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

Objectives for Chapter 8

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

Rise of the Hackers

- Rise of the Hackers

What Is Cloud Computing?

- A model for :
  - enabling convenient, on-demand network access to a shared pool of configurable computing resources.”
- A new way of providing services by using technology

What Is Cloud Computing?

- The cloud consists of networks, servers, storage, applications, and services that are connected
  - in a loose and easily reconfigurable way
- Potential users contact a cloud service provider
  - specify the configuration they want
    - Saves significant implementation resources for users,

Cloud Computing Characteristics

- 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

Cloud Computing Characteristics

- Rapid elasticity
  - Services can quickly and automatically scale up or down to meet customer need
- Measured service
  - Like water, gas, or telephone service, usage can be monitored for billing

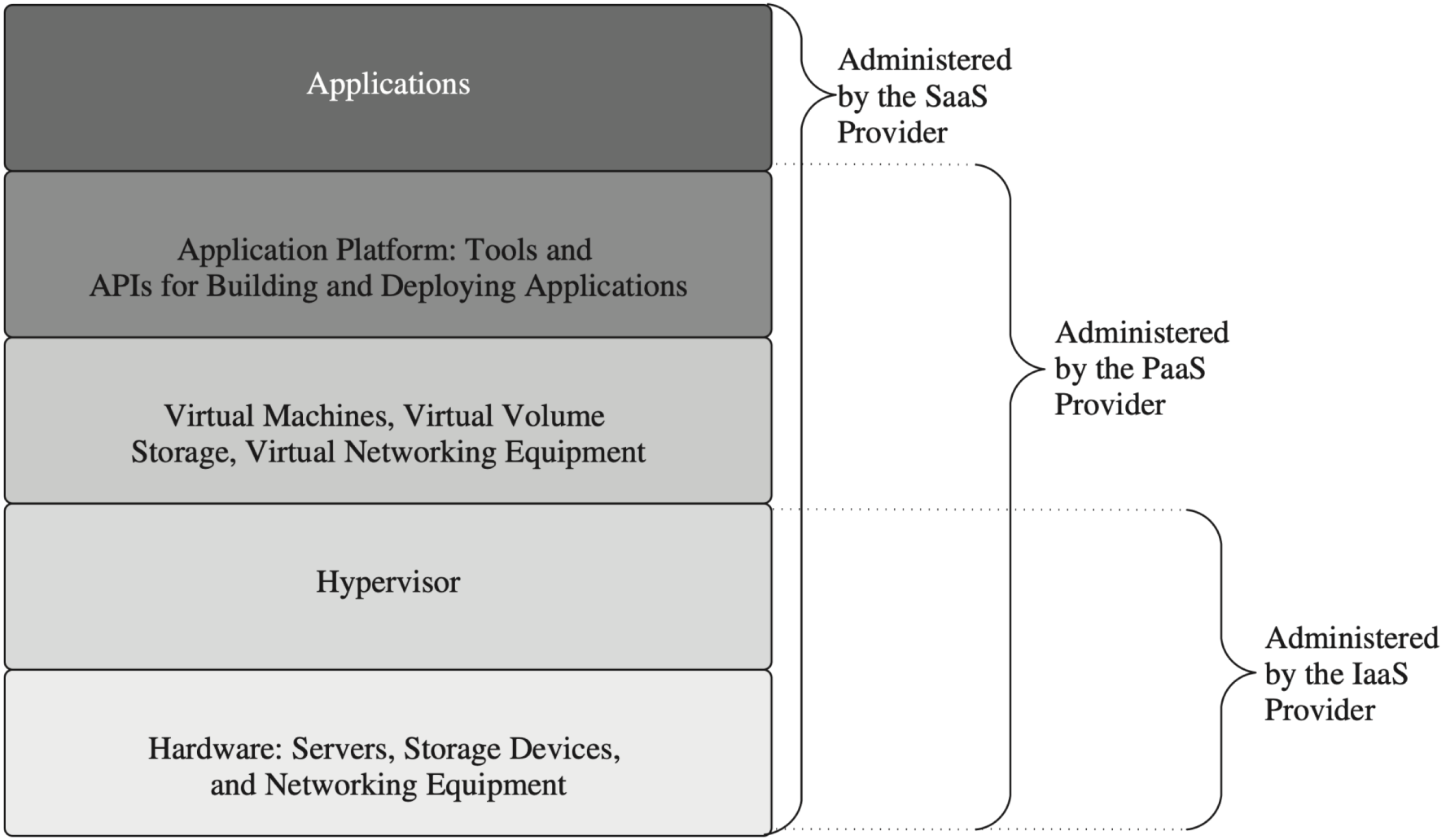
Service Models

- Software as a service (SaaS)
  - The cloud provider gives the customer access to applications already running in the cloud
    - like renting an application.
- Platform as a service (PaaS)
  - The customer has his or her own applications
  - The cloud provides the languages and tools for creating and running them
  - The customer has no control over the infrastructure used.

Service Models

- Infrastructure as a service (IaaS)
  - The cloud provider offers resources:
    - processing, storage, networks, and other computing resources
    - enable customers to run any kind of software.
  - The customer configures the resources that they need.

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

Deployment Models

- 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 – necessary before using cloud resources

- Identify assets
  - i.e. functionality and data that is needed
- Determine vulnerabilities
  - both locally and by accessing resources remotely
- Estimate likelihood of exploitation
- Compute expected loss
  - if an attack occurs, where will the greatest loss occur

Cloud Migration Risk Analysis (Cont.)

- Survey and select new controls
  - what controls need to be in place before moving to a cloud service provider.
- Project savings
  - will it be less or more expensive using cloud services.

Cloud Migration Risk Analysis

- Risk analysis steps are same as for a normal risk analysis
- However, need to be approached from a specific perspective:
  - How does a cloud deployment, compared to an on-premise deployment, change the answers?

Cloud Migration Risk Analysis

- Risk analysis components:
  - Vulnerabilities, likelihood of exploitation, and control options
- Risk analysis is different in cloud environments
  - Components are dependent on compatible tools, security mechanisms, and incident response capabilities.

Cloud Provider Assessment with respect to security concerns

- Security issues to consider:
  - Authentication, authorization, and access control options
  - Encryption options
  - Audit logging capabilities
  - Incident response capabilities
  - Reliability and uptime – this is usually stated and negotiated in the contract with the cloud provider

Cloud Provider Assessment

- Specifics of the security issues will depend on:
  - the security requirements of the capability that's being moved to the cloud
    - therefore on the risk assessment.
- Example of databases of cloud providers:
  - FedRAMP, PCI DSS and CSA STAR
  - Compliant with well-known cloud security standards.

