DIPLOMA IN CLOUD SECURITY

Project Assignment 2: Security Challenges

By

Juan José Para Catalá

02nd November 2018

Table of Contents:

	Page(s)
Background	3
Assess the security challenges that the system may encounter.	
Summary	4
Security policy implementation	4 - 5
Intrusion Detection	6
Government Regulations	6
Virtualization security management	6
CSIRT	7
SECURITY RISKS	7 - 8
RECOMMENDATIONS	8 - 9
Conclusion	9

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. *Assess the security challenges that the system may encounter.*

Summary

Here we are going to see some of the characteristics and features to have in consideration when comes to security challenges and applying them to Google as our CSP for CARS program.

We are also going to see where Google stands referring to the following challenges that our system may encounter (Security Policy implementation, Encryption, Intrusion Detection, Government regulations, Virtualization security management and the importance of CSIRT).

To assess the security challenges we need to determine the levels of responsibility in place. So in our case and based on the background, the service delivery model is Platform as a Service (PaaS), and our level of responsibility begin with Platform Security as a shared responsibility, follow by the Application Security, Data Security and Security Governance as you can see in the following graph.



Figure 1: Mile2/v4/t/lecture/10845814?start=630

Security policy implementation

One of the Cloud security concerns in our service delivery mode is to manage user privileges. Google offer security products that help us meet our policy, regulatory, and business objectives.

The disruption by DoS attacks or misconfiguration errors by cloud service operators or customers, could be well considered one of the many challenges we should think about too. These errors have the potential to cascade across the cloud and disrupt the network, systems and storage hosting cloud applications.

Another big challenge and concern is our data manipulation. The need of encryption to protect our data is fundamental.
Google Cloud Storage always encrypts the data on the server side, before it is written to disk, at no additional charge. Besides this default behavior, there are additional ways to encrypt the data when using Google Cloud Storage.

Below is a summary of the encryption options available by Google:

Server-side encryption: encryption that occurs after Cloud Storage receives your data, but before the data is written to disk and stored.

Google-managed encryption keys: Cloud Storage uses its server-side encryption keys to encrypt your data. This is the default for Cloud Storage encryption.
Customer-supplied encryption keys: You can create and manage your own encryption keys for server-side encryption, which replace the Google-managed encryption keys.
Customer-managed encryption keys: You can generate and manage your encryption keys using Cloud Key Management Service. These replace the Google-managed encryption keys.
Client-side encryption: encryption that occurs before data is sent to Cloud Storage. Such data arrives at Cloud Storage already encrypted but also undergoes server-side encryption.

https://cloud.google.com/storage/docs/encryption/

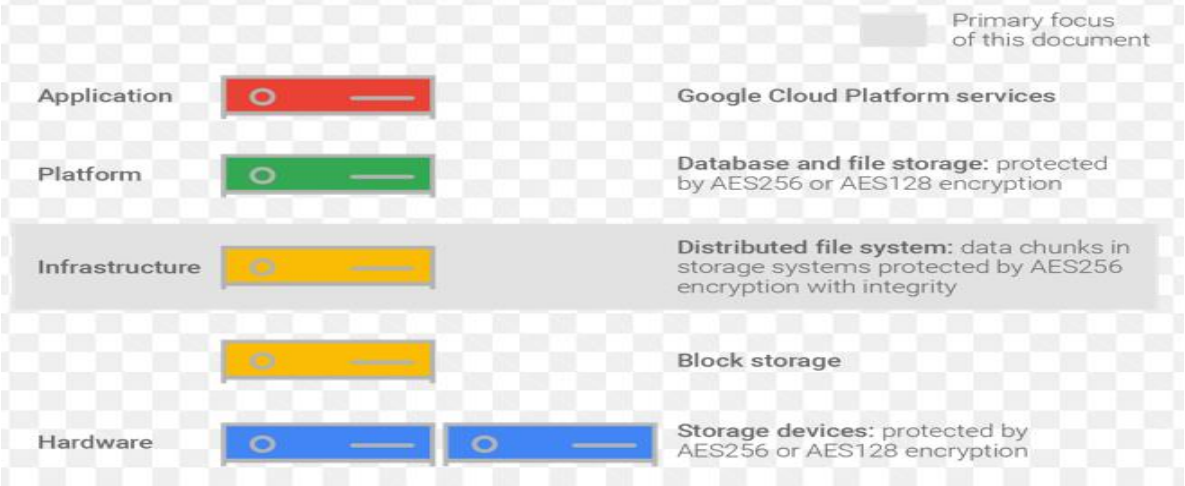


Figure 2: https://cloud.google.com/security/encryption-at-rest/default-encryption/

Another use case to have under consideration is Single Sign-On (SSO). SSO implemented within an enterprise may not be extensible to the cloud application unless it is a federation architecture using SAML 1.1 or 2.0 supported by the cloud service provider.

In this case implement sso with saml exchange - Google recommends using fully managed corporate google accounts for increased visibility, auditing, and control over access to cloud platform resources. Cloud identity provides free, managed google accounts you can use with google services including cloud platform.

