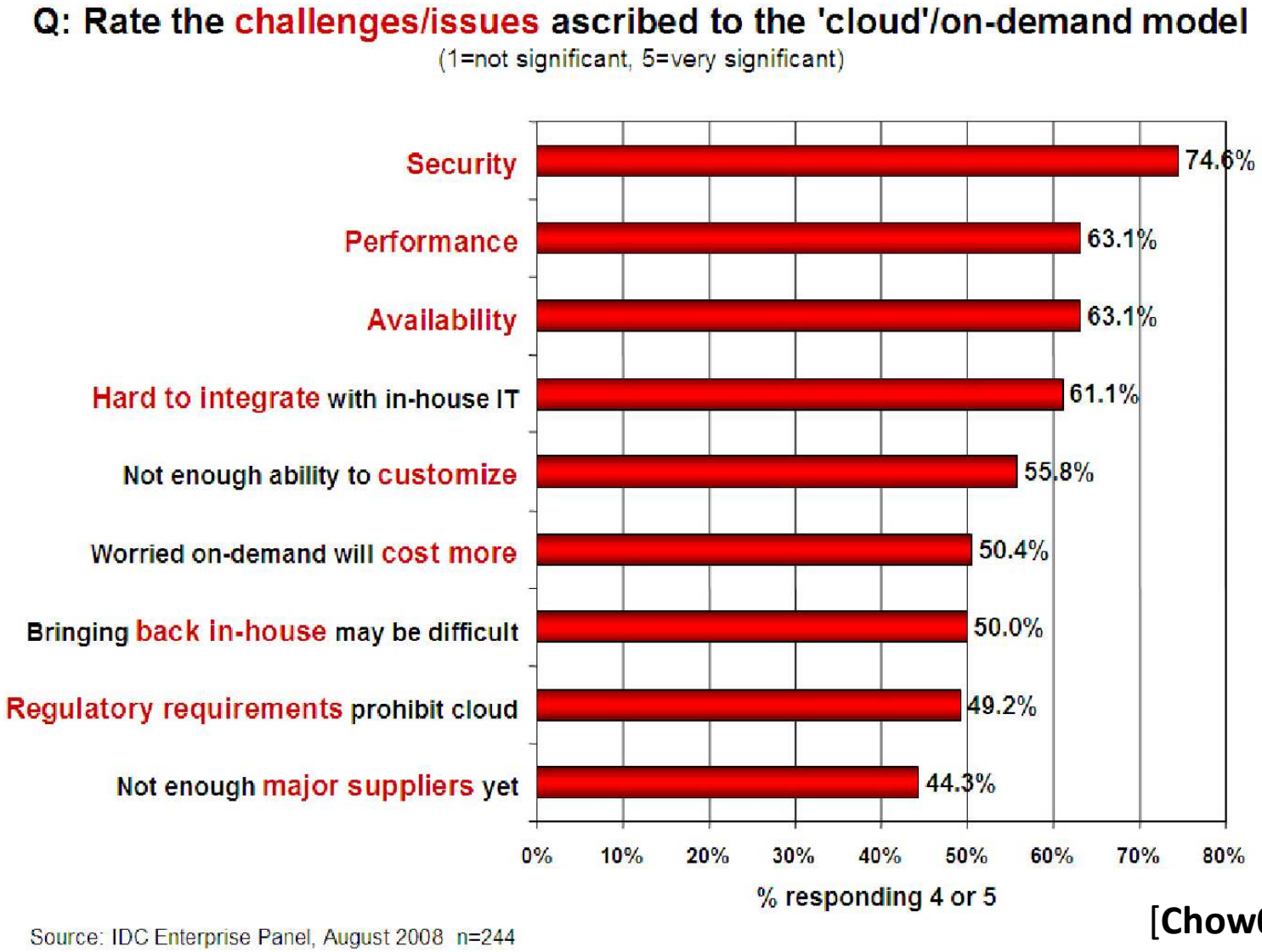
Research in Cloud Security and Privacy

Modified from Bharat Bhargava, Anya Kim, YounSun Cho

Outline

- Introduction
- Security and Privacy Issues in Cloud Computing
- Possible Solutions

Companies are afraid to use clouds



[Chow09ccsw]

Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Security and Privacy Issues in Cloud Computing - Big Picture

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
  - Processing of data, including multitenancy
    - For any application to process data

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Data Security and Storage (cont.)

