GOOGLE INFRASTRUCTURE SECURITY DESIGN

Shehryar Kamran

Table of Contents

Executive Summary

This document provides information on security of google infrastructure, belongs to security executive, security architects and auditors

Introduction

This document contains following information:

- Secure services deployment
- Secure data and end-user privacy safeguards
- Secure and private communication over internet
- Safe operations

Security layers are described in following sections.

Secure low-level infrastructure

Security of hardware, software stack running on the hardware and physical premises of data centers covered in this section,

Security of physical premises

- Multiple layered tightly controlled personal data centers
- Multiple physical security layers
- Metal detector, biometric identification, laser-base intrusion detection system, cameras, vehicle barriers

Hardware design and provenance

- Design server board and networking equipment
- Audit and validate components properties by external auditors
- Design custom hardware chips to authenticate legitimate devices

Secure boot stack and machine identity

- Cryptographic signature for low-level components
- Validate signatures during each boot or update cycle
- Continually improve security with every new generation of hardware

Automated system to do following functionality:

- Ensure servers have software's stack up to date
- Detect and diagnose software hardware
- Machines and peripherals integrity verification with verified boot and implicit attestation
- Intended software and firmware can only access the credentials to communicate on production network
- Services and machines remove or re-allocate after they no longer needed

Secure service deployment

Infrastructure follows zero trust model, trust no service, device, users by default from inside as well as outside of network.

Service identity, integrity, and isolation

- Cryptographic authentication and authorization for inter-service communication
- Do not rely on firewall and internal network segmentation as primary security mechanism
- Security policies confirm that communication is done with intended server with limited access to data and functionality
- Sandbox use to separate services execution from other services

Inter-service access management

- Audit logging, justifications and unilateral access restriction
- Services can be allowed or deny their access according to their identities
- Logging, approval chains and notification are used for managing identities
- System verifies that an engineer cannot perform sensitive operations without approval from another authorized engineer

Encryption of inter-service communication

- All communication is verified and encrypted
- Automatic end-to-end encryption for infrastructure traffic

Access management of end-user data in Google Workspace

- Return data of only end-user to whom it belongs
- Verify user by taking credentials to generate a ticket for short time period

Secure data storage

Data security stored on infrastructure is described here.

Encryption at rest

- Several layers of encryption to protect data
- Encrypt all data before writing to storage
- Hardware encryption is activated in HDD and SSD
- Track each drive through their lifecycles
- Before a decommissioned, storage devices cleaned by multi step process, if it is not pass through this process then it will physically destroy

Deletion of data

- Marking specific data as schedule started for deleting data
- When user deletes its account, infrastructure tells service to delete data associated with its account
- End user have full control to delete their data

Secure internet communication

Communication between internet and services that run on Google infrastructure.

Google Front End service

- Services available on internet must register itself from Google Front End (GFE)
- GFE verifies TLS connection termination with correct certificate
- Provides protection against DOS attack
- Internal services use as externally uses GFE as smart reverse-proxy frontend

DoS protection

- Absorbs many DOS attacks
- Multi-tier, multi-layer Dos protection
- Software and hardware level load balancer are used for connections
- Load balancer report information about incoming traffic to central DOS service running
- Drop or throttle traffic associated with the attack by dos service after detection

- GFE give application layer information to DOS service which load balancer don't have access, drop that traffic also

User authentication

- Central identity service used
- User can interact with this service using Google login
- Get information from user according to risk factor

Operational Security

Protect infrastructure, employees' machine and credentials from inside as well as outside attacks

Safe software development

- Prevent developer from security bugs using specific libraries
- Manual security review of each aspect in depth
- Bug Bounty program
- Invest in zero-day vulnerability

Source code protections

- Confirm that software and configuration are reviewed and authorized
- Confirm that code meet certain minimum standards
- Limit the insider to perform changes, give forensics facility to them

Keeping employee devices and credentials safe

- Mandatory use of U2F-compatible security keys
- Monitor client devices to check their device is up to date, don't have any malicious application, suitable for corporate
- Zero trust mechanism is used to secure employee access to resources

Reducing insider risk

- Limit and actively monitor employee having administration privileges
- Eliminate privilege access by automating task in safe environment

Threat monitoring

- Threat Analysis group monitors threat actors

Intrusion detection

- Red Team Exercise to improve effectiveness
- Investigation and incident response team work 24 hours a day,365 days a year
- Sophisticated data processing pipelines on individual devices
- Rules and machine intelligence on top of this pipelines give warning to engineers about incident

(Team, 2022)

Conclusions

Google Infrastructure Security Design tell us that to secure corporate we should focus on following:

- Secure low-level infrastructure
- Secure service deployment
- Secure data storage
- Secure internet communication
- Operational Security

Bibliography

Team, C. A. (2022, March). *Google infrastructure security design overview*. Retrieved from Google Cloud: https://cloud.google.com/static/docs/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf