SECURITY IN COMPUTING, FIFTH EDITION

Chapter 8: Cloud Computing

Objectives for Chapter 8

- Define cloud services, including types and service models
- How to define cloud service requirements and identify appropriate services

- Survey cloud-based security capabilities and offerings

- Discuss cloud storage encryption considerations
- Protection of cloud-based applications and infrastructures
- Explain the major federated identity management standards and how they differ

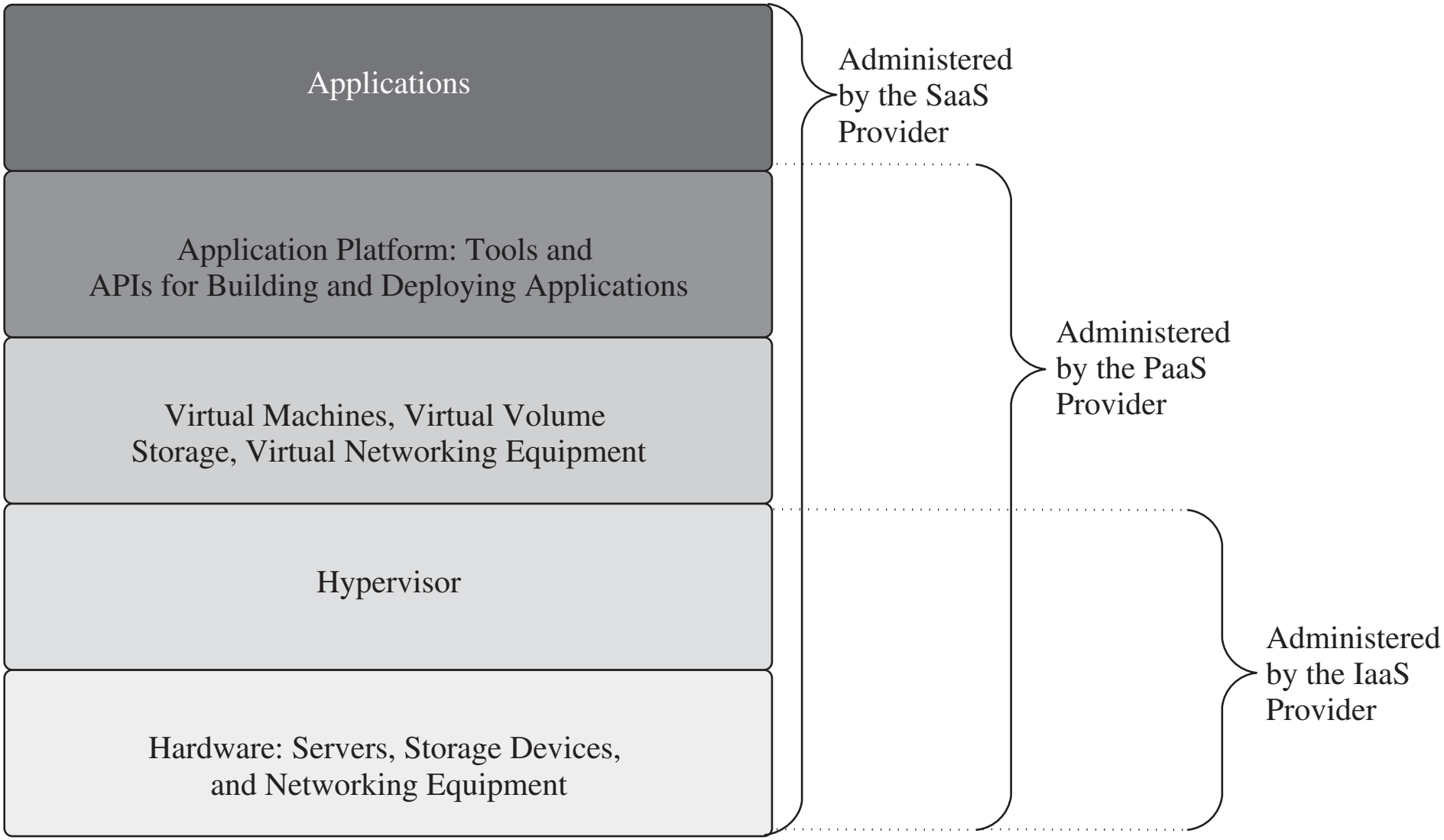
What Is Cloud Computing?

