IG Perspective on Cloud Security

SA Bill Yurek
Program Director, Cyber Intrusions
NCIJTF / IC4 Liaison

What Needs to be Considered when Choosing Cloud Services?

- COST
- AVAILABILITY
- Security
- Services
  - SaaS, PaaS, IaaS
  - Public, Private, Hybrid, VPC
- Reliability
- Capacity
- Connectivity
- Location
  - Data
  - Facilities

- Resilience
- Accessibility
- Compatibility
  - Existing resources
  - Future resources
  - Hardware and Software
- Ease of Upload / Download
- Termination factors

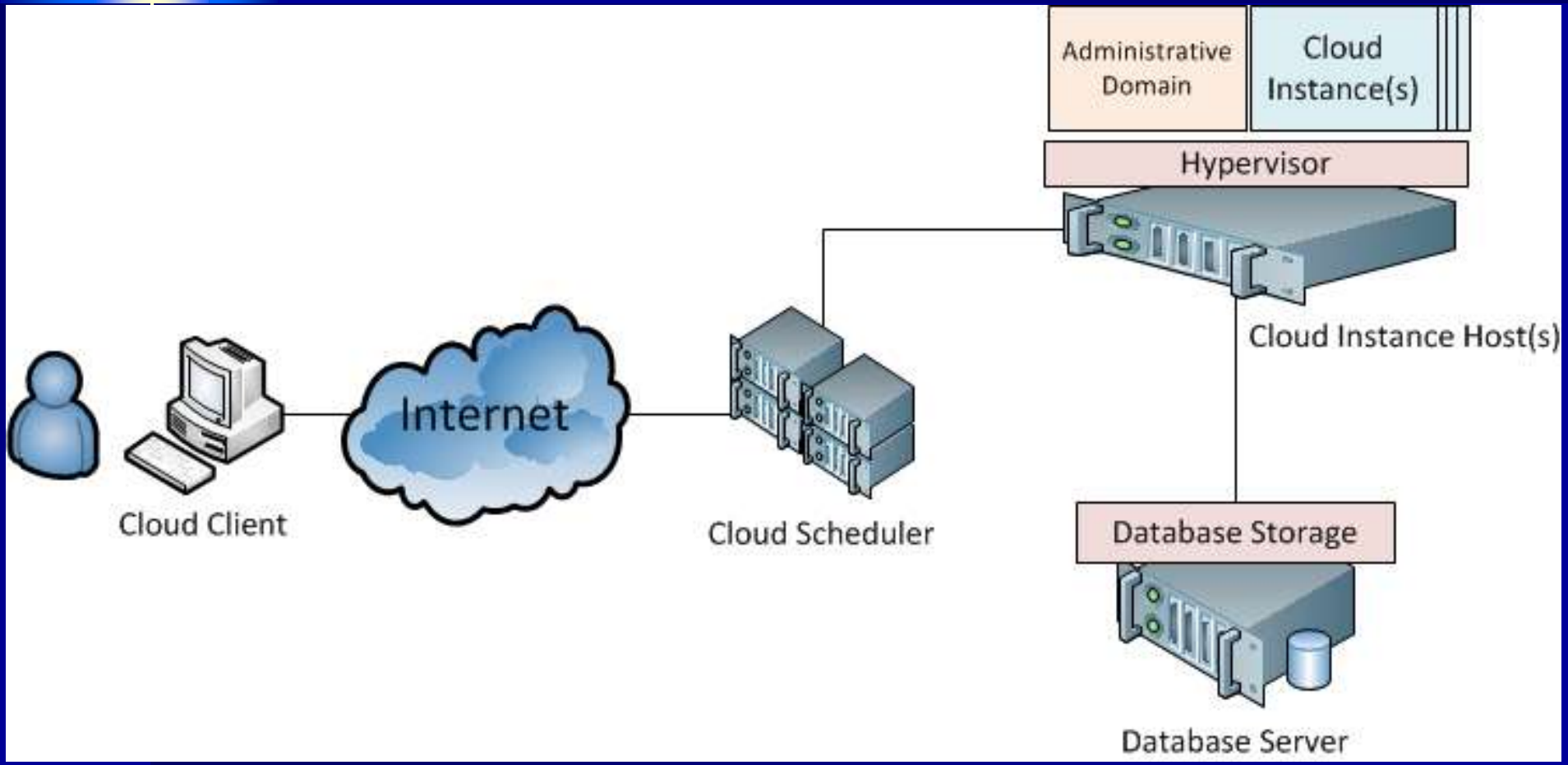
What Needs to be Considered when Choosing Cloud Services?

