DIPLOMA IN CLOUD SECURITY

Project Assignment 1: Security Architecture Report

By

Juan José Para Catalá

9th October 2018

Background

The Department of Transportation is composed of a number of different agencies, including the Office of the Secretary of Transportation (OST) and the National Highway Traffic and Safety Administration (NHTSA), but also encompasses aviation, rail, maritime and even pipeline administrations. On June 24, 2009, President Obama signed the Consumer Assistance to Recycle and Save (CARS) Act, which directed the Secretary of Transportation (acting through NHTSA) to establish and administer what would come to be popularly known as the "cash for clunkers" program. The Car Allowance Rebate System, was a $3 billion U.S. federal scrappage program intended to provide economic incentives to U.S. residents to purchase a new, more fuel-efficient vehicle when trading in a less fuel-efficient vehicle. The program was promoted as providing stimulus to the economy by boosting auto sales, while putting safer, cleaner and more fuel-efficient vehicles on the roadways. NHTSA was called on to lead the CARS program at the implementation level. Given the sheer size and scope – and just a 30 day timeline – everyone who could be spared within the DOT was pulled onto the project. That meant leveraging as many existing resources and services as possible, as well as working closely with DOT partners, systems and networks to make this mandate happen. Cloud computing was one obvious way to realize the kind of scale and speed that was required. However, at the time, cloud computing seemed to offer more problems than solutions, presenting security challenges that appeared to be incompatible with the government's certification and accreditation process. There was also the issue of the extensive eligibility requirements for consumers to trade in their cars.

They were the following: ▪ Vehicle must be less than 25 years old on the trade-in date. ▪ Only the purchase or 5-year minimum lease of new vehicles qualify. ▪ Generally, trade-in vehicles must get a weighted combined average rating of 18 or fewer miles per gallon (some very large pickup trucks and cargo vans have different requirements). ▪ Trade-in vehicles must be registered and insured continuously for the full year preceding the trade-in. ▪ Trade-in vehicles must be in drivable condition. ▪ The program ran from July 1, 2009 until August 24, 2009. ▪ The program requires the scrapping of the eligible trade-in vehicle and that the dealer disclose to the customer an estimate of the scrap value of the trade-in. The scrap value, however minimal, will be in addition to the rebate, and not in place of the rebate. ▪ The new car bought under the plan must have a suggested retail price of no more than $45,000, and for passenger automobiles, the new vehicle must have a combined fuel economy value of at least 22 mpg. The CARS program will be administrated through a central system that will be accessible by car dealers involved in the program and centrally managed by the NHTSA. The system will track the incoming and outgoing vehicles, as well as consumer information and eligibility requirements. The program will need to be central so as to track vehicles and consumers. The 'clunkers', that the car dealer received were not allowed be resold. To ensure that vehicles traded-in under were not resold by dealers, the program outlines a procedure for destructively disabling the engine. You have been contracted by the company as IT security manager to assess the security concerns surrounding the CARS program being hosted in the cloud. Your findings will form a security report.

You will also be required to test current cloud solutions offered by Google and Microsoft.

1. *Assessment of the security architecture of the below cloud providers.*

This report is based on cloud solutions offered by Google and Microsoft.

Taking into consideration the Background of this project and starting with the first cloud solution offered by Google (Google App Engine), I'm going to say that in this scenario; the service delivery model is Platform as a Service (PaaS).

Google (Google App Engine)

We are going to explore the architectural frameworks; tools that cloud architects have, to develop and implement the application for the CARS program, and the disclosure of security architectural details.

Google Infrastructure Security Design Overview:

- Secure Low Level Infrastructure
- Hardware Design and Provenance
- Secure Service Deployment
- Inter-Service Access Management
- Access Management of End User Data
- Encryption at Rest
- Secure Internet Communication
- Denial of Service (DoS) Protection
- Operational Security
- Keeping Employee Devices and Credential Safe
- Intrusion Detection
- Security of Physical Premises
- Secure Boot Stack and Machine Identity
- Service Identity, Integrity and Isolation
- Encryption of Inter-Service Communication
- Secure Data Storage
- Deletion of Data
- Google Front End Service
- User Authentication
- Safe Software Development
- Reducing Insider Risk
- Securing the Google Cloud Platform (GCP)