- On-demand self-service
  - Add or subtract resources as necessary
- Broad network access
  - Mobile, desktop, mainframe
- Resource pooling
  - Multiple tenants share resources that can be reassigned dynamically according to need and invisibly to the tenants
- Rapid elasticity
  - Services can quickly and automatically scale up or down to meet customer need
- Measure service
  - Like water, gas, or telephone service, usage can be monitored for billing

Service Models

- Software as a service (SaaS)
  - The cloud provider gives the customer access to applications running in the cloud
- Platform as a service (PaaS)
  - The customer has his or her own applications, but the cloud provides the languages and tools for creating and running them
- Infrastructure as a service (IaaS)
  - The cloud provider offers processing, storage, networks, and other computing resources that enable customers to run any kind of software

Service Models



Deployment Models

- Private cloud
  - Infrastructure that is operated exclusively by and for the organization that owns it
- Community cloud
  - Shared by several organizations with common needs, interests, or goals
- Public cloud
  - Owned by a cloud service provider and offered to the general public
- Hybrid cloud
  - Composed of two or more types of clouds, connected by technology that enables data and applications to balance loads among those clouds

Cloud Migration Risk Analysis

- Identify assets
- Determine vulnerabilities
- Estimate likelihood of exploitation
- Compute expected loss
- Survey and select new controls
- Project savings

Cloud Provider Assessment

- Security issues to consider:
  - Authentication, authorization, and access control options
  - Encryption options
  - Audit logging capabilities
  - Incident response capabilities
  - Reliability and uptime
- Resources to help with assessment:
  - FedRAMP
  - PCI DSS
  - CSA STAR

Security Benefits of Cloud Services

- Geographic diversity
  - Many cloud providers run data centers in disparate geographic locations and mirror data across locations, providing protection from natural and other local disasters.
- Platform and infrastructure diversity
  - Different platforms and infrastructures mean different bugs and vulnerabilities, which makes a single attack or error less likely to bring a system down. Using cloud services as part of a larger system can be a good way to diversify your technology stack.