- Data lineage
  - Knowing when and where the data was located w/i cloud is important for audit/compliance purposes
  - e.g., Amazon AWS
    - Store <d1, t1, ex1.s3.amazonaws.com>
    - Process <d2, t2, ec2.compute2.amazonaws.com>
    - Restore <d3, t3, ex2.s3.amazonaws.com>
- Data provenance
  - Computational accuracy (as well as data integrity)
  - E.g., financial calculation: sum ((((2*3)*4)/6) -2) = $2.00 ?
    - How about dollars of different countries?
    - Correct exchange rate?
- Data remanence
  - Inadvertent disclosure of sensitive information is possible

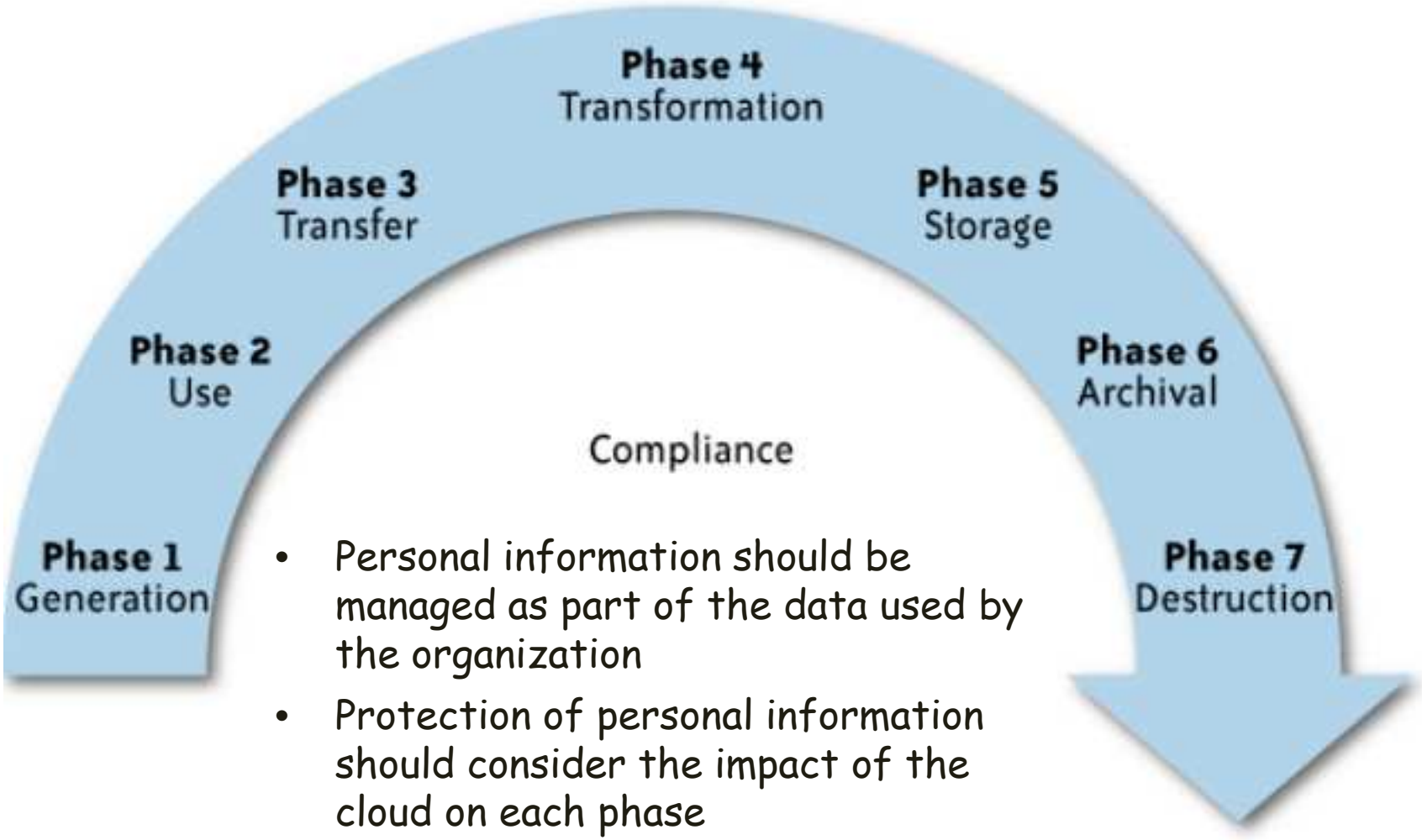
From [6] Cloud Security and Privacy by Mather and Kumaraswamy

