Emerging Topics

EECS 195

Spring 2019

Zhou Li

Objectives

- Issues with cloud computing
- Issues with mobile computing
- Issues with IoT

Cloud Computing

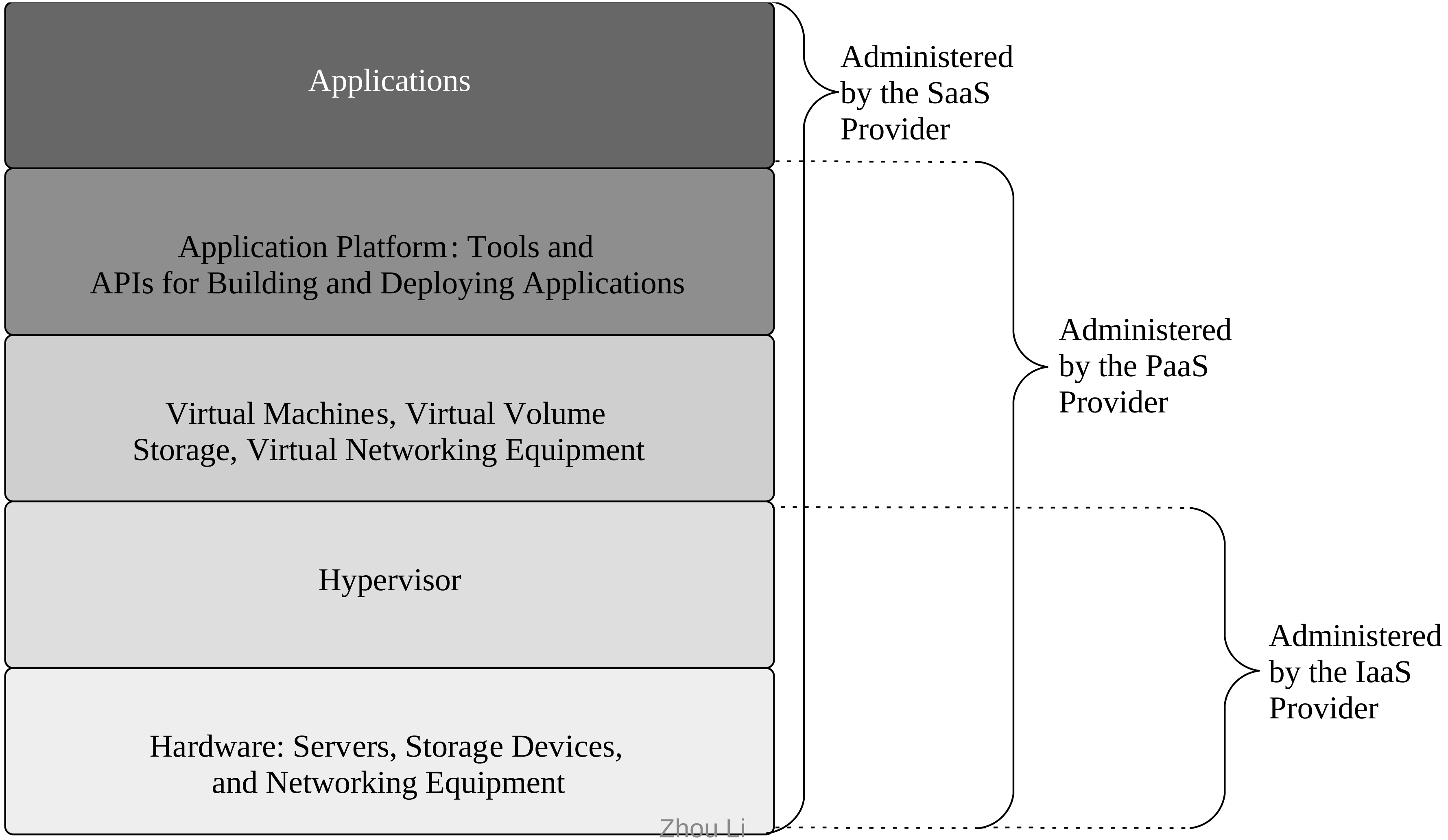
Features of Cloud Computing

- On-demand self-service
  - Add or subtract resources as necessary
- Broad network access
  - Services can be accessed through 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