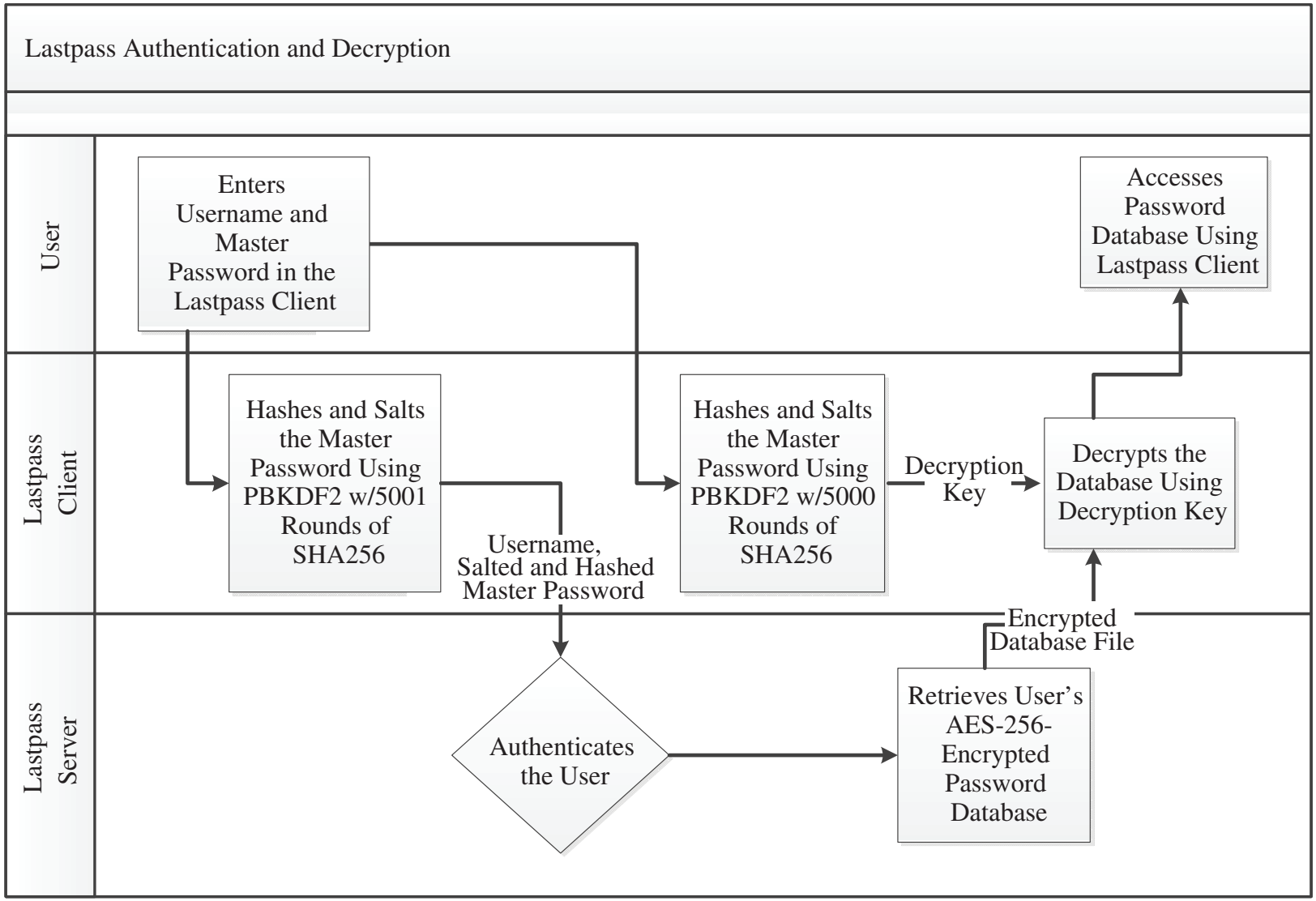
Cloud-Based Security Functions

- Some security functions may be best handled by cloud service providers:
  - Email filtering
    - Since email is already hopping through a variety of SMTP servers, adding a cloud-based email filter is as simple as adding another hop.
  - DDoS protection
    - Cloud-based DDoS protection services update your DNS records to insert their servers as proxies in front of yours. They maintain sufficient bandwidth to handle the flood of attack traffic.
  - Network monitoring
    - Cloud-based solutions can help customers deal with steep hardware requirements and can provide monitoring and incident response expertise.
- Discussion Topic: DDoS protection via cloud – pros and cons are?

