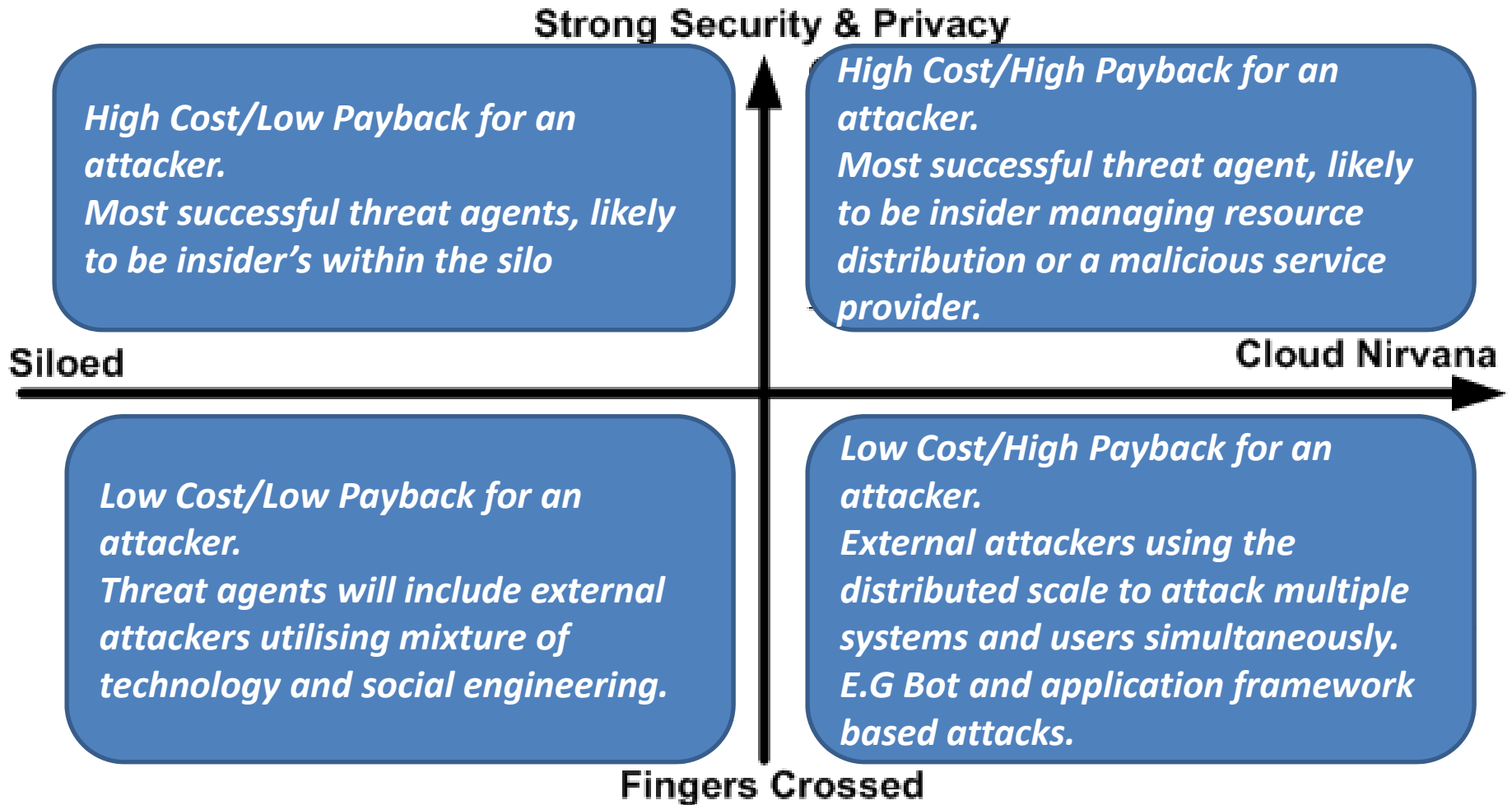
- **Data security concerns**
- **Privacy compromise/ practice**
- **Service dependability and QoS**
- **Loss of control over IT and data**
- **Management difficulties around performance, support and maintenance**
- **Service integration**
- **Lock-in**
- **Usability**
- **Lack of market maturity**

What's different about the Cloud?

Scale and Business Models

- Length and depth of relationships
- Mobility of data
- Volumes of data
- Nature of data (more sensitive)
- Lack of perimeter
- Global nature
- Location of control

Futures – Scenarios



Thinking Like an Attacker

(A few) potential future attack scenarios

- **Denial of service**
 - resource consumption, traffic redirection, inter-cloud and user to cloud
- **Trojan Clouds**
 - Imitate providers, infiltrate supply chains, sympathetic cloud
- **Inference Attacks**
 - Due to privileged (~admin) roles, cohabiting risks (via hypervisor)
- **Application Framework attacks**
 - Repeatable, pervasive
- **Sticky Clouds**
 - Lack of responsiveness, complex portability
- **Onion storage**
 - Moving global location, fragmenting, encrypting
- **Covert channels within the cloud network across services**

And?

(A few) Implications for Security

- **Regulatory/Legislation**
 - Nothing is transparent about data handling in cloud, privacy protection
- **Investigations**
 - Technical forensics and legal, across borders
- **Monitoring/Auditing**
 - Mechanisms
- **Encryption**
 - At some point decryption happens for anything other than storage...
 - Recent IBM breakthrough indicates potential for processing encrypted data but not practical yet..
- **Contracting/Due Diligence**
 - Service Level Agreements

Our current research directions...

- **Digital Forensics**
- **Vulnerability Models / Threat Models and Cascade Effects**
- **Service Level Agreements**
- **Enterprise Capability Maturity Model**
- **Designing in Privacy -> via patterns and architectures**
- **Insider Threat Detection**

**Thank-you
Questions?**