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations;
  - as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

What is the data life cycle?



- Personal information should be managed as part of the data used by the organization
- Protection of personal information should consider the impact of the cloud on each phase

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Storage

- Is it commingled with information from other organizations that use the same CSP?
- The aggregation of data raises new privacy issues
  - Some governments may decide to search through data without necessarily notifying the data owner, depending on where the data resides
- Whether the cloud provider itself has any right to see and access customer data?
- Some services today track user behaviour for a range of purposes, from sending targeted advertising to improving services

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Retention

- How long is personal information (that is transferred to the cloud) retained?
- Which retention policy governs the data?
- Does the organization own the data, or the CSP?
- Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Destruction

- How does the cloud provider destroy PII at the end of the retention period?
- How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?
- Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide.
  - How do you know that the CSP didn't retain additional copies?
  - Did the CSP really destroy the data, or just make it inaccessible to the organization?
  - Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Auditing, monitoring and risk management

- How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.
  - These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Privacy breaches

- How do you know that a breach has occurred?
- How do you ensure that the CSP notifies you when a breach occurs?
- Who is responsible for managing the breach notification process (and costs associated with the process)?
- If contracts include liability for breaches resulting from negligence of the CSP?
  - How is the contract enforced?
  - How is it determined who is at fault?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Who is responsible for protecting privacy?

- Do
- e.g., Suppose a hacker breaks into Cloud Provider A and steals data from Company X. Assume that the compromised server also contained data from Companies Y and Z.
  - Who investigates this crime?
  - Is it the Cloud Provider, even though Company X may fear that the provider will try to absolve itself from responsibility?
  - Is it Company X and, if so, does it have the right to see other data on that server, including logs that may show access to the data of Companies Y and Z?
- stew
- Organizations can trans[illegible]liability, but not accountability
- Risk assessment and mitigation throughout the data life cycle is cr[illegible]cal.
- Many new risks and unknowns
  - The overall complexity of privacy protection in the cloud represents a bigger challenge.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Possible Solutions

Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud
      - But can they be managed in some way by the consumer?
  - Lack of trust
    - Increase trust (mechanisms)
      - Technology
      - Policy, regulation
      - Contracts (incentives)
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

Third Party Cloud Computing

- Known issues: Already exist

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

More on attacks…

- Collaborative attacks
- Mapping of internal cloud infrastructure
- Identifying likely residence of a target VM
- Instantiating new VMs until one gets co-resident with the target
- Cross-VM side-channel attacks
- Extract information from target VM on the same machine

More on attacks…

1. Can one determine where in the cloud infrastructure an instance is located?
2. Can one easily determine if two instances are co-resident on the same physical machine?
3. Can an adversary launch instances that will be co-resident with other user instances?
4. Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all