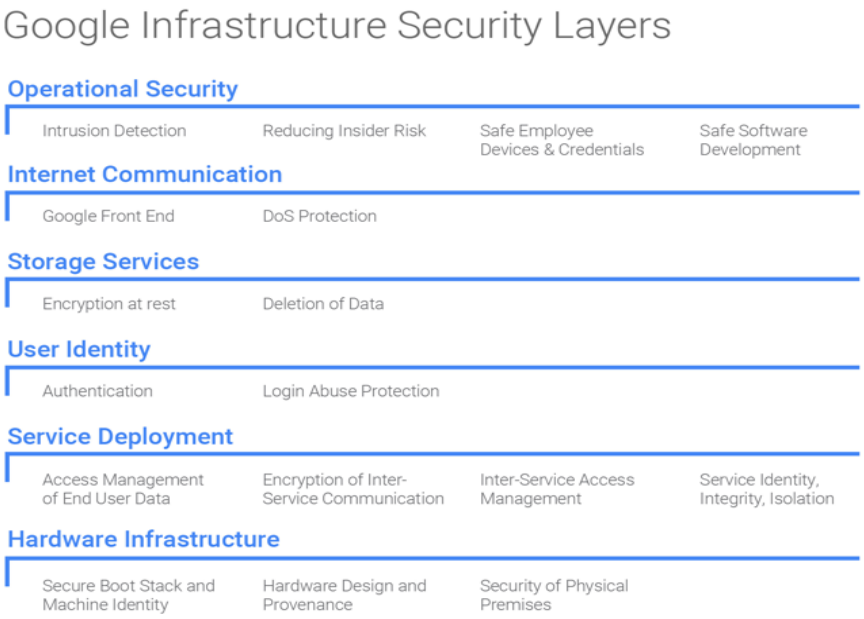


Figure 1: Google Infrastructure Security Layers
https://cloud.google.com/security/infrastructure/design/#secure_low_level_infrastructure

TOOL	DESCRIPTION	BENEFITS
Cloud SDK	Command-line interface for Google Cloud Platform products and services	Manage all of your Google Cloud Platform projects from the command line including compute, networking, storage and development products.
Cloud Shell	Manage your infrastructure and applications from the command-line in any browser	Your own Linux VM accessible from your browser allows you to manage your GCP resources with all of the necessary tools pre-installed and up-to-date.
Cloud Source Repositories	Private Git repositories hosted on Google Cloud Platform	Enable collaborative development with hosted Git repositories and improve developer productivity with automatic integration with Stackdriver Debugger and other Google Cloud Platform diagnostic tools.
Cloud Tools for Android Studio	Build backend services on Google Cloud Platform for your Android apps	Google Cloud Platform plugin for Android Studio lets you unify the development experience by letting you code, build, test and validate your backends in the same environment you use to develop your mobile apps.
Cloud Tools for IntelliJ	Deploy and debug production cloud applications right inside of IntelliJ	Google Cloud Platform plugin for IntelliJ lets you easily deploy and debug your Java applications directly from your IDE.
Cloud Tools for Eclipse	Deploy and debug App Engine Standard applications right inside of Eclipse	Google Cloud Platform plugin for Eclipse lets you easily deploy and debug your Java App Engine Standard applications directly from your IDE.
Cloud Tools for PowerShell	Full Google Cloud Platform control from Windows PowerShell	Cloud Tools for PowerShell lets you script, automate, and manage your Google Cloud Platform projects.
Cloud Tools for Visual Studio	Deploy Visual Studio applications to Google Cloud Platform	Google Cloud Platform plugin for Visual Studio lets you easily deploy your .NET applications directly and manage your projects from Visual Studio.
Cloud Deployment Manager	Create and manage cloud resources with simple templates	Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format using yaml.
Maven App Engine Plugin	Build and deploy your App Engine apps using Maven	The Google Maven Plugin and archetypes lets you easily build and deploy your App Engine applications using Maven.
Gradle App Engine Plugin	Build and deploy your App Engine apps using Gradle	The Google Gradle Plugin lets you easily build and deploy your App Engine applications using Gradle.

Figure 2: Choosing Developer Tools on GCP https://cloud.google.com/tools/docs/

Microsoft (Azure)

Microsoft Infrastructure Security Design Overview:

- DevOps tool integrations
- SDKs
- Azure Kubernetes Service (AKS)
- Container Instances
- Network Watcher
- Cloud Shell
- SQL Data Warehouse
- Developer tool integrations
- Big Custom Search
- Cost Management
- Container Registry
- CLIs
- Azure Data Lake Storage
- Azure Test Plans

The Azure Architecture Center contains guidance for building end-to-end solutions on Microsoft Azure.

Here you will find reference architectures, best practices, design patterns, scenario guides, and reference implementations.