Resources to help with assessment (1)

- Federal Risk and Authorization Management Program (FedRAMP) goals:
  - Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations
  - Increase confidence in security of cloud solutions
  - Achieve consistent security authorizations
    - using a baseline set of agreed upon standards to be used for cloud product approval in or outside of FedRAMP
  - Ensure consistent application of existing security practice

Resources to help with assessment (1)

- Federal Risk and Authorization Management Program (FedRAMP) goals (cont.):
  - Increase confidence in security assessments
  - Increase automation and near real-time data for continuous monitoring benefits
  - Increase re-use of existing security assessments across agencies
  - Save significant cost, time, and resources – “do once, use many times”
  - Improve real-time security visibility

Resources to help with assessment (1)

- Federal Risk and Authorization Management Program (FedRAMP) goals (cont.):
  - Provide a uniform approach to risk-based management
  - Enhance transparency between government and Cloud Service Providers (CSPs)
  - Improve the trustworthiness, reliability, consistency, and quality of the Federal security authorization process

Resources to help with assessment (2)

- PCI DSS - Payment Card Industry Data Security Standard goals:
  - Help merchants and financial institutions understand and implement standards for security policies
    - For technologies and ongoing processes
    - To protect their payment systems from breaches and theft of cardholder data.
  - Help vendors understand and implement standards for creating secure payment solutions.

Resources to help with assessment (3)

- CSA STAR – Cloud Security Alliance Security, Trust & Assurance Registry
  - Key principles of transparency, rigorous auditing, harmonization of standards, with continuous monitoring
  - Indicate best practices and offer the validation of security posture of cloud offerings.

Cloud Security

- How it works: Cloud Security

Switching Cloud Providers (1)

- Switching cloud providers is expensive and difficult
  - sometimes becomes necessary and urgent
- It is best to have backup options in place
  - in case a migration away from a cloud provider is necessary
    - However, many cloud providers make that practically impossible
- SaaS providers are generally hardest to migrate away from, followed by PaaS, then IaaS

Switching Cloud Providers (2)

- Why is a switch necessary?
- A major security vulnerability is discovered that can not be easily remedied.
- The software or API is no longer compatible
- The cloud provider merges with a competitor's company
- The cloud provider moves its operations to another company
  - where the organizations data can not be stored
- The cloud provider ceases operations

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
    - 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.

Cloud-Based Security Functions

- Some security functions may be best handled by cloud service providers (cont.):
  - Network monitoring – audit logging and SIEM
    - Cloud-based solutions can help customers deal with steep hardware requirements and can provide monitoring and incident response expertise.

Cloud Security Tools

- Cloud security similar to general InfoSec, but has unique characteristics
  - Shared processing, storage and communication resources
    - All have potential adversaries
  - => Same security basic tools:
    - Encryption, secure programming, network security products
      - Adapted to cloud products and resources
  -

Data Protection in the Cloud

- Cloud services users typically send private data to the service provider
  - Via the internet
- Store data on cloud provider's services
- It is user's responsibility to chose the appropriate service
  - That offers adequate data protection
    - As per your service guarantees to your clients
    - => mutual authentication can be performed

Data Protection in the Cloud

- Data in transit can be protected by network secure communication tools
  - Such as TLS, SSH and VPN
  - VPN has additional advantage: supports certificate authentication
    - => mutual authentication can be performed

Cloud Storage

- By default, most cloud storage solutions either:
  - store users' data unencrypted
  - 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.
  - This can be a vulnerability

Cloud Storage

- For maximum confidentiality, some cloud providers embrace a ‘trust no one’ (TNO) model
  - even the provider does not have the keys to decrypt user data.

EXAMPLE - LASTPASS

Lastpass

- A password manager
  - Allows customers to store the login information they use to access other websites
- Goal:
  - Main a confidential password database

Lastpass Implementation

- Information is encrypted with AES-256 encryption
- users' AES decryption keys *never* sent to Lastpass servers
  - or any other information that may lead to those keys
- Requires users to log in to a *local* client using a username and a "master password"
- To protect the master password, the client uses a form of PBKDF2

PBKDF2 Function

- Password-Based Key Derivation Function are key derivation functions
  - used to reduce vulnerabilities to brute force attack
- Part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series

Lastpass Implementation

- Salting master password with random data
- Hashing it
  - using many SHA-256 rounds
- Lastpass servers never receive the master password
  - Only the resulting Hash
- The hash cannot be used to decrypt the user's password database
  - nor can it be used to derive the decryption key.

Lastpass Implementation

- The hash allows the client to log in to the server and download the encrypted password database
  - The client derives the decryption key from the master password just as it did the login hash
    - Done locally
      - using one fewer SHA-256 round