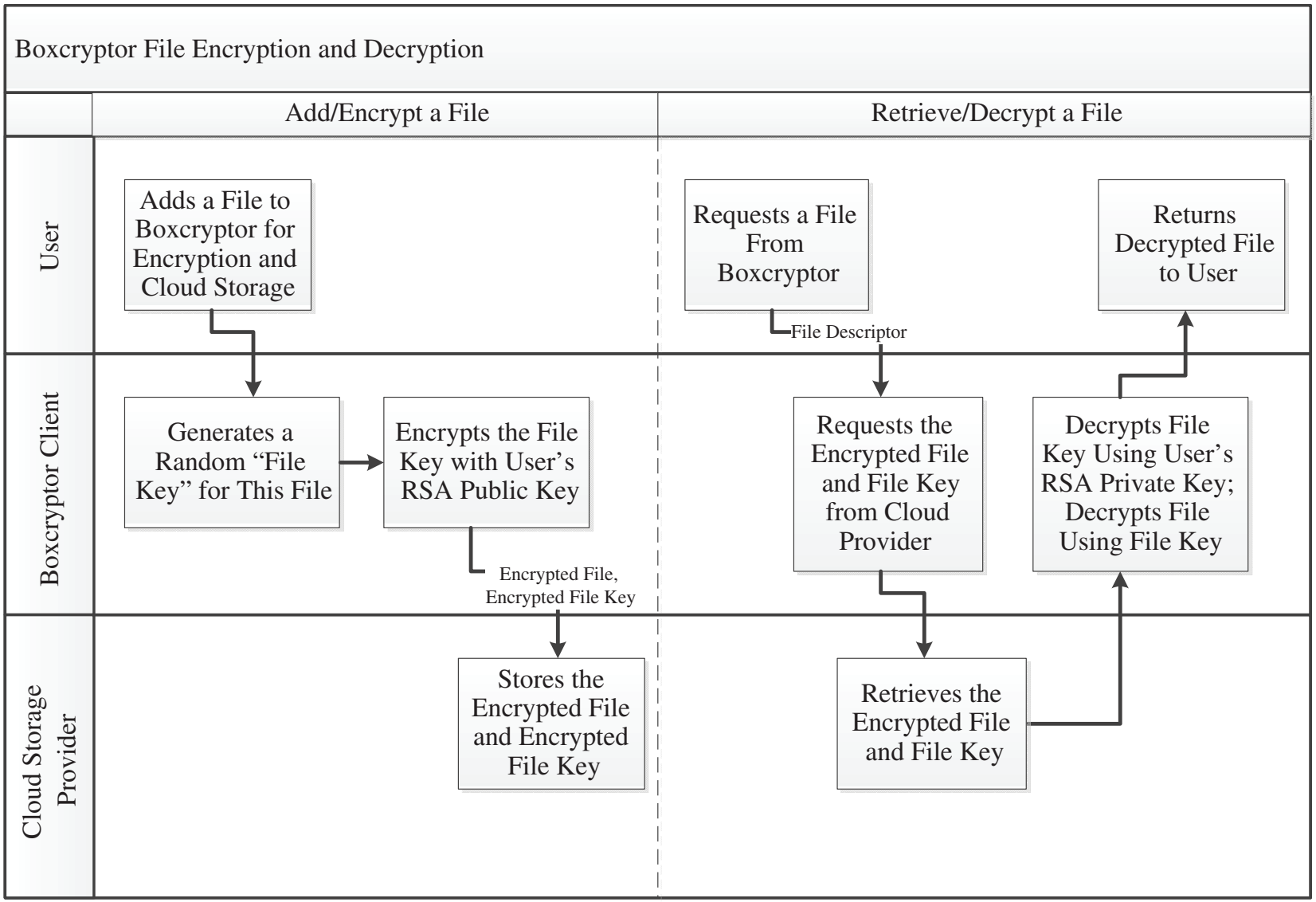
Cloud Storage

- By default, most cloud storage solutions either store users' data unencrypted or encrypt all data for all customers using a single key and therefore don't provide strong confidentiality
- Some cloud services provide better confidentiality by generating keys on a per-user basis based on that user's password or some other secret
- For maximum confidentiality, some cloud providers embrace a trust no one (TNO) model in which even the provider does not have the keys to decrypt user data