INVESTIGATABLE

"Investigatability"

- The decisions and choices made in the procurement and implementation of cloud services will impact the ability to investigate for a long time to come
- Who in your organization makes the decision?
  - One office? One person?
  - If a group, who is in the group?
  - Who / what office has the trump card? Is their primary value the organization's primary value?
  - "I never thought of that"
- When you see clouds, prepare for rain

Cloud Computing Architecture



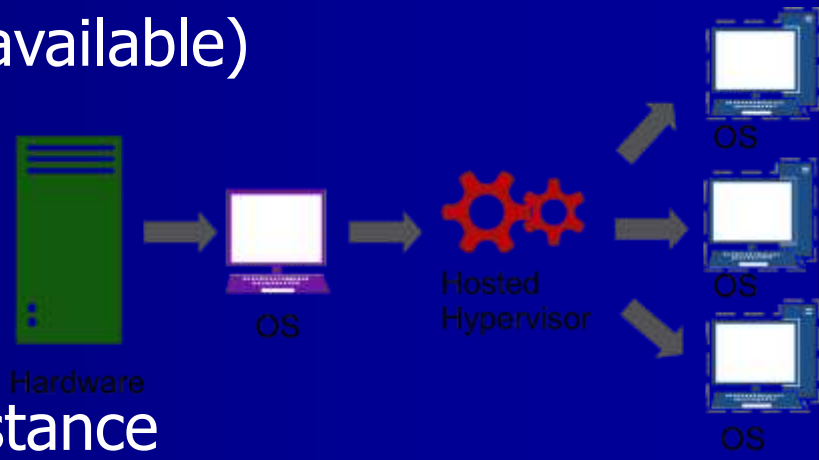
What do you control?

Forensics and Cloud Computing: Evidence Locations

- Cloud Client
  - Traditional forensics (hard disk, memory, etc.)
  - ISPs may also retain IP address allocations
- Cloud Scheduler/Manager
  - Logs of inbound connections, cloud instances and physical hardware used to service clients
  - Consumer account information, etc.
  - Internal cloud service provider audit logs
  - Authentication and access logs
    - Control granted to customers for use of applications and services
- Cloud Instances
  - Traditional forensics (hard disk, memory, etc.)
  - May require remote acquisition and credentials

Forensics and Cloud Computing: Evidence Locations

- Hypervisor
  - Dependent on type of hypervisor
  - Log files detailing cloud instance behavior
  - Cloud instance memory and disk state
  - VM introspection data (if available)
- Administrative Domain
  - Virtual disk images
  - Cloud instance memory
- Cloud Storage
  - Data stored by a cloud instance
- Physical Systems
  - Traditional acquisition of disks and memory



Cloud Computing Attack Vectors

- Traditional attacks against cloud instances
- Supply chain attacks against firmware and hardware of physical systems
- Virtualization break-out attacks
  - "Hyperjumping"
- Traditional insider threats within the consumer's organization
- Malicious insiders at the cloud provider
- Malicious cloud providers
- Foreign espionage facilitated by offshore hosting and data storage

Forensic Challenges in the Cloud

- Physical access limited at best: you don't own the hardware
- Cloud architectures vary between providers, affecting where evidence exists and how collection occurs
  - Traditional techniques can sometimes be used in cloud forensics. But this is very dependent on the level of investigator access.
- Data may be distributed across multiple jurisdictions
  - DFAR 239.7602-2
  - Microsoft v. U.S., 2nd Circuit, Jul 2016
- Cloud systems are large and, by their nature, constantly changing
  - Static acquisition can rarely find a static location
  - Passage of time rapidly overwrites / deletes data and logs