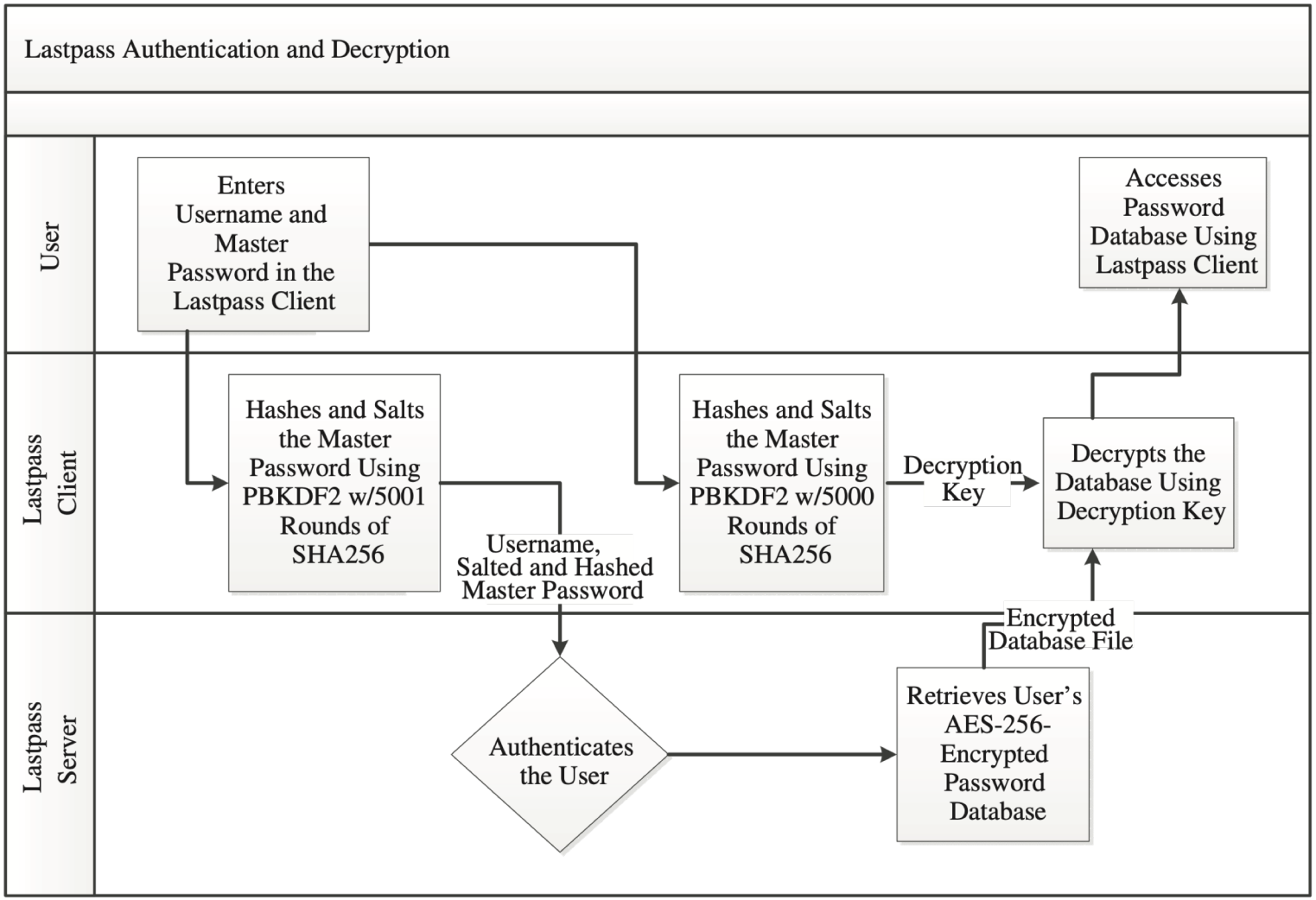
Lastpass Implementation

- This design provides customers with a strong degree of protection from attacks against the Lastpass service.

Lastpass TNO Implementation – SaaS product

- Lastpass is able to authenticate users but unable to decrypt those users' data
- Lastpass uses a hash for authentication
  - Derived from the user's password
- Decryption takes place client-side
  - Uses a different hash than the one used for authentication

Lastpass TNO Implementation – SaaS product

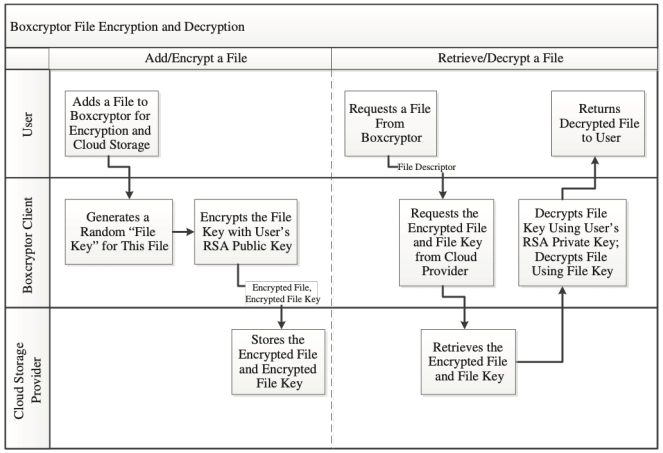


BoxCryptor

- An encryption client
- Provides TNO on a cloud storage service that doesn’t offer TNO
- Augments generic cloud storage providers
  - such as Dropbox

Boxcryptor TNO Implementation – use with a cloud provider

- Boxcryptor allows users to selectively share files with other users.
  - by generating a per-file random key
  - using each authorized user's public key to encrypt that random key



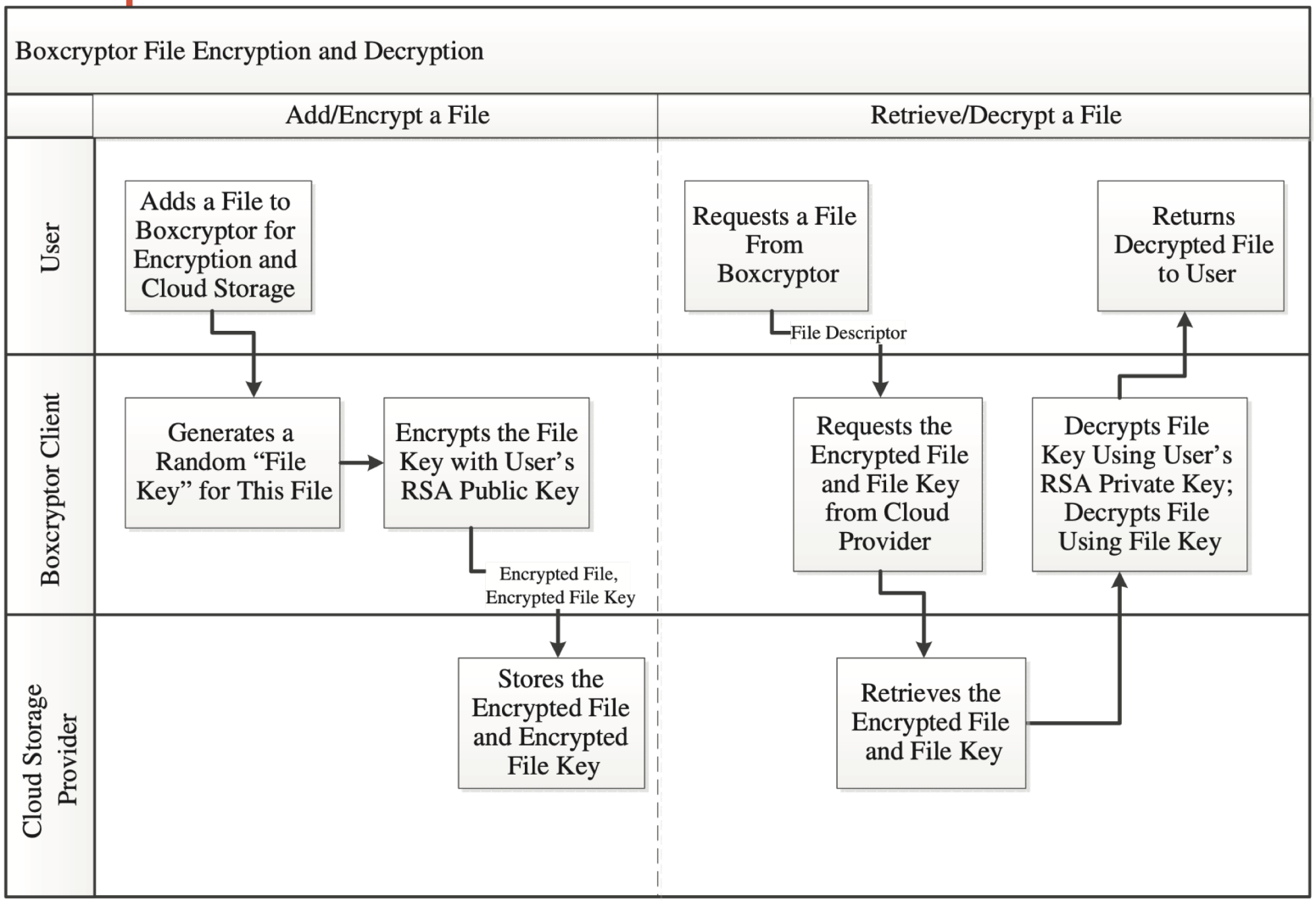
Boxcryptor

- Encryption:
  - Creates a unique AES encryption key (“file key”)
    - for every file a customer uploads to the cloud.
  - Encrypts the file key by using the customer’s unique RSA public key
  - Stores the encrypted file key with the encrypted file.