Lastpass TNO Implementation



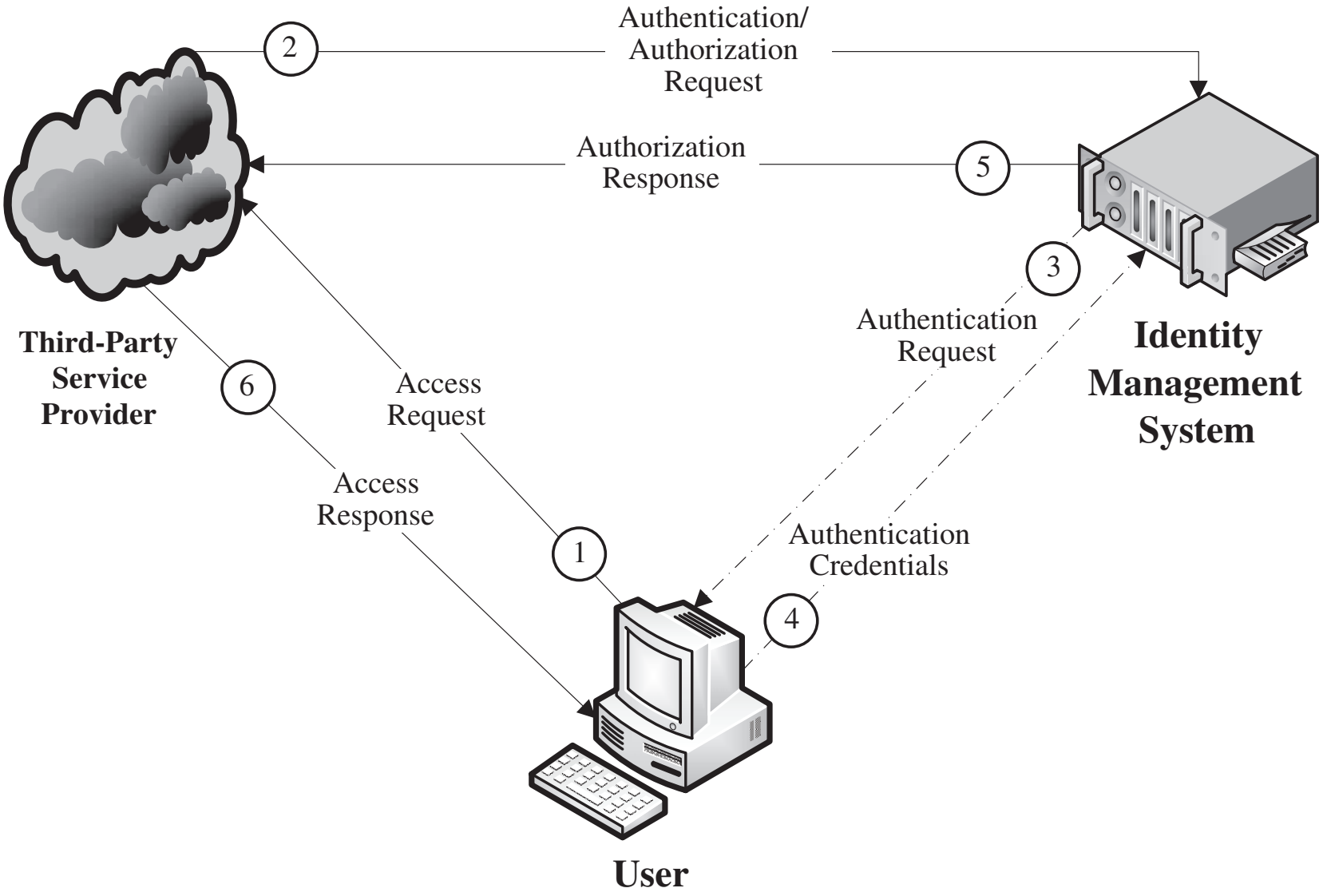
Boxcryptor TNO Implementation



Cloud Application Security

- Attacks against shared resources
  - Shared computing resources change the threat landscape. Sharing a system with a vulnerable application may result in those shared resources becoming compromised and consequently spreading attacks to your applications. There are also attacks, such as cryptographic side-channel attacks, that specifically target shared resource environments.
- Attacks against insecure APIs
  - Cloud vendors have a history of using known broken APIs. A recent survey of cloud security incidents over a 5-year period found that almost one-third of those incidents were caused by insecure interfaces and APIs.[1] A separate study found major security weaknesses in SSL libraries used by major cloud service providers, including Amazon and PayPal.[2]