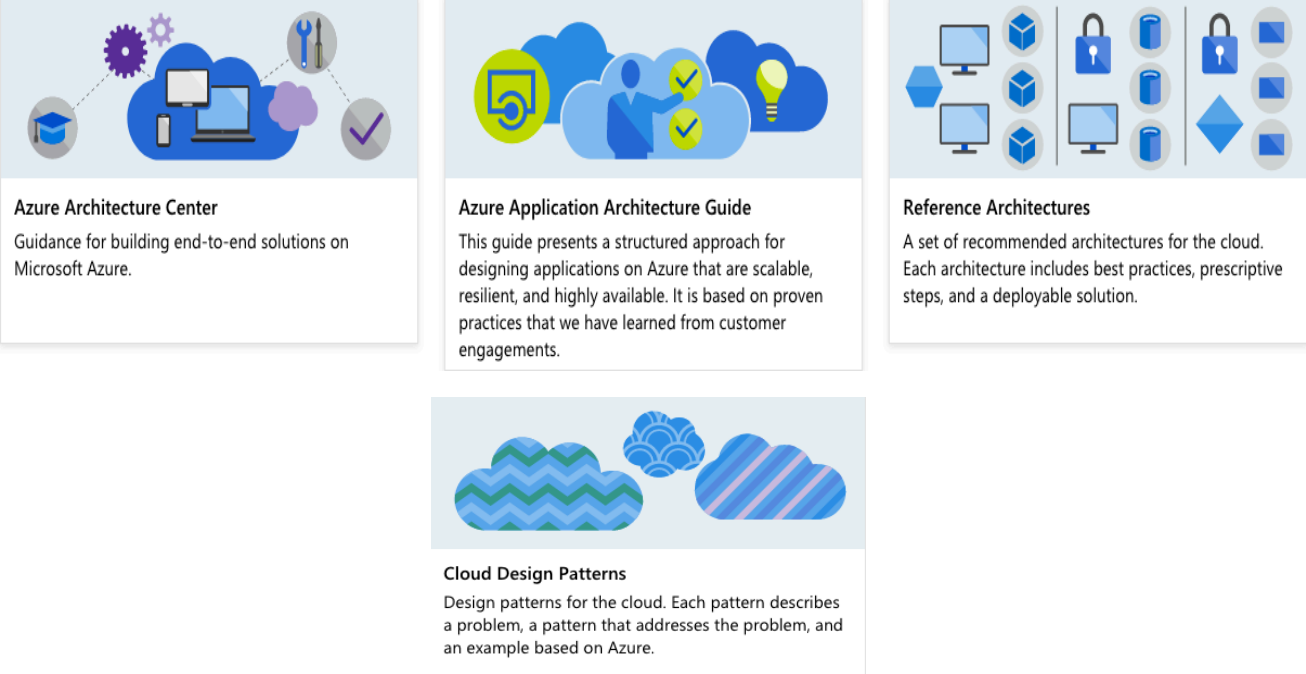


Figure 3: https://docs.microsoft.com/en-us/azure/index#pivot=architecture

2a. Report on ISO27001 (Google App Engine)

The ISO/IEC 27000 family of standards helps organizations keep information assets secure. ISO/IEC 27001 is a security standard that outlines and provides the requirements for an information security management system (ISMS). It specifies a set of best practices and details a list of security controls concerning the management of information risks.

Google Cloud Platform, our Common Infrastructure, and G Suite are certified as ISO 27001 compliant.

Google Cloud services that are in scope for ISO 27001:

Google Cloud Platform:

- Access Context Manager
- App Engine
- App Engine Flexible Environment
- BigQuery
- BigQuery Data Transfer Service
- Cloud Armor
- Cloud Bigtable
- Cloud Billing API
- Cloud CDN (Content Delivery Network)
- Cloud Console
- Cloud Console Mobile App
- Cloud Dataflow
- Cloud Datalab
- Cloud Dataproc
- Cloud Datastore
- Cloud Deployment Manager
- Cloud DNS (Domain Name System)
- Cloud Endpoints
- Cloud Firestore
- Cloud Functions
- Cloud Healthcare API
- Cloud Identity & Access Management
- Cloud Identity-Aware Proxy
- Cloud Interconnect
- Cloud IoT Core
- Cloud Job Discovery
- Cloud Key Management Service
- GCP Marketplace
- Cloud Load Balancing
- Cloud Machine Learning Engine
- Cloud Natural Language API
- Cloud Pub/Sub
- Cloud Resource Manager
- Cloud Router
- Cloud SDK
- Cloud Security Scanner
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speech-to-Text

- Cloud Translation API
- Cloud Video Intelligence API
- Cloud Vision API
- Cloud VPN
- Compute Engine
- Cloud Build
- Container Registry
- Data Loss Prevention API
- Dialogflow Enterprise Edition
- Genomics
- Google Service Control
- Kubernetes Engine
- Orbitera
- Persistent Disk
- Service Consumer Management API
- Service Management API
- Stackdriver Debugger
- Stackdriver Error Reporting
- Stackdriver Logging
- Stackdriver Profiler
- Stackdriver Trace