Boxcryptor

- Decryption - when a customer wants to retrieve and decrypt a file from cloud storage:
  - The client uses the customer's RSA private key to decrypt the file key
  - Uses the file key to decrypt the file.

Boxcryptor TNO Implementation – use with a cloud provider



Data Loss Prevention (DLP) - reminder

- DLP is a set of technologies
- can detect and possibly prevent attempts to send sensitive data where it is not allowed to go
- Can be implemented as
  - Agent installed as an OS rootkit
  - Guard

DLP

- Defending organizations against both data loss and data leakage prevention
- Data loss refers to an event in which important data is lost to the enterprise
  - such as in a ransomware attack.
- Data loss prevention focuses on preventing illicit transfer of data
  - outside organizational boundaries.

DLP

- Organizations typically use DLP to:
  - Protect Personally Identifiable Information (PII) and comply with relevant regulations
  - Protect Intellectual Property critical for the organization
  - Achieve data visibility in large organizations
  - Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
  - Secure data on remote cloud systems

Data Loss Prevention (DLP) - reminder

- Indicators DLP looks for:
  - Keywords
  - Traffic patterns
  - Encoding/encryption
- DLP useful for preventing accidental incidents
- However, malicious users will often find ways to circumvent it
  - DLP may slow attackers

Data Loss Prevention (DLP)

- DLP is more difficult in cloud environments than on-premise environments
  - cloud customers have much less control over data ingress and egress points

Data Loss Prevention (DLP)

- DLP options for cloud-based corporate data:
  - Force users to work through the corporate virtual private network (VPN)
    - to access corporate-contracted cloud resources
  - Install DLP agents on users' corporate systems
  - In IaaS environments, insert a DLP server as a proxy
    - between user systems and other corporate cloud servers

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
    - consequently spreading attacks to your applications.
  - Some attacks, specifically target shared resource environments.
    - Such as cryptographic side-channel attacks

Cloud Application Security

- Cryptographic side-channel attacks use incidental information—to reduce the search space of cryptographic keys.
  - Attacks may use processor and memory response, temperature, etc.
  - They have been proven effective in small, cloud-like laboratory environments

Cloud Application Security

- Attacks against insecure APIs
  - Cloud vendors have a history of using known broken APIs.
  - Almost one-third of those incidents were caused by insecure interfaces and APIs [Ko et. Al]
    - Cloud security incidents surveyed over a 5-year period
  - Major security weaknesses in SSL libraries used by major cloud service providers
    - including Amazon and PayPal [Georgiev et. Al|

1. Ko, R., et al. “Cloud Computing Vulnerability Incidents: A Statistical Overview.” Cloud Security Alliance white paper, 13 Mar 2013.

2. Georgiev, M., et al. “The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software.”ACM Conf on Comp and Comm Security ’12, 2012.

Logging and incident responses

- SaaS systems
  - Provide users with application layer logfiles
  - User has no access to underlying hardware or software
- PaaS systems
  - Customers generate their own application layer logfiles
  - They can often configure the runtime environment.
  - User has no access to underlying hardware or OS.

Logging and incident responses

- IaaS systems
  - Customers can generate their own logfiles concerning applications, OS and virtual networks.
  - Customers do not have access to hardware and provider networks.

Cloud Identity Management

- Access control needs to guarantee that users are who they claim to be
- Cloud providers can be hacked
  - do not necessarily provide good protection of usernames and passwords.
- Cloud providers may allow customers to have weak passwords
  - may not provide multifactor authentication.
- How does an organization manage multiple user accounts?
  - on different networks and cloud providers?

Federated Identity

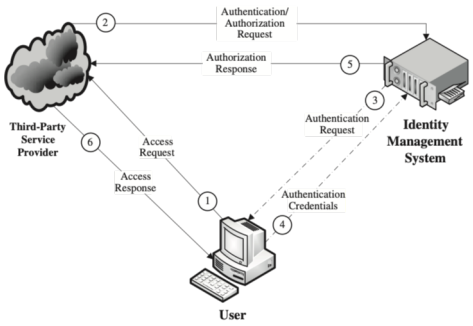
- The means of linking a person's electronic identity and attributes
  - stored across multiple distinct identity management systems
- Addresses the need to ensure appropriate access to resources
  - across increasingly diversified technology environments
  - meet increasingly rigorous compliance requirements