Applications

Application Platform: Tools and APIs for Building and Deploying Applications

Virtual Machines, Virtual Volume Storage, Virtual Networking Equipment

Hypervisor

Hardware: Servers, Storage Devices, and Networking Equipment

Administered by the SaaS Provider

Administered by the PaaS Provider

Administered by the IaaS Provider

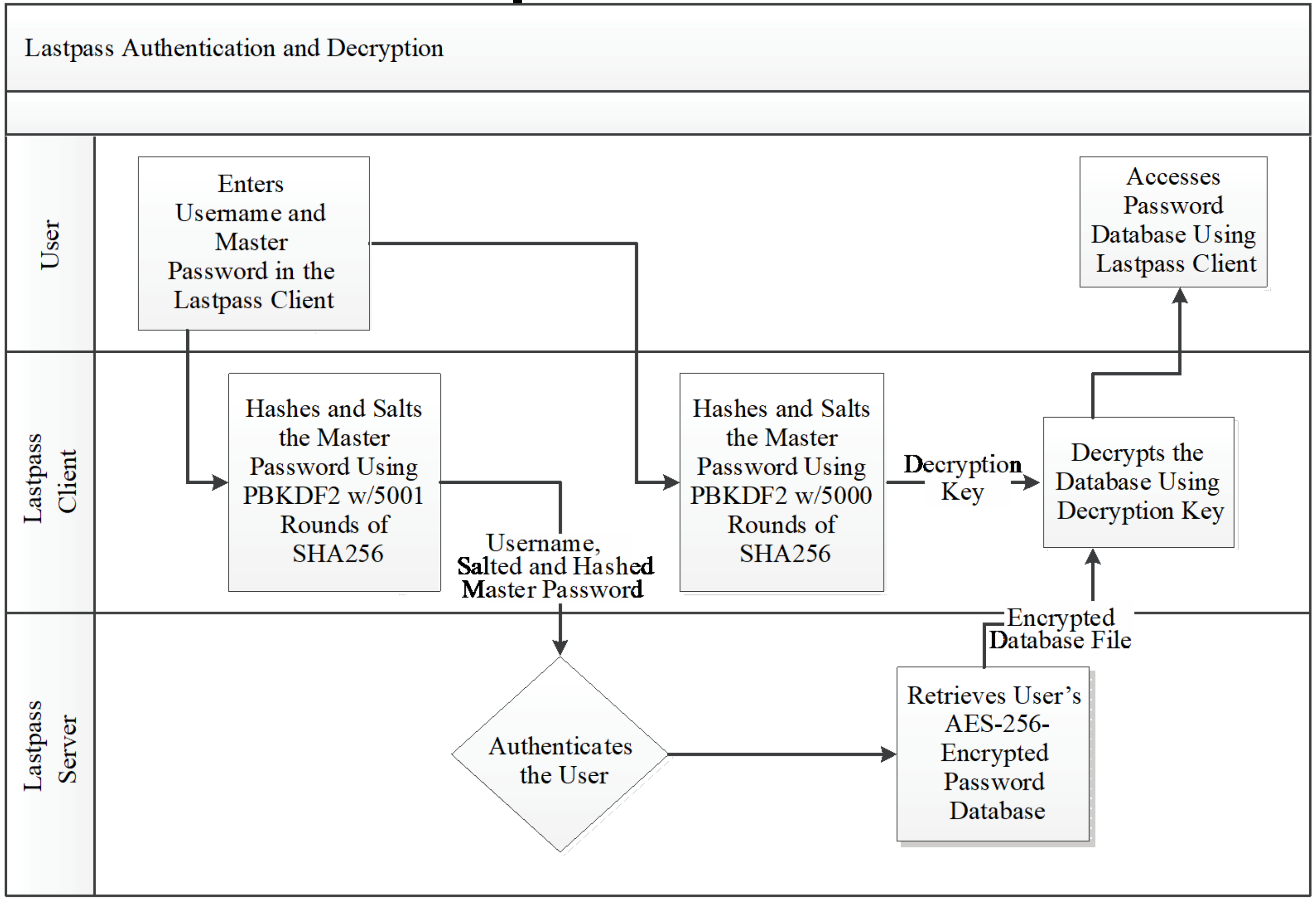
Security Benefits of Cloud Services

- Mitigating single point of failure
  - Data centers of cloud in different geographic locations provide protection from natural and other local disasters.
- Diversifying platform and infrastructure to reduce attack impact
  - Different bugs and vulnerabilities for rented machines, single attack less likely to bring a system down