Intrusion Detection

Google intrusion detection involves tightly controlling the size and make-up of Google's attack surface through preventative measures, employing intelligent detection controls at data entry points, and employing technologies that automatically remedy certain dangerous situations.

https://cloud.google.com/security/overview/

Government Regulations

Improve citizen services, increase operational effectiveness, and deliver proven innovation at your government agency with our highly secured, powerful technology.

With Google Cloud Platform's (GCP) powerful technology, you can scale your storage and analytics capabilities without affecting speed or security. No matter the size or complexity of the datasets, you can design a robust disaster recovery plan without having to worry about managing capacity or infrastructure.

We do our part to help you protect sensitive PII — protecting your agency and preserving your citizens' privacy by offering comprehensive data protection, identity management, network security, and threat detection and response capabilities.

https://cloud.google.com/solutions/government/

We have a look at ENISA (European Network & Information Security Agency):

ENISA, supported by a group of subject matter expert comprising representatives from Industries, Academia and Governmental Organizations, has conducted, in the context of the Emerging and Future Risk Framework project, and risks assessment on cloud computing business model and technologies.

Virtualization security management

On Compute Engine, virtual machines are called **virtual machine (VM) instances**. You can create and manage these instances in several ways, including:

The Google Cloud Platform Console, a web UI that is comparable to management tools like vCenter or XenCenter.

The Google Cloud SDK.

The Compute Engine API, which allows you to interact with your Compute Engine resources from applications.

Each virtual machine (VM) runs with an associated virtual machine manager (VMM) service instance. The infrastructure provides these services with two identities. One identity is used by the VMM service instance for its own calls and one identity is used for calls that the VMM makes on behalf of the customer's VM. This allows us to further segment the trust placed in calls coming from the VMM.

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

CSIRT

There are important considerations before starting a program. Some of them are operational and technical issues such as equipment, security, and team staffing considerations. In addition, it's critical to determine resources needed for both newly formed teams as well as existing teams, including CSIRT consultants, who can be brought on board to help with planning.

http://www.disaster-resource.com/index.php?option=com_content&view=article&id=2535:the-important-role-of-a-cyber-security-incident-response-program&catid=6:information-technology

A CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

A CSIRT can be a formalized team or an ad hoc team. A formalized team performs incident response work as its major job function. An ad hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises.

The primary mission of a CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents, and to contribute to the prevention of such incidents by engaging in threat assessment and detection, mitigation planning, incident trend analysis, and security architecture review.



Figure 3: https://ondemandelearning.cisco.com/cybersec-fastlane/secops/sections/14/pages/2

Typical CSIRT mission statements include the following:

Responsible for global 24-hour monitoring, investigation, and response to cybersecurity incidents.
Engage in proactive threat assessment, mitigation planning, incident detection and response, incident trending with analysis, and the development of security architecture.

https://ondemandelearning.cisco.com/cybersec-fastlane/secops/sections/14/pages/4

SECURITY RISKS

The most important classes of cloud-specific risks are:

LOSS OF GOVERNANCE: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security.

LOCK-IN: there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can

make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment.

ISOLATION FAILURE: multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants. However it should be considered that attacks on resource isolation mechanisms (e.g.,. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

COMPLIANCE RISKS: investment in achieving certification may be put at risk by migration to the cloud: - if the CP cannot provide evidence of their own compliance with the relevant requirements - if the CP does not permit audit by the cloud customer (CC).

MANAGEMENT INTERFACE COMPROMISE: customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

DATA PROTECTION: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way.

INSECURE OR INCOMPLETE DATA DELETION*:* when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

MALICIOUS INSIDER: while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk.

file:///C:/Users/ParaJ/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/Cloud%20Computing%20Security%20Risk%20Assessment.pdf

RECOMMENDATIONS

ASSURANCE FOR CLOUD CUSTOMERS Cloud customers need assurance that providers are following sound security practices in mitigating the risks facing both the customer and the provider (e.g., DDoS attacks)

LEGAL RECOMMENDATIONS Most legal issues involved in cloud computing will currently be resolved during contract evaluation

BUILDING TRUST IN THE CLOUD Effects of different forms of breach reporting on security. End-to-end data confidentiality in the cloud and beyond. Higher assurance clouds, virtual private clouds, etc.

DATA PROTECTION IN LARGE SCALE CROSS-ORGANIZATIONAL SYSTEMS Forensics and evidence gathering mechanisms, Incident handling - monitoring and traceability, International differences in relevant regulations including data protection and privacy.

LARGE SCALE COMPUTER SYSTEMS ENGINEERING Resource isolation mechanisms - data, processing, memory, logs etc. Interoperability between cloud providers. Resilience of cloud computing.

file:///C:/Users/ParaJ/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/Cloud%20Computing%20Security%20Risk%20Assessment.pdf

Conclusion

Previously we have mentioned some of the most important security risks to have in consideration such as *LOCK-IN,* which Google (GCP) with open-source tools like Grafeas, Spinnaker, and Kubernetes, provides a secure, repeatable, and traceable deployment pipeline to prevent lock-in. Choose from Google App Engine (GAE), Google Kubernetes Engine (GKE), Google Compute Engine (GCE).
DATA PROTECTION, Google Cloud takes a customer-centric approach on protection, control, and compliance, assisting on GDPR.

Although Google has covered its part regarding security, they offer advice, guidance and possible solutions to adapt to all our needs.