Identity Management

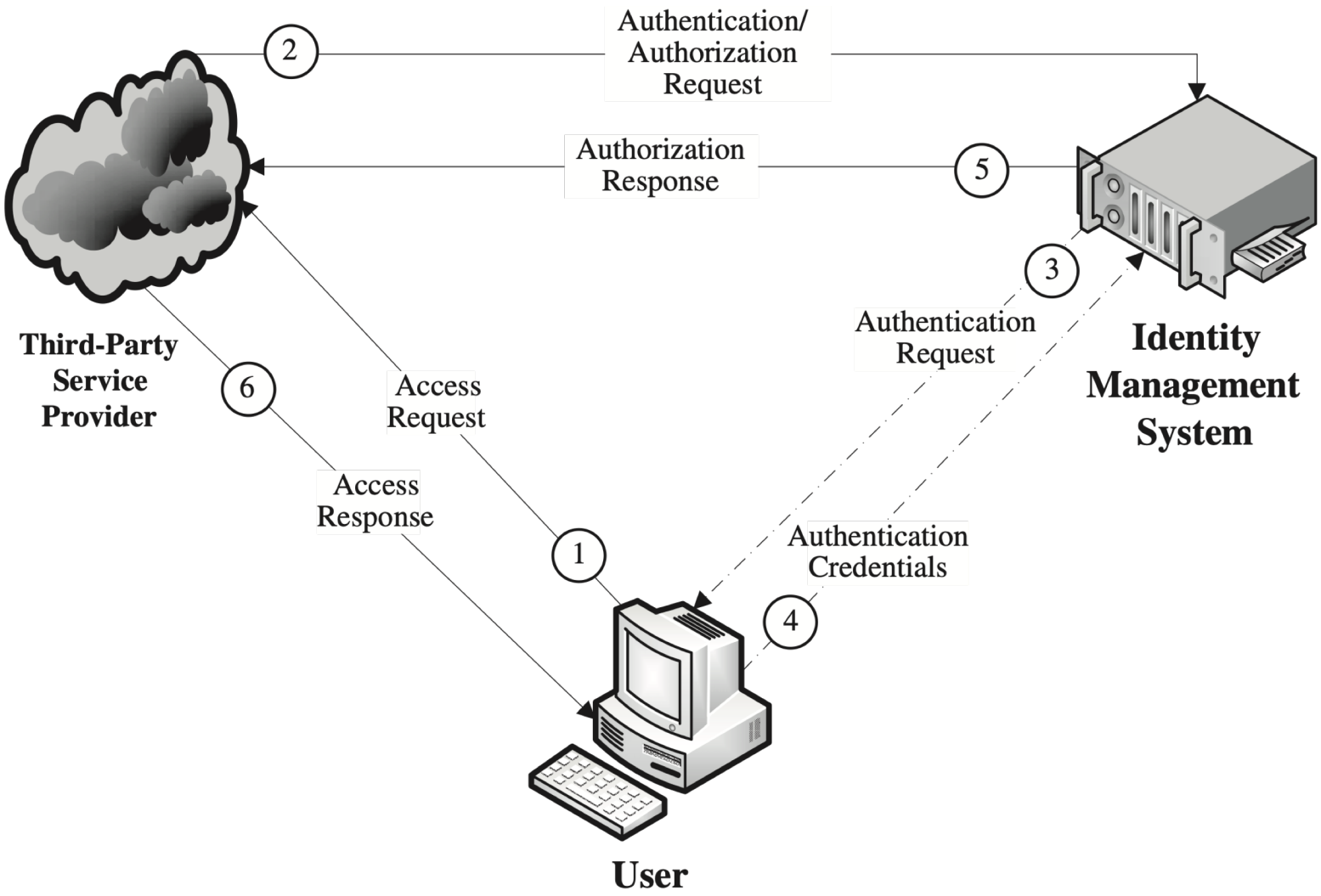
- Business Identity Management

Federated Identity Management (FidM) –

- Provides trust and standardization
- Enables identity information to be shared among several entities and across trust domains.
- In this example:
  - The user wishes to access the service provider
  - The service provider needs to check with a completely unrelated, but trusted, identity provider
    - to ensure the user's validity and authority first.



Federated Identity Management (FidM) – provides trust and standardization



Federated Identity Management (FidM)

- Two prerequisites make FIdM work:
  - Trust
  - Standardization
- Trust:
  - System that requests ID information must trust the data it receives
  - The system that provides ID information must trust the recipient
  - The two systems need a standard way to communicate
  - => **Security Assertion Markup Language** (SAML) makes these exchanges possible

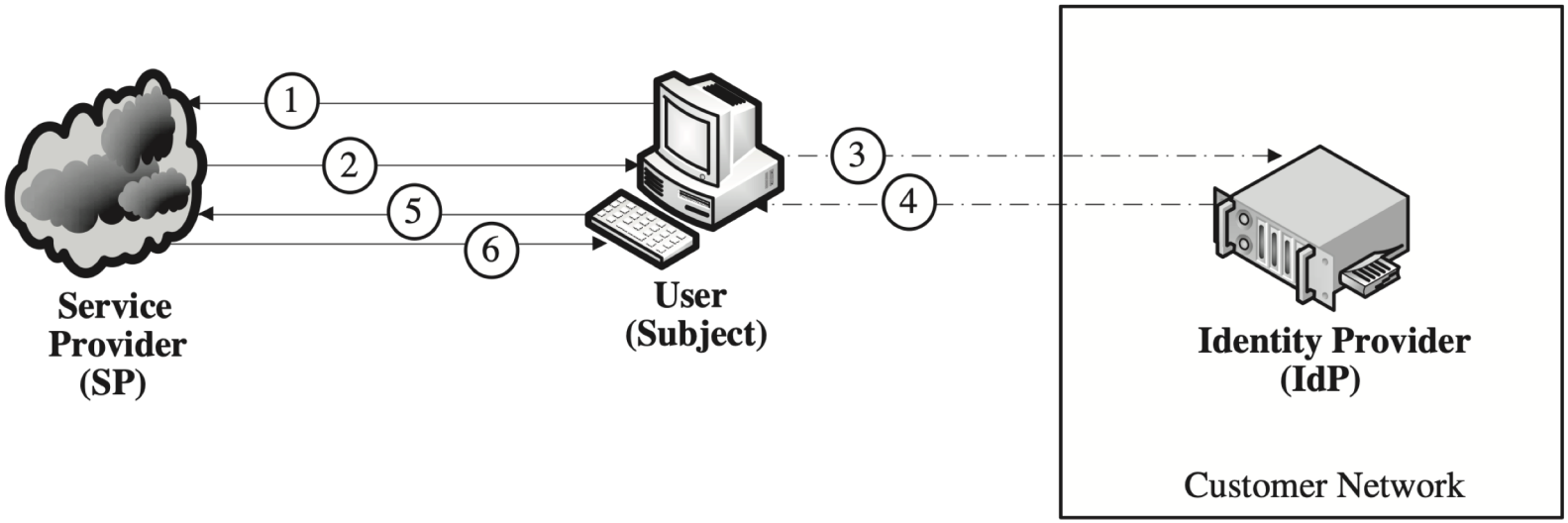
Security Assertion Markup Language (SAML)

- An XML(extensible mark-up language) based standard
  - Defines a way for systems to securely exchange user identity and privilege information.
- Used when a company wants to give employees access to corporate cloud service subscriptions
- If an employee leaves the company, his corporate login credentials are disabled
  - => so are his login rights to the cloud service

Security Assertion Markup Language (SAML)

- Three parties who participate in identity exchanges:
  - The **Service Provider (SP)** or **Relying Party**:
    - A SAML-enabled service, that needs to obtain identity information from a third party
  - The **Subject**:
    - The entity, be it user or system, that is attempting to log in to the SP
  - The **Identity Provider (IdP)** or **Asserting Party**:
    - An SAML-enabled system that can authenticate the Subject and make assertions about the Subject's identity

