IoT: Cloud Services

Cloud security

Introduction

- Cloud is a massive concentration of resources
- Also a massive concentration of risk expected loss from a single breach
- It can be significantly larger concentration of "users" represents a concentration of threats
  - "*Ultimately, you can outsource responsibility but you can't outsource accountability.*" From [2] John McDermott, ACSAC 09

Cloud Security

Security is one of the most difficult task to implement in cloud computing.

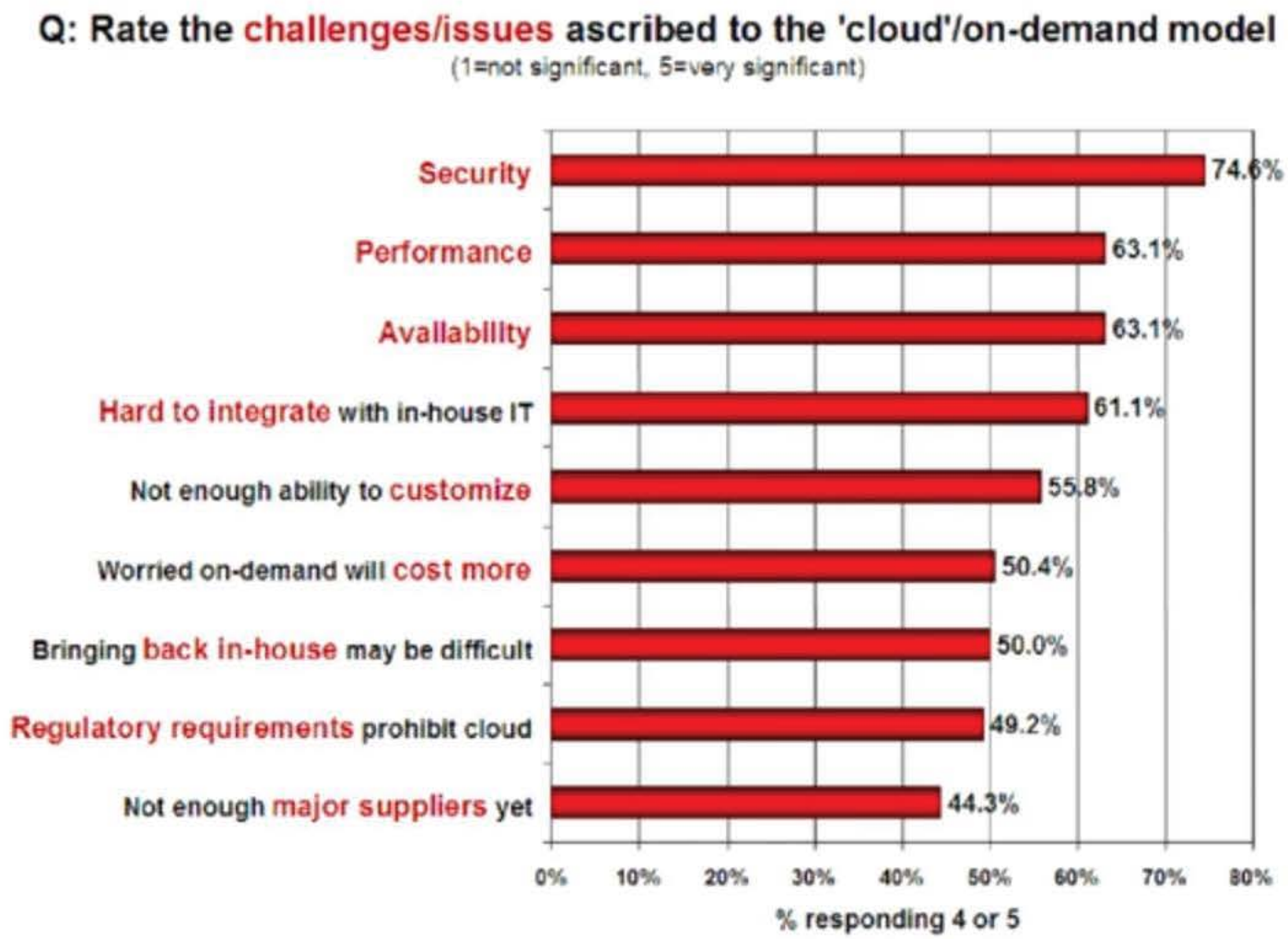
- Different forms of attacks in the application side and in the hardware components