- Security functions handled better by cloud service providers:
  - Cloud-based email filter removes spam before reaching customers inbox.
  - Cloud-based DDoS protection services have sufficient bandwidth to handle attack traffic volume, by replacing customers' DNS records
  - Cloud-based SIEM solutions can correlate attacks across customers

Cloud Storage

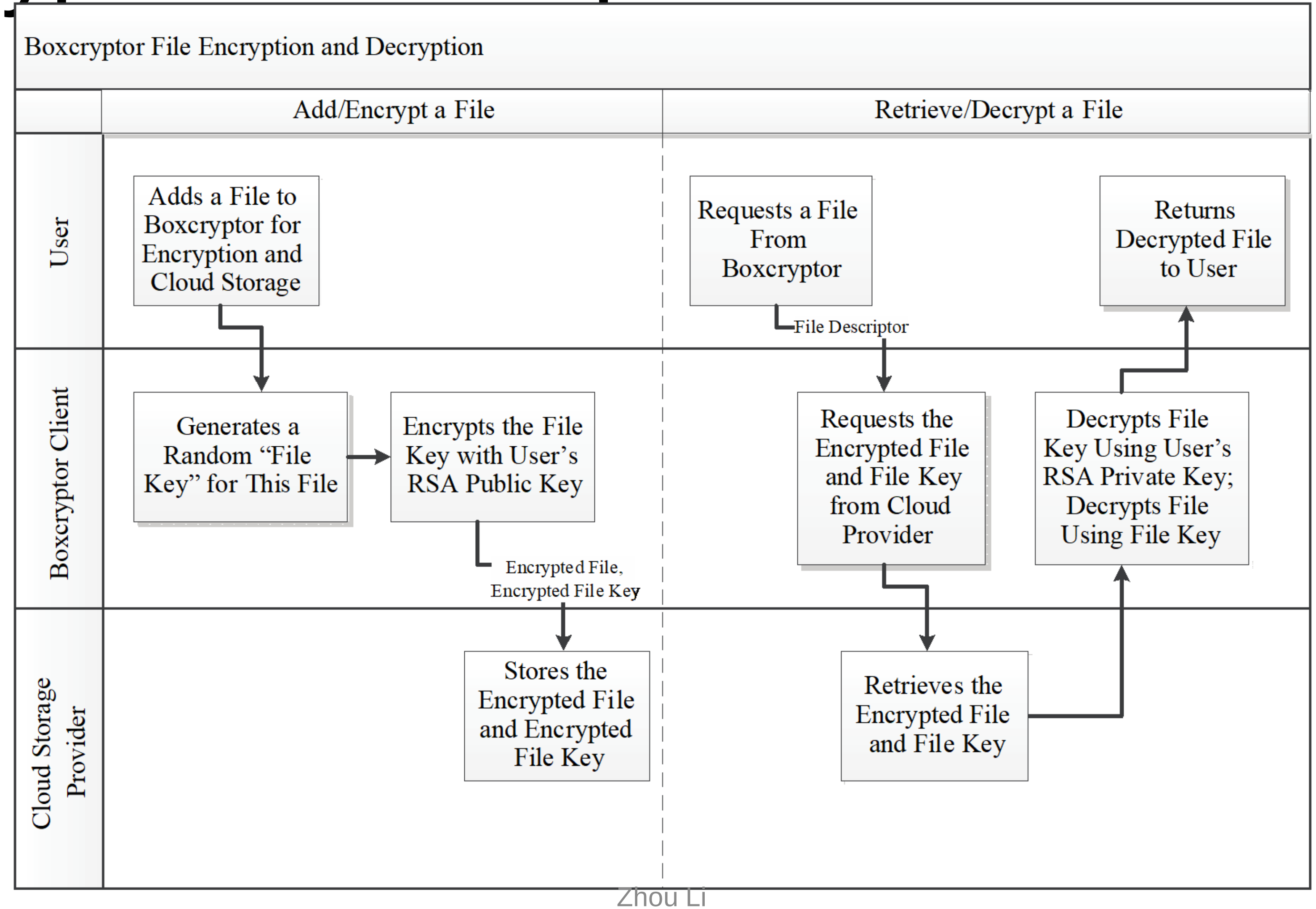
- Most cloud storage either store users' data unencrypted or encrypt data for all customers using a single key
  - Don't provide strong confidentiality
  - If access control is breached and attacker obtains one key, all customers' data will be breach
- Some provide better confidentiality by generating 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