SAML Authentication Process

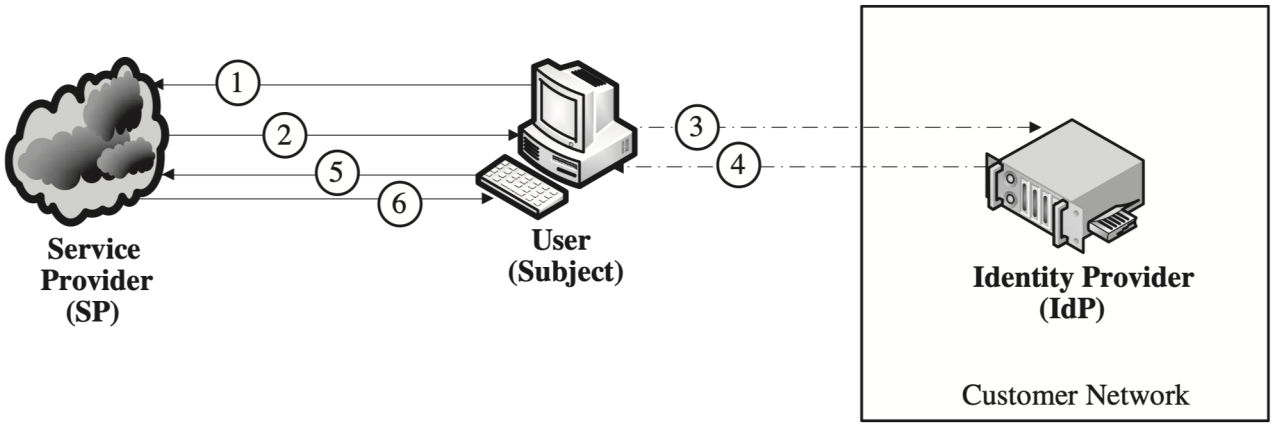


SAML Authentication Process

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

SAML Authentication Process

- The IdP is often a corporate identity store, and the SP is often a cloud service provider



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 for an API
  - SAML is designed to handle authentication, authorization, and single sign-on for users and systems
  - OAuth was built to handle a different aspect of FIdM: API access
  - OAuth does not exchange identity information, just authorization

OAuth

- 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;

OAuth

- Users can revoke access at any time
- Another benefit of OAuth is that it is designed to work with native applications, not just in a web browser
  - unlike SAML

OAuth Authorization

- OAuth framework doesn’t specify any signatures or encryption
  - Strongly recommends using TLS wherever possible.
- In SAML, signatures and encryption are important
  - Protect the integrity and confidentiality of assertions from malicious users
- SAML is designed to handle authentication, authorization, and single sign-on
  - for users and systems

OAuth Authorization

- In OAuth tokens, the primary concern is confidentiality against eavesdroppers
  - OAuth does not exchange identity information, just authorization
  - Less likely that data will be modified

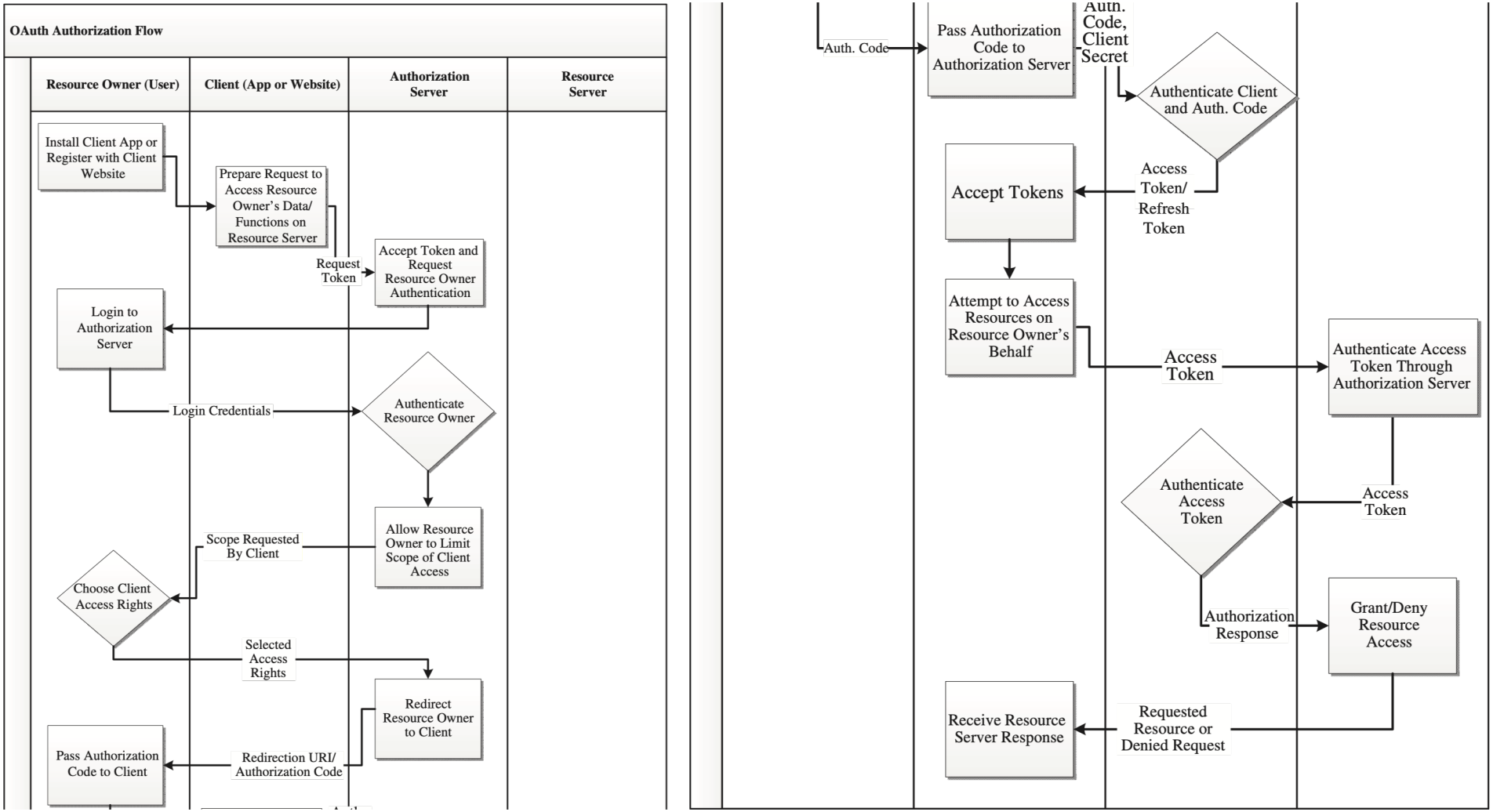
Oauth Roles

- The **Resource Owner**, is the user with a password-protected online account.
  - analogous to the SAML subject
- The **Resource Server** is the server on which the APIs reside.

Oauth Roles (cont.)

- The **Client**, is the application that is attempting to access the account APIs.
  - analogous to the SAML SP
- The **Authorization Server** is the server that can authenticate the resource owner and grant the client access to the resource server
  - analogous to the SAML IdP

OAuth Authorization



OAuth

- What if you want all the identity management and authentication features of SAML, but built into a native application rather than one running in a browser?