Minimize Lack of Trust: Policy Language

- Consumers have specific security needs but don't have a say-so in how they are handled
  - Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
- Standard language to convey one's policies and expectations
  - Agreed upon and upheld by both parties
  - Standard language for representing SLAs
- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable),
  - Easy to combine/merge and compare

Minimize Lack of Trust: Certification

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
    - Sarbanes-Oxley, DIACAP, DISTCAP, etc
- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail, what is the effect of the failure to the mission logic
  - What recovery measures can be taken
    - by provider and consumer
- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping
    - create new or move existing fault domains
  - shutting down offending components or targets
    - and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle
  - application-level monitoring
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user's application to another cloud

Minimize Loss of Control: Utilize Different Clouds

- The concept of 'Don't put all your eggs in one basket'
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - A multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
    - Increase chance of mission completion for critical applications
  - Possible issues to consider:
    - Policy incompatibility (combined, what is the overarching policy?)
    - Data dependency between clouds
    - Differing data semantics across clouds
    - Knowing when to utilize the redundancy feature
      - monitoring technology
    - Is it worth it to spread your sensitive data across multiple clouds?
      - Redundancy could increase risk of exposure

Minimize Loss of Control: Access Control

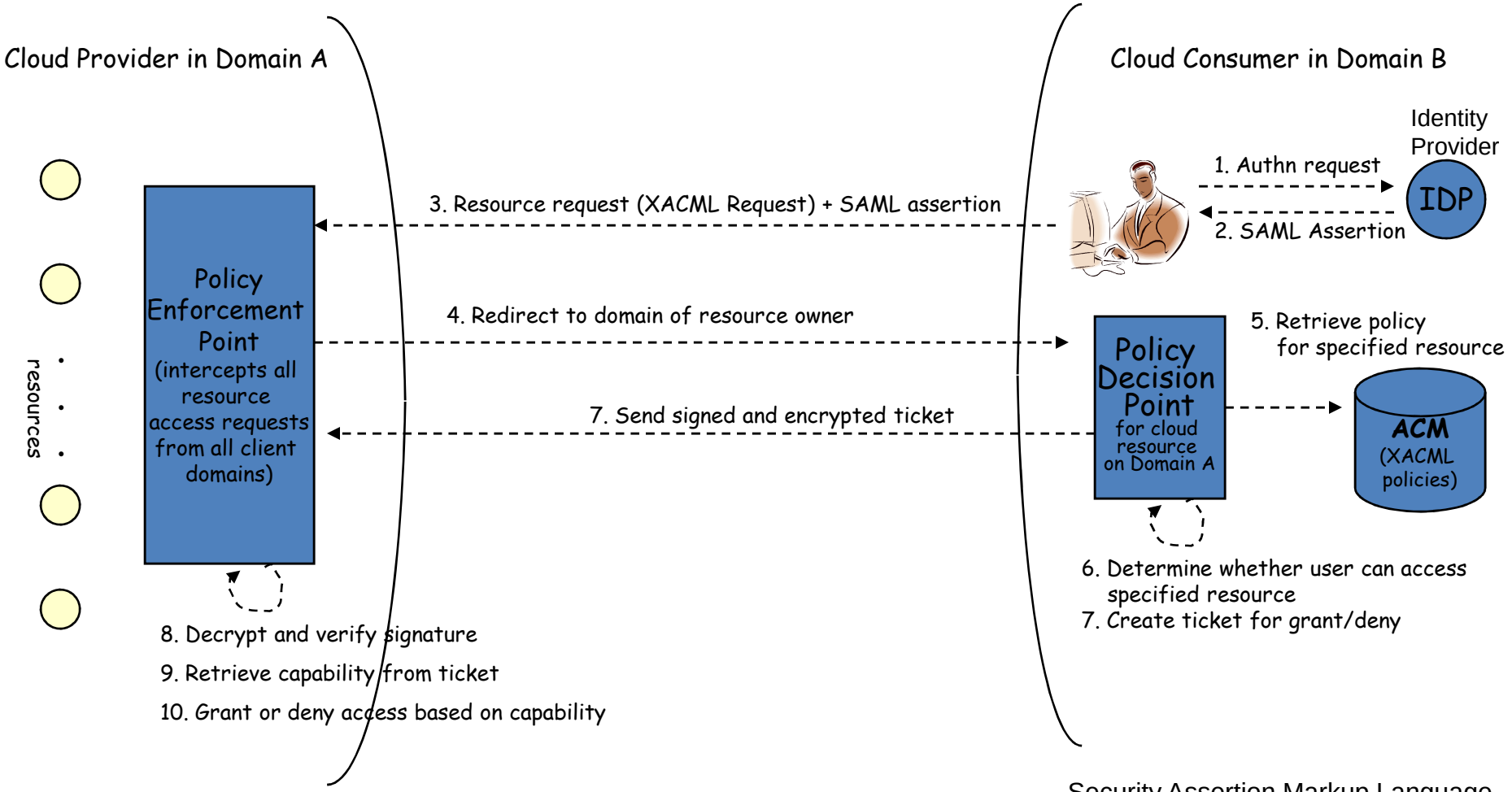
- Many possible layers of access control
  - E.g. access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM
  - Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer

- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
  - Federated Identity Management: access control management burden still lies with the provider
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies.
    - This can be burdensome when numerous users from different organizations with different access control policies, are involved

Minimize Loss of Control: Access Control (Cont.)

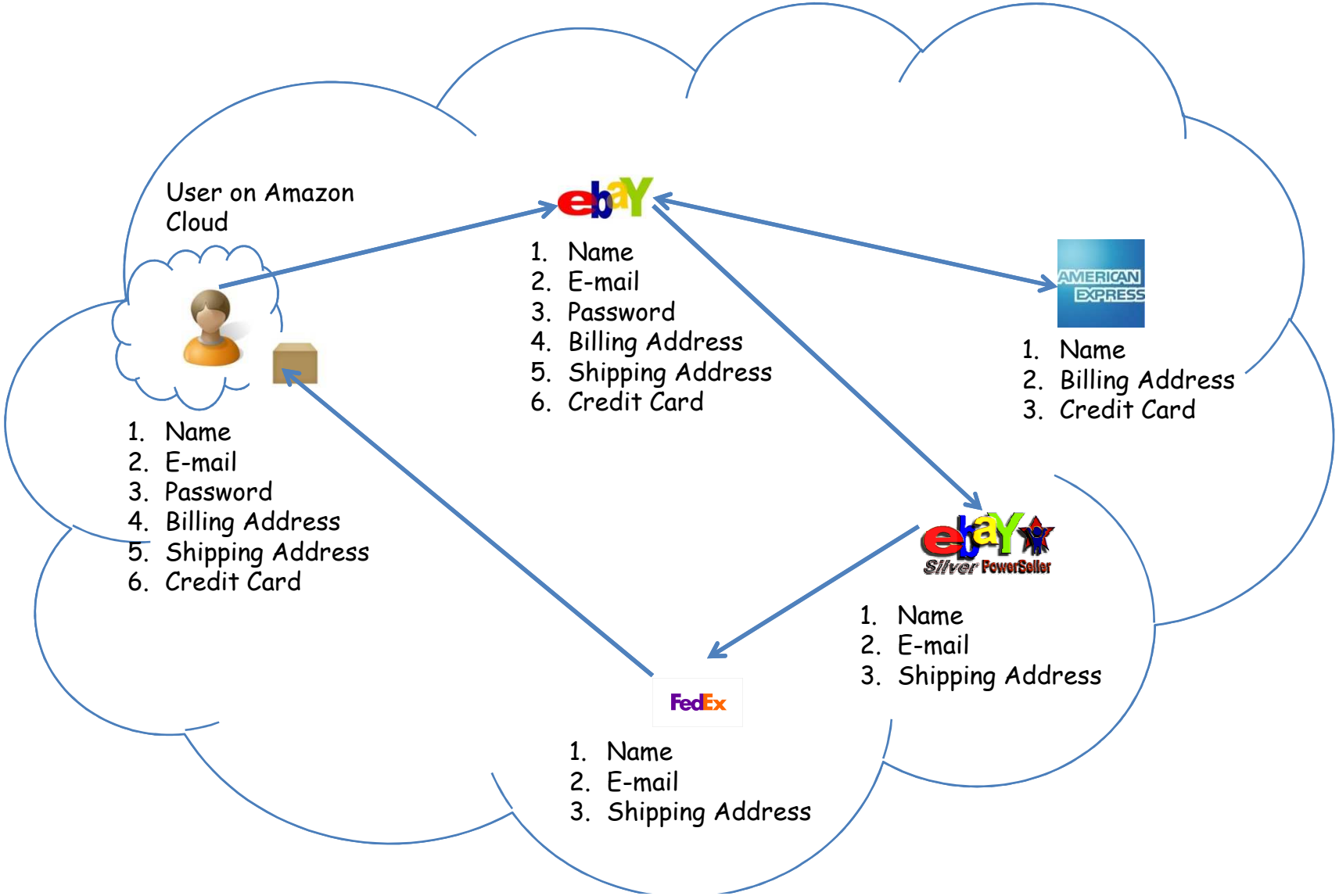
- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider
  - Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer.
    - It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.
  - Should be at least as secure as the traditional access control model.

