Day 18

"CLOUD SECURITY"

Secure Low-level Infrastructure of GCP:

- **Physical and Environmental Security**: Google protects its data centers with multi-layered physical security including biometrics, surveillance, intrusion detection, and restricted employee access—even in third-party data centers.
- **Custom Hardware and Trusted Components**: Google designs its own servers, network equipment, and custom security chips, ensuring hardware provenance and secure component sourcing to verify authenticity and reduce risks.
- **Secure Boot and Machine Identity**: Each server uses cryptographic signatures and hardware-based roots of trust to verify the software stack during boot, with unique machine identities used for secure authentication and automation.

Secure Service Deployment of GCP:

1. **Service Identity, Integrity, and Isolation**: Every service has a unique identity using cryptographic credentials to authenticate and authorize inter-service communication. Google ensures service integrity through source code auditing and isolation via sandboxes and virtualization, especially for higher-risk services.
2. **Access Management**: Services and Google engineers are managed with strong access controls, approval workflows, and whitelisting mechanisms. Access control policies are enforced by the infrastructure based on service and employee identities maintained in a global namespace.
3. **Encrypted Communication and End-User Data Protection**: All inter-service communication is encrypted by default, including WAN traffic. End-user access is restricted through "permission tickets" issued by a central identity service, ensuring services can access data only on behalf of authorized users.

Securing the GCP:

1. **Service and Control Plane Security**: Google Compute Engine (GCE) runs on secure infrastructure with features like secure boot, service isolation via discrete service accounts, and a secure control plane protected by DoS prevention, SSL/TLS via Google Front End (GFE), and centralized identity and access management.
2. **Encryption and Traffic Protection**: Control plane traffic is encrypted both in-transit (WAN and some internal data center links) and at rest (persistent disks via centralized key management). Google also provides optional VM traffic encryption, with automatic WAN encryption being implemented.
3. **VM Isolation and Operational Controls**: GCE uses hardened KVM-based hardware virtualization for VM isolation, tested with fuzzing and code review. Google enforces strict operational security and customer data policies to ensure access to user data is limited and controlled.

--The End--