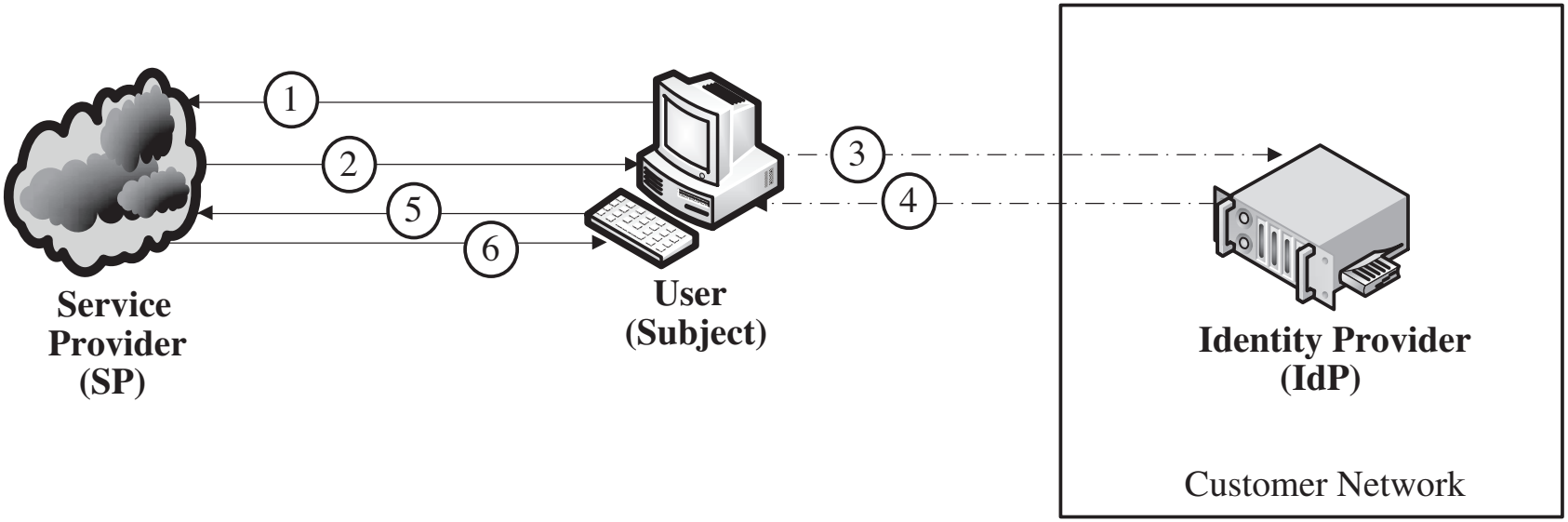
Federated Identity Management (FIdM)



Security Assertion Markup Language (SAML)

- An XML-based standard that defines a way for systems to securely exchange user identity and privilege information
- Commonly used when a company wants to give its employees access to corporate cloud service subscriptions
- If an employee leaves the company, his corporate login credentials are disabled and, by extension, so are his login rights to the cloud service