Lastpass Authentication and Decryption
User
Lastpass Client
Lastpass Server
Enters Username and Master Password in the Lastpass Client
Accesses Password Database Using Lastpass Client
Hashes and Salts the Master Password Using PBKDF2 w/5001 Rounds of SHA256
Hashes and Salts the Master Password Using PBKDF2 w/5000 Rounds of SHA256
Decryption Key
Decrypts the Database Using Decryption Key
Username, Salted and Hashed Master Password
Encrypted Database File
Authenticates the User
Retrieves User's AES-256-Encrypted Password Database

Boxcryptor TNO Implementation


Boxcryptor File Encryption and Decryption
Add/Encrypt a File
Retrieve/Decrypt a File
User
Boxcryptor Client
Cloud Storage Provider
Adds a File to Boxcryptor for Encryption and Cloud Storage
Generates a Random “File Key” for This File
Encrypts the File Key with User’s RSA Public Key
Encrypted File, Encrypted File Key
Stores the Encrypted File and Encrypted File Key
Requests a File From Boxcryptor
File Descriptor
Requests the Encrypted File and File Key from Cloud Provider
Retrieves the Encrypted File and File Key
Decrypts File Key Using User’s RSA Private Key; Decrypts File Using File Key
Returns Decrypted File to User

Data Loss Prevention (DLP)

- DLP products have been deployed by many companies to protect their data within their networks
- DLP is more difficult in cloud environment, as cloud customers have much less control over data ingress and egress points
- DLP options for cloud-based corporate data:
    - Force users to work through the corporate 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