Minimize Loss of Control: Access Control



Security Assertion Markup Language
eXtensible Access Control Markup Language

Minimize Loss of Control: IDM Motivation



Minimize Loss of Control: IDM Identity in the Cloud

Minimize Loss of Control: IDM Issues in Cloud Computing

- Cloud introduces several issues to IDM
  - Users have **multiple accounts** associated with **multiple service providers.**
  - Present IDMs require a **trusted third party** and do not work on an **untrusted host.**
  - Lack of trust
    - Use of Trusted Third Party is not an option
    - Cloud hosts are untrusted
  - Loss of control
    - Collusion between Cloud Services
      - Sharing sensitive identity information between services can lead to undesirable **mapping of the identities to the user.**

IDM in Cloud needs to be user-centric

Minimize Multi-tenancy

- Can't really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
      - C.f. VM Side channel attacks (T. Ristenpart et al.)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who's the insider, where's the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

References

1. NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).
2. J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.
3. J. Camp. (2001), "Trust and Risk in Internet Commerce," MIT Press
4. T. Ristenpart et al. (2009) "Hey You Get Off My Cloud," Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA
5. Security and Privacy in Cloud Computing, Dept. of CS at Johns Hopkins University. www.cs.jhu.edu/~ragib/sp10/cs412
6. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and Subra Kumaraswamy
7. Afraid of outside cloud attacks? You're missing the real threat. http://www.infoworld.com/d/cloud-computing/afraid-outside-cloud-attacks-youre-missing-real-threat-894
8. **Amazon downplays report highlighting vulnerabilities in its cloud service. http://www.computerworld.com/s/article/9140074/Amazon_downplays_report_highlighting_vulnerabilities_in_its_cloud_service**
9. **Targeted Attacks Possible in the Cloud, Researchers Warn. http://www.cio.com/article/506136/Targeted_Attacks_Possible_in_the_Cloud_Researchers_Warn**
10. **Vulnerability Seen in Amazon's Cloud-Computing by David Talbot. http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf**
11. **Cloud Computing Security Considerations by Roger Halbheer and Doug Cavit. January 2010. http://blogs.technet.com/b/rhalbheer/archive/2010/01/30/cloud-security-paper-looking-for-feedback.aspx**
12. **Security in Cloud Computing Overview.http://www.halbheer.info/security/2010/01/30/cloud-security-paper-looking-for-feedback**
13. **Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds by T. Ristenpart, E. Tromer, H. Shacham and Stefan Savage. CCS'09**
14. **Cloud Computing Security. http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html**
15. **Update From Amazon Regarding Friday's S3 Downtime by Allen Stern. Feb. 16, 2008. http://www.centernetworks.com/amazon-s3-downtime-update**
16. R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, "Protection of Identity Information in Cloud Computing without Trusted Third Party," Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
17. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane, "A User-Centric Approach for Privacy and Identity Management in Cloud Computing," 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
18. H. Khandelwal, *et al.*, "Cloud Monitoring Framework," Purdue University. Dec 2010.