SAML Authentication Process



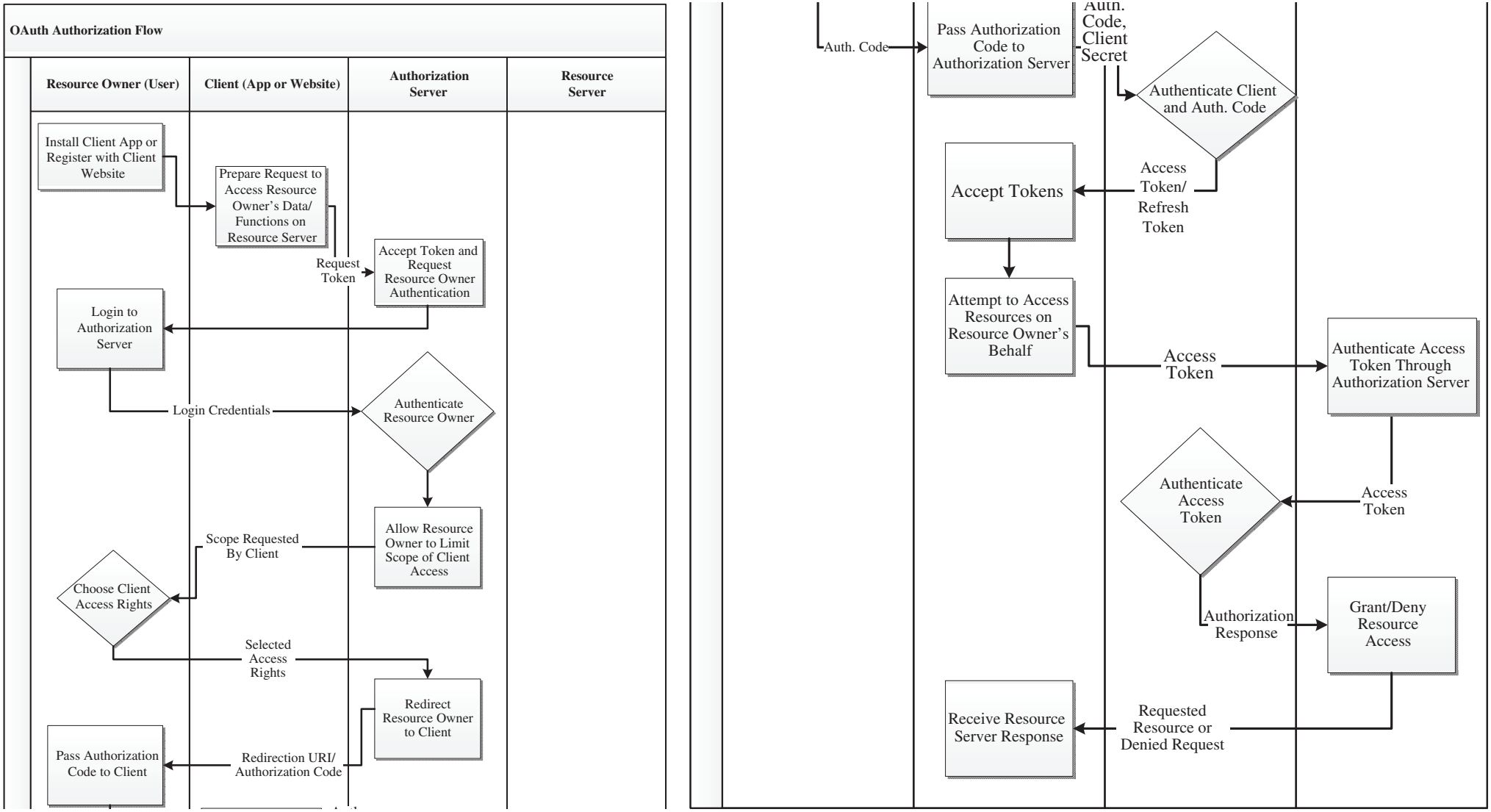
SAML Authentication Process

1. Subject navigates to the SP site for login
2. SP sends the subject's browser an authentication request
3. Browser relays the authentication request to the IdP
4. IdP attempts to authenticate the subject, then returns the authentication response to the browser
5. Browser relays the authentication response to the SP
6. SP reads the authentication response and, if the user is authorized, logs the user in with the privileges the IdP specified

OAuth

- Whereas SAML is an authentication standard, OAuth is an authorization standard
- OAuth enables a user to allow third-party applications to access APIs on that user's behalf
- When Facebook asks a user if a new application can have access to his photos, that's OAuth
- OAuth allows users to give third-party applications access to only the account resources they need, and to do so without sharing passwords; users can revoke access at any time