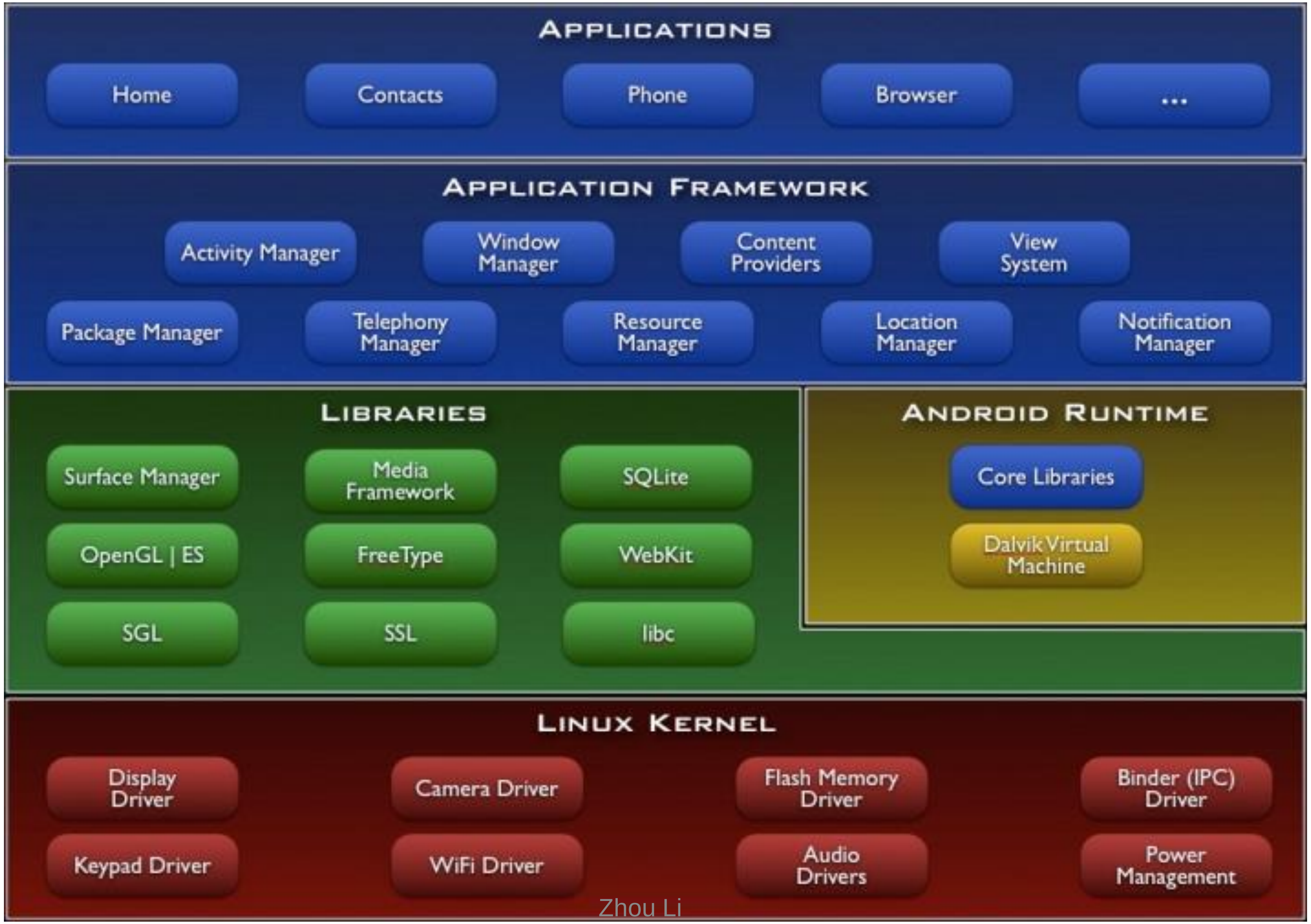
- Writing secure software is no different in cloud environment, but some new issues need to be considered
- Attacks against shared resources
  - Your VM can share the same physical machine with an attacker's VM (called VM co-location), malicious VM can attack your VM exploiting vulns.
  - New side-channel attacks can infer your cryptographic keys.
- Attacks against insecure APIs
  - Cloud users can use APIs to access their resources.
  - The APIs might be insecure, exploitable to retrieve sensitive info.[1]
  - SSL libraries used by major cloud service providers, including Amazon and PayPal, were insecure once in 2012.[2]

[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.

Mobile Computing

Focus of this lecture



APPLICATIONS

Home | Contacts | Phone | Browser | ...

APPLICATION FRAMEWORK

Activity Manager | Window Manager | Content Providers | View System

Package Manager | Telephony Manager | Resource Manager | Location Manager | Notification Manager