2b. Report on ISO27001 (Microsoft Azure)

Azure compliance: Azure Cosmos DB certified for *ISO 27001*, HIPAA, and the EU Model Clauses

*azure.microsoft.com/updates/azure-compliance-documentdb-certified-for-**iso**-**27001**-hipaa-and-the-eu-model-clauses/*

The Azure Cosmos DB team is excited to announce that Azure Cosmos DB is ***ISO 27001***, HIPAA, and EU Model Clauses compliant

Azure Data Catalog is *ISO*, CSA STAR, HIPAA, EU Model Clauses compliant

azure.microsoft.com/updates/data-catalog-compliance/

Azure Data Catalog is ***ISO***/IEC ***27001***, ***ISO***/IEC 27018, HIPAA, CSA STAR, and EU Model Clauses compliant

Logic Apps is *ISO*, HIPAA, CSA STAR, PCI DSS, SOC, and EU Model Clauses compliant

*azure.microsoft.com/updates/azure-logic-apps-is-**iso**-soc-pci-dss-csa-star-hipaa-eu-model-clauses-compliant/*

The Logic Apps feature of Azure App Service is now ***ISO***/IEC ***27001***, ***ISO***/IEC 27018, HIPAA, CSA STAR, PCI DSS, SOC, and EU Model Clauses compliant

https://azure.microsoft.com/en-us/search/updates/?q=ISO+27001

3. *Dependencies to consider when architecting security for the cloud.*

	Public/Hybrid Cloud- Threats	*Private Cloud - Threats*	*Mitigation*
PaaS	*OWASP Top 10* *Data leakage* *Privilege escalation via management console misconfiguration* *Exploiting VM weakness* *DoS attack via API* *Weak protection of privileged keys* *VM Isolation failure* *Privilege escalation via API* *Authorization weakness in platform services such as Message Queue, NoSQL, Blog services* *Vulnerabilities in the run time engine resulting in tenant isolation failure*	*OWASP Top 10* *Data theft (insiders)* *Privilege escalation via management console misconfiguration* *Privilege escalation via API*	*Testing apps and API for OWASP Top 10 vulnerabilities* *Hardening of VM image* *Security controls including encryption, Multi-factor authentication, fine granular authorization, logging* *Security automation – Automatic provisioning of firewall policies, privileged accounts, DNS, application identity*

Conclusion:

When the time comes to decide which service provider to choose based on the security architecture and after the review of the cloud platform´s maturity, transparency, compliance with enterprise security standards focusing on the CARS program; I would be leaning towards the cloud solution Google offers, as this program has a short life expectancy (1 month). Besides the solution Microsoft offers is notably more expensive.

Google has a global scale technical infrastructure designed to provide security through the entire information processing lifecycle at Google. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.

Google uses this infrastructure to build its internet services, and enterprise services such as G Suite and Google Cloud Platform.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the

infrastructure, and finally, the technical constraints and processes in place to support operational security.

Google invests heavily in securing its infrastructure with many hundreds of engineers dedicated to security and privacy distributed across all of Google, including many who are recognized industry authorities.

This global scale infrastructure is designed to provide security through the entire information processing lifecycle at Google. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.

https://cloud.google.com/security/infrastructure/design/

Microsoft Azure runs in datacenters managed and operated by Microsoft. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity.

- Infrastructure security
- Availability
- Network architecture
- SQL Database
- Monitoring
- Data protection
- Physical security
- Components and boundaries
- Production network
- Operations
- Integrity
- Microsoft Antimalware

https://docs.microsoft.com/en-us/azure/security/azure-security

Articles; to consider when choosing a cloud service provider for this Government´s program (CARS):

Google bows out of running for JEDI contract

Google has opted to drop out of the running for the Department of Defense's $10 billion cloud computing contract. The company said the contract could violate its artificial intelligence principles and that it will use its cloud to support the US government in other ways.

https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition?srnd=technology-vp

Microsoft, Grab launch 5-year collaboration

Microsoft and ride-sharing service Grab have launched a five-year agreement in which Grab will use the Azure cloud platform and artificial intelligence capabilities to expand its platform in Southeast Asia. Microsoft also announced a strategic investment in the ride-sharing company, working together to develop mobile facial recognition for drivers and passengers.

https://www.zdnet.com/article/microsoft-buys-into-grab-as-pair-focus-on-big-data-and-ai-on-azure/