Forensic Challenges in the Cloud

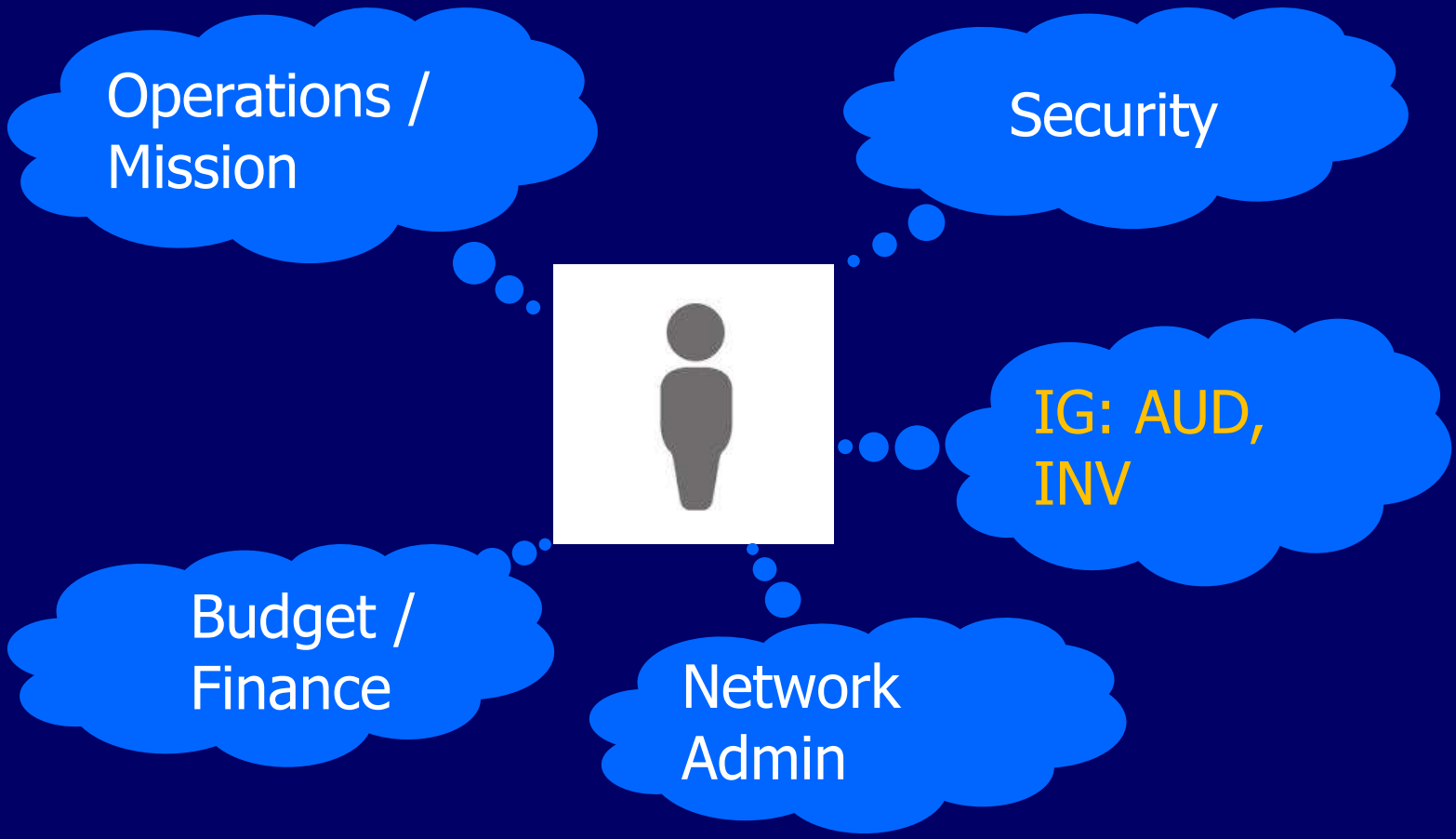
- **Malware**
  - Malware can function in virtual environments, and can even work its way into static systems if configuration is open.
  - Malware operating at the hardware level, or upper levels of virtualization (e.g. hypervisor) may be undetected if examination isn't at that level
- Clouds often service many customers
  - Each of them "owns" a constantly changing physical and virtual space
  - Forensics may cause service interruptions for other customers, may violate cloud provider SLA

Get Ahead of the Problem from the Outset

- In a cloud environment, security and investigatability considerations must be built into the contracting / procurement process

- Once that contract is signed, things become more difficult and more expensive

IG Involvement in Cloud Contracting and Storage Decisions



Negotiating and Procuring Cloud Services

- Generally, customers do not negotiate on an equal footing with providers
  - Especially true of customers with large scale requirements and/or those that have to comply with DFAR or other restrictions
- Local logging and data retention can be increased to provide more data, and more control over that data.

Negotiating and Procuring Cloud Services

- Talk with your security / investigative team about virtual / cloud analogs to current logs and monitoring
  - May have to get outside consulting. Or make that part of the contract
  - How long are they maintained? Can they be backed up / downloaded to your domestic system?
  - Access: Who what when where how
- What logging / intrusion detection / intrusion prevention software and processes does the cloud provider currently use?
  - Not just customer-level, but at provider level
  - Can you get that service directly? Can you get the data? How often? How readily?

Negotiating and Procuring Cloud Services

- Physical location of data? Can you access it? When/how?
  - Best data collection is at the source
- Monitoring capabilities? Real-time and on demand
  - Proprietary encryption?
- Can your contracted access rights be transferred to your agent (e.g. consultants, law enforcement)?
- Can you conduct security reviews / assessments on cloud resources?
  - Provider may consider some techniques as forbidden “malware”
- How will data be protected, conveyed, and destroyed?
  - Inquire into how data is deleted (affirmative deletion, overwrite, session destruction, etc.)

Outsourcing Security

- Can / will the provider do what you would do?
  - At what cost?
- Will provider security satisfy your contractual and compliance requirements?
- Remember, you can outsource security, but

  YOU CAN'T OUTSOURCE RESPONSIBILITY

Questions?

SA Bill Yurek
Defense Criminal Investigative Service
Cyber Intrusion Program Director
william.yurek@dodig.mil
(703) 699-5443