LIBRARIES

Surface Manager | Media Framework | SQLite

OpenGL | ES | FreeType | WebKit

SGL | SSL | libc

ANDROID RUNTIME

Core Libraries

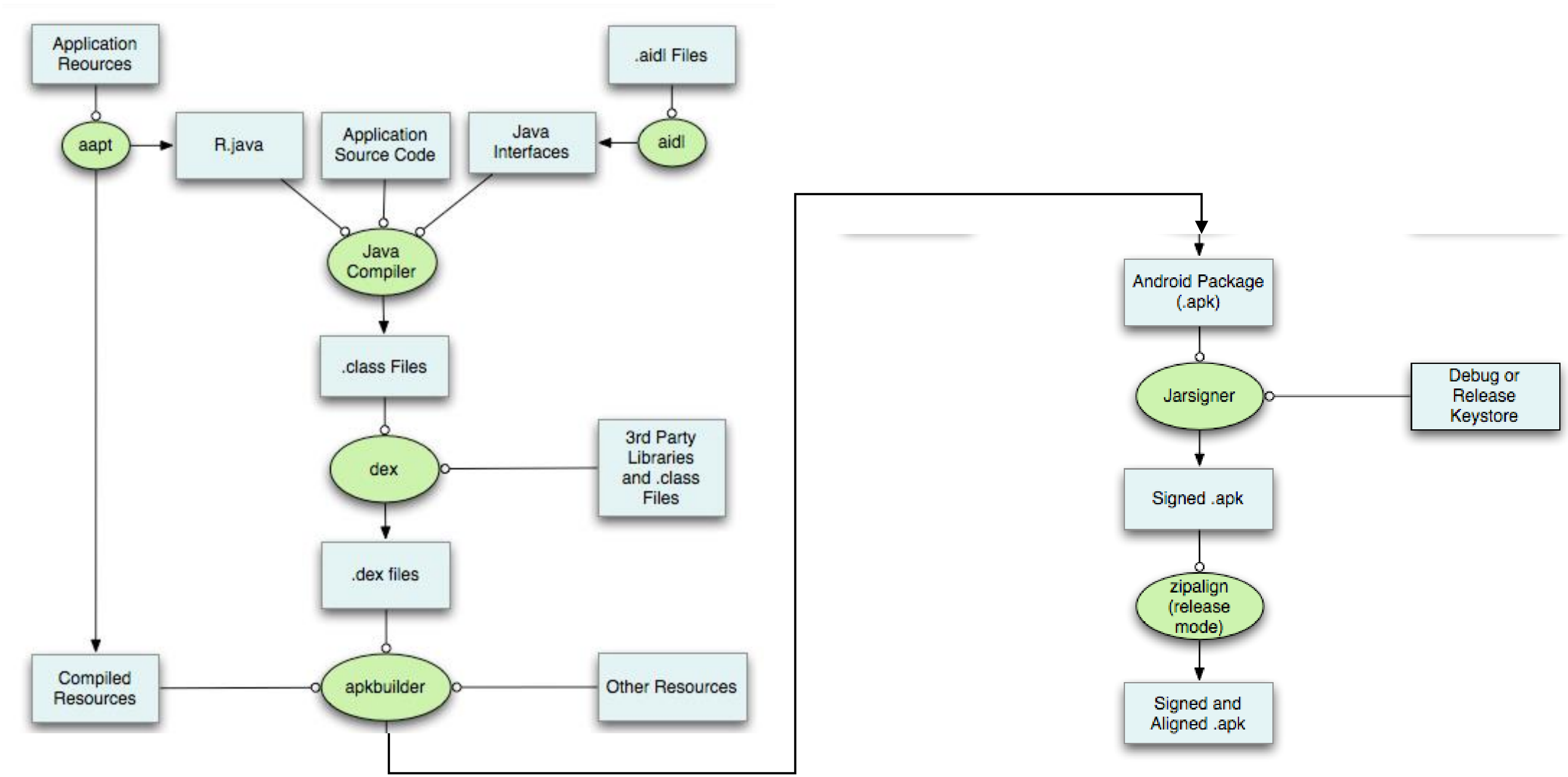
Dalvik Virtual Machine

LINUX KERNEL

Display Driver | Camera Driver | Flash Memory Driver | Binder (IPC) Driver

Keypad Driver | WiFi Driver | Audio Drivers | Power Management

Managed Code Runs in App Sandbox (VM)



Application development process: source code to bytecode