OAuth

- One solution: combining OAuth and SAML
  - OAuth client sends a Request Token to the Authorization Server
  - The Authorization Server redirects the user to his or her SAML IdP to authenticate.
    - The only extra information the OAuth Client needs is the name of the user's IdP
  - The SAML authentication process completes as it normally would
  - The OAuth authorization process then proceeds normally as well

OAuth

- Another solution: OpenID Connect (OIDC)

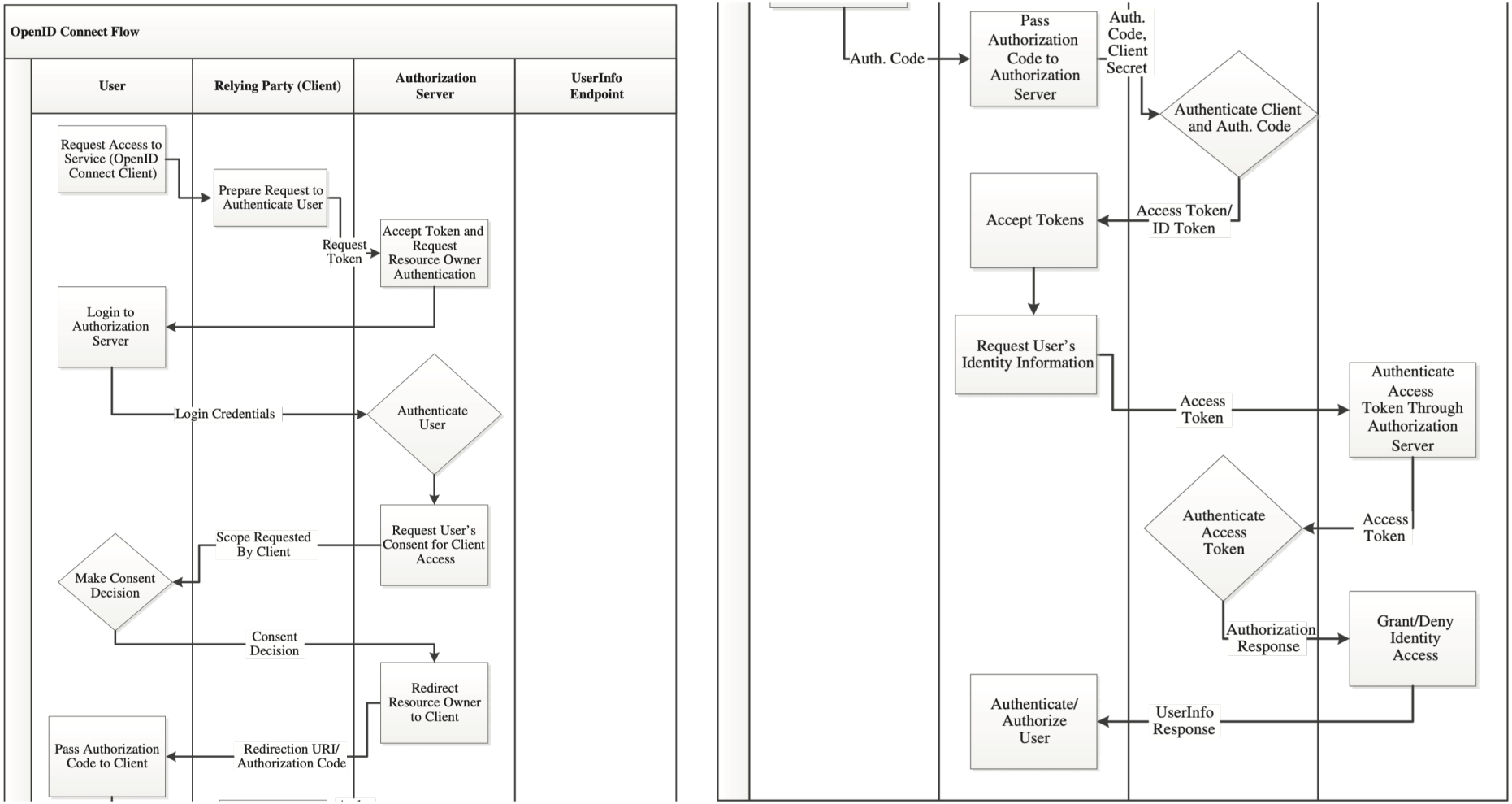
OpenID Connect (OIDC)

- OIDC is a relatively new standard for FidM
  - OAuth has been extended to support authentication in the form of OIDC
- Allows users to access multiple applications with a single set of credentials.
- OIDC Can handle typical SAML use cases:
  - Allowing enterprise users to log in to multiple third-party services by using a single set of corporate credentials
  - However, OIDC has a broader goal: allowing users to access every site on the Internet with a single set of credentials

OpenID Connect (OIDC)

- OIDC provides much better support for native applications (versus web applications) than does SAML because it is based on Oauth 2.0.
- Works by adding an identity token to the existing authorization tokens, essentially treating identity information as another authorization right