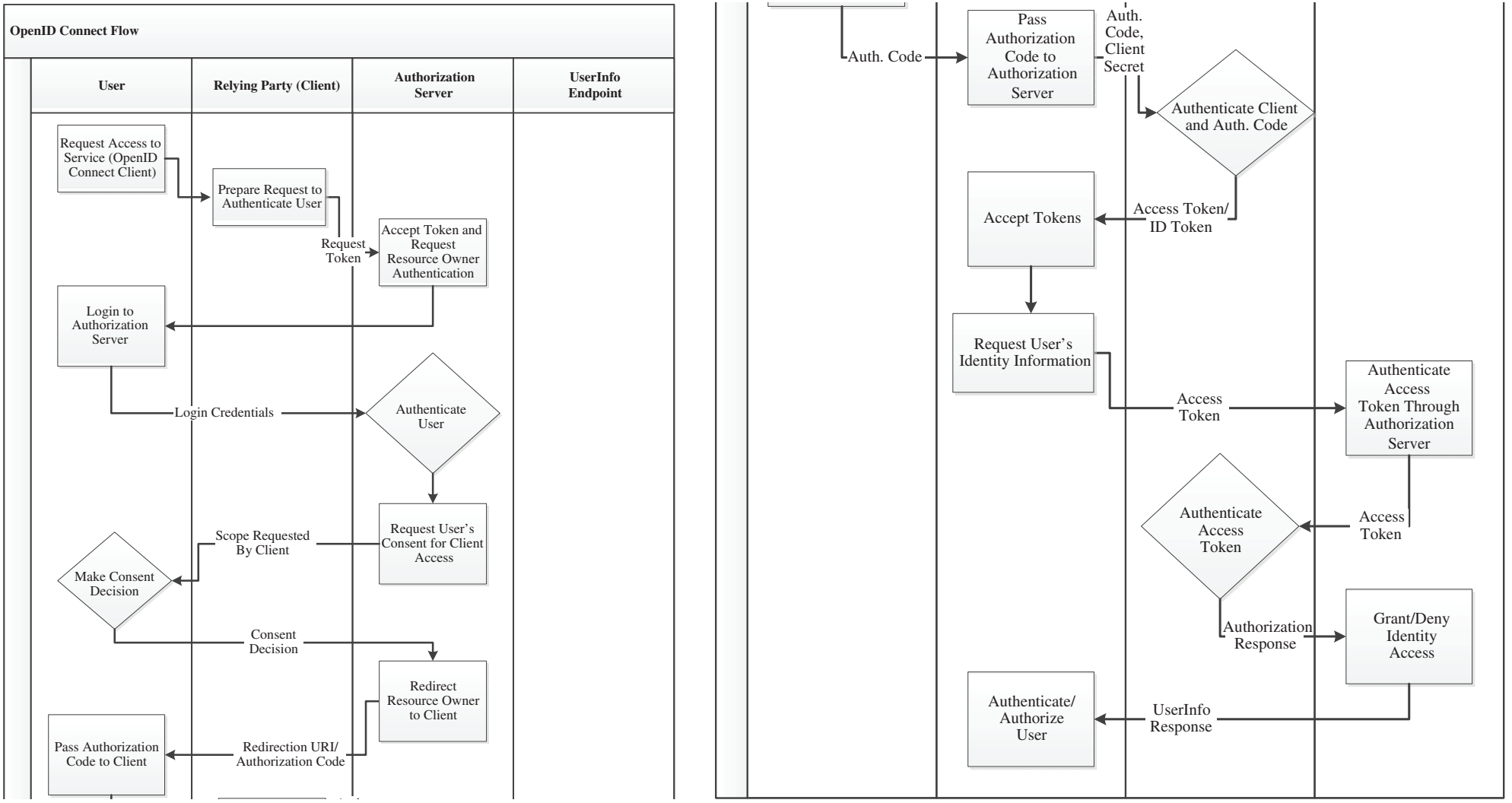
OAuth Authorization



OpenID Connect (OIDC)

- OAuth has been extended to support authentication in the form of OIDC
- OIDC is a relatively new standard for FIdM
- OIDC provides much better support for native applications (versus web applications) than does SAML
- Works by adding an identity token to the existing authorization tokens, essentially treating identity information as another authorization right

OIDC Authentication



Securing IaaS

- Shared storage
  - When you deallocate shared storage, it gets reallocated to other users, potentially exposing your data. Encrypted storage volumes are the most reliable mitigation.
- Shared network
  - Typical practice among IaaS providers prevents users from sniffing one another's network traffic, but the safest bet is to encrypt all network traffic to and from virtual machines whenever possible
- Host access
  - Require two-factor authentication
  - Do not use shared accounts
  - Enforce the principle of least privilege
  - Use OAuth rather than passwords to give applications access to API interfaces
  - Use FIdM wherever possible so as to only manage one set of accounts

Summary

- When considering a move to cloud infrastructure, a full risk assessment will reveal critical requirements and bring up important unexpected issues
- Cloud storage encryption options vary widely—confidentiality requirements are a key consideration
- FIdM, including SAML, OAuth, and OIDC, provides strong security benefits by centralizing account and authorization management
- In IaaS infrastructures, use server specialization, security enclaves, and application whitelisting to greatly limit the potential attack surface