Attacks with catastrophic effects only needs one security flaw

Why is everybody not moving to the Cloud?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Security is a paramount challenge



Source: IDC Enterprise Panel, August 2008 n=244

IoT: Cloud Services

Security Problems

Cause of Cloud security problems

- 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

Loss of Control

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust

- **Trusting a third party requires taking risks**
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed towards the same path?

Lack of Trust

- What if the Cloud provider has a conflicting business?
  - For example Amazon sells products, streams movies and music, offers an online grocery and many others
  - How do companies like Netflix, Lyft etc use AWS although they have a competitive product?
  - How does Amazon, as a Cloud provider benefit from having these companies run their infrastructure on AWS?

Multi-Tenancy

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

Multi-Tenancy

- Cloud Computing brings new threats
- Multiple independent users share the same physical infrastructure
- Thus an attacker can legitimately be in the same physical machine as the target

Core Issue

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

IoT: Cloud Services

Taxonomy of Fear

Confidentiality & Integrity

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Availability

- Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
- What happens if cloud provider goes out of business?
- Would cloud scale well-enough?
- Often-voiced concern
  - Although cloud providers argue their downtime compares well with cloud user's own data centers

More fears…

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

Auditability and Forensics

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

IoT: Cloud Services

Threat Model

What is a threat model?

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

Why thread model is useful?

- Threat modeling is useful in any software context, but is particularly valuable in cloud computing due to the widespread preoccupation with security.
- It's also useful because technical and non-technical people alike can follow the diagrams easily.

Threat Model components

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

Malicious Insider

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

Outside Attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

Thread modeling in Cloud Computing

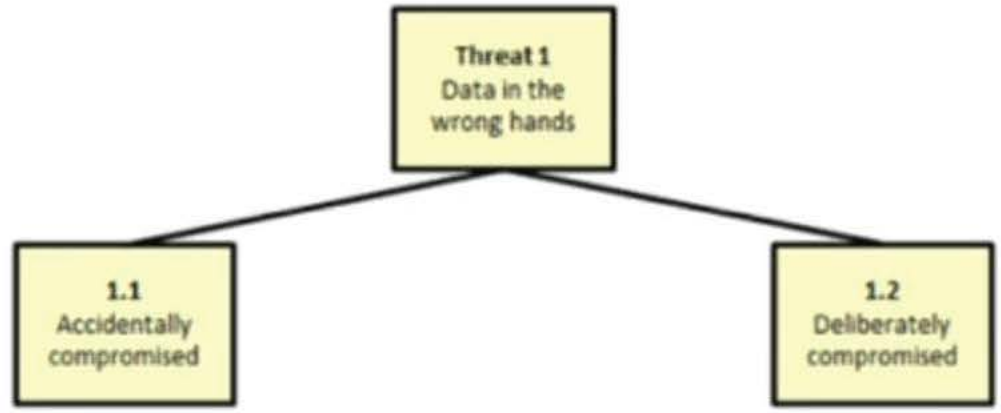
- A common concern is that the use of shared resources in the cloud might compromise the security of your data by allowing it to fall into the wrong hands—what we call *Data Isolation Failure*.

- A data isolation failure is one of the primary risks organizations considering cloud computing worry about.