Other References for Cloud Security

- M. Armbrust, *et al.*, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems LaboratoryFebruary 10 2009.
- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2009.
- M. Jensen, *et al.*, "On Technical Security Issues in Cloud Computing," presented at the 2009 IEEE International Conference on Cloud Computing, Bangalore, India 2009.
- P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2009.
- N. Santos, *et al.*, "Towards Trusted Cloud Computing," in *Usenix 09 Hot Cloud Workshop*, San Diego, CA, 2009.
- R. G. Lennon, *et al.*, "Best practices in cloud computing: designing for the cloud," presented at the Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, 2009.
- P. Mell and T. Grance, "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology LaboratoryOctober 7 2009.
- C. Cachin, *et al.*, "Trusting the cloud," *SIGACT News,* vol. 40, pp. 81-86, 2009.
- J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner 2008.
- A. Joch. (2009, June 18) Cloud Computing: Is It Secure Enough? *Federal Computer Week*.
- AWS Amazon EC2: http://aws.amazon.com/ec2/
- Amazon CloudWatch: http://aws.amazon.com/cloudwatch/
- Iperf: http://iperf.sourceforge.net/

Cloud Blind References

- L. Ran, A. Helal, and S. Moore, "Drishti: An Integrated Indoor/Outdoor Blind Navigation System and Service," 2nd IEEE Pervasive Computing Conference (PerCom 04).
- S.Willis, and A. Helal, "RFID Information Grid and Wearable Computing Solution to the Problem of Wayfinding for the Blind User in a Campus Environment," IEEE International Symposium on Wearable Computers (ISWC 05).
- Y. Sonnenblick. "An Indoor Navigation System for Blind Individuals," Proceedings of the 13th Annual Conference on Technology and Persons with Disabilities, 1998.
- J. Wilson, B. N. Walker, J. Lindsay, C. Cambias, F. Dellaert. "SWAN: System for Wearable Audio Navigation," 11th IEEE International Symposium on Wearable Computers, 2007.
- J. Nicholson, V. Kulyukin, D. Coster, "ShopTalk: Independent Blind Shopping Through Verbal Route Directions and Barcode Scans," The Open Rehabilitation Journal, vol. 2, 2009, pp. 11-23.
- Bach-y-Rita, P., M.E. Tyler and K.A. Kaczmarek. "Seeing with the Brain," International Journal of Human-Computer Interaction, vol 15, issue 2, 2003, pp 285-295.
- Y.K. Kim, K.W. Kim, and X.Yang, "Real Time Traffic Light Recognition System for Color Vision Deficiencies," IEEE International Conference on Mechatronics and Automation (ICMA 07).
- R. Charette, and F. Nashashibi, "Real Time Visual Traffic Lights Recognition Based on Spot Light Detection and Adaptive Traffic Lights Templates," World Congress and Exhibition on Intelligent Transport Systems and Services (ITS 09).
- A.Ess, B. Leibe, K. Schindler, and L. van Gool, "Moving Obstacle Detection in Highly Dynamic Scenes," IEEE International Conference on Robotics and Automation (ICRA 09).
- P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L. B. Othmane, "A User-centric Approach for Privacy and Identity Management in Cloud Computing," submitted to SRDS 2010.