OIDC Authentication



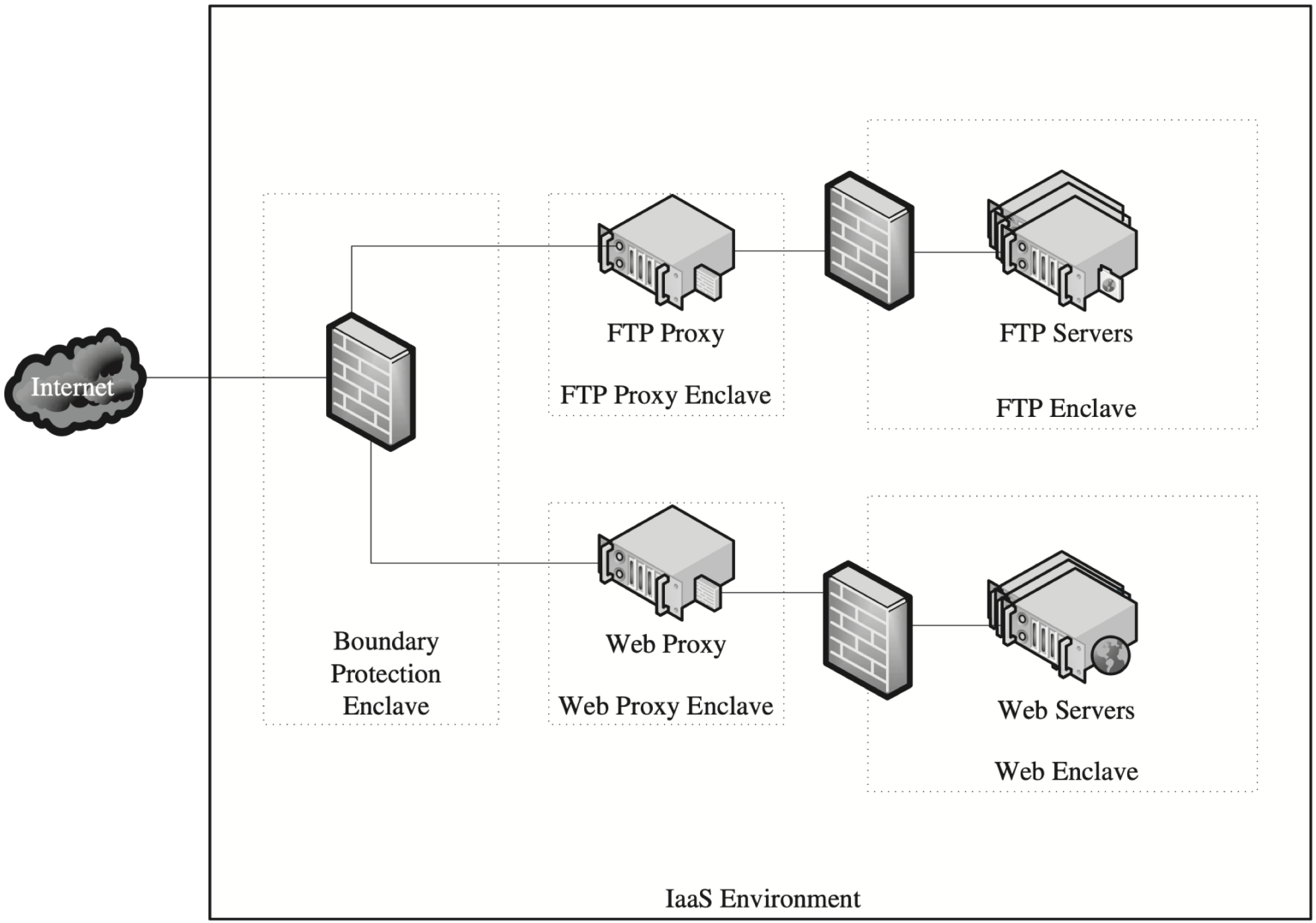
Security and IaaS

- 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

Security and IaaS

- 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

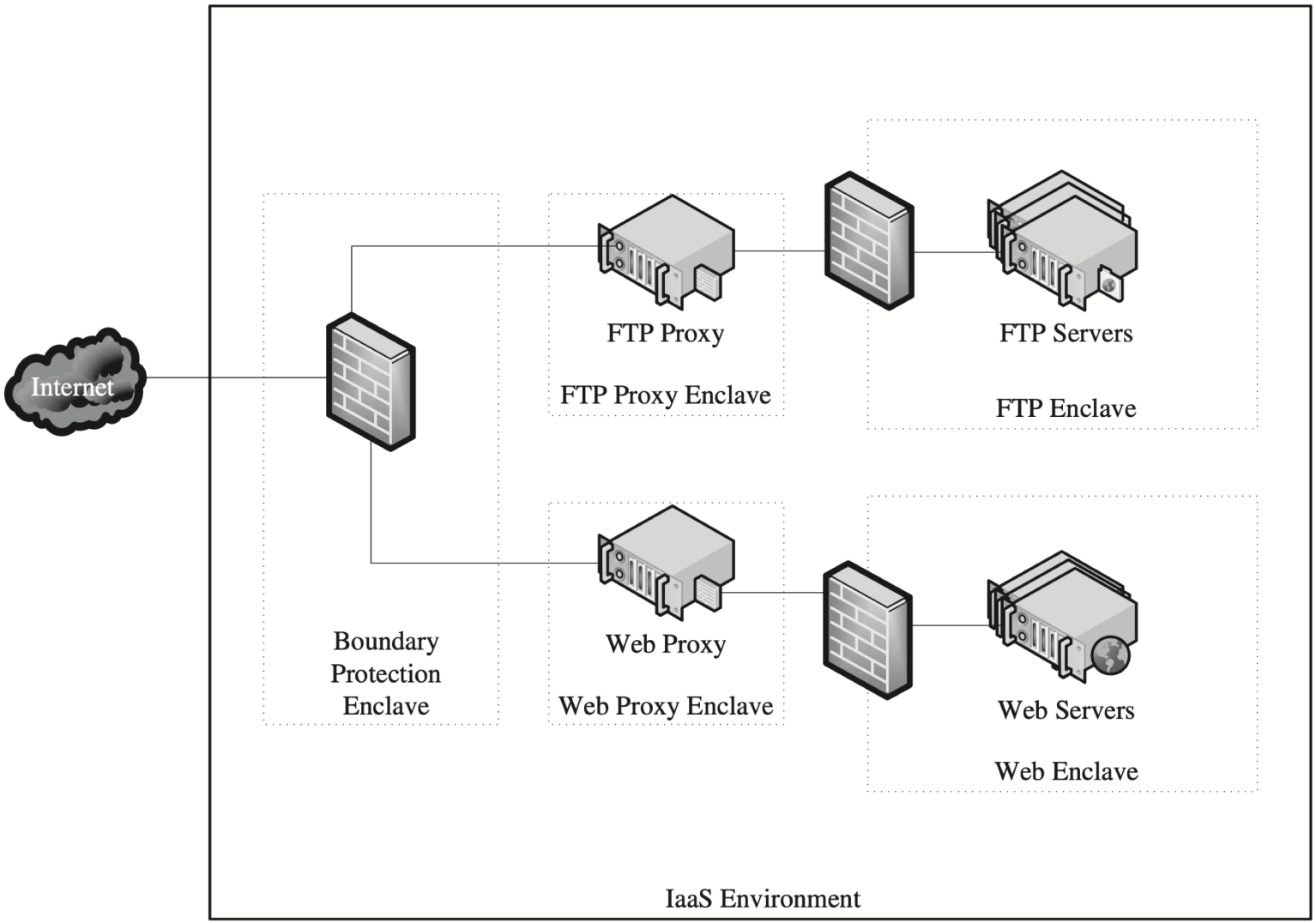
IaaS Security Architecture - Example



IaaS Security Architecture - Example

- Each server type is in its own security enclave
  - with the critical servers being protected by both firewalls and application proxies.
- Each of these servers is dedicated to a very specific purpose and
  - therefore simple and predictable enough to allow for application whitelisting
    - which greatly limits malware potential.
- This level of VM specialization is not always practical, but it greatly limits potential vulnerability

IaaS Security Architecture



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

Summary

- FIdM, including SAML, OAuth, and OIDC, provides strong security benefits
  - by centralizing account and authorization management
- In IaaS infrastructures, use server specialization, security enclaves
  - application whitelisting to greatly limit the potential attack surface

- Questions?