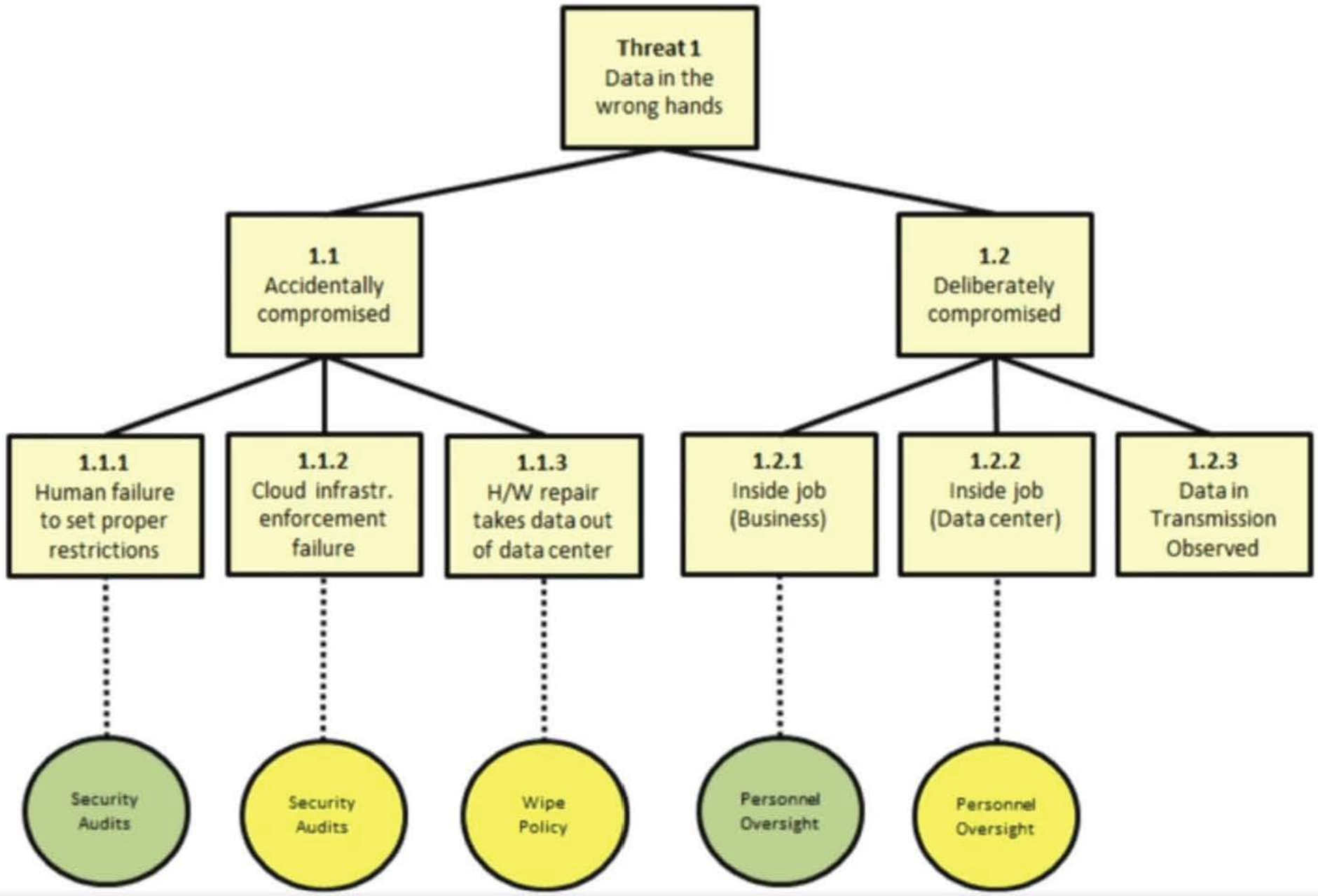
- To create our threat model, we'll start with the end result we're trying to avoid: data in the wrong hands.

What can lead to this result?

Either one of these conditions is sufficient to cause data to be in the wrong hands, so this is an OR condition. We'll see later on how to show an AND condition.



Threat Modeling and Mitigations



Challenges for Attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?