Risks of Impersonated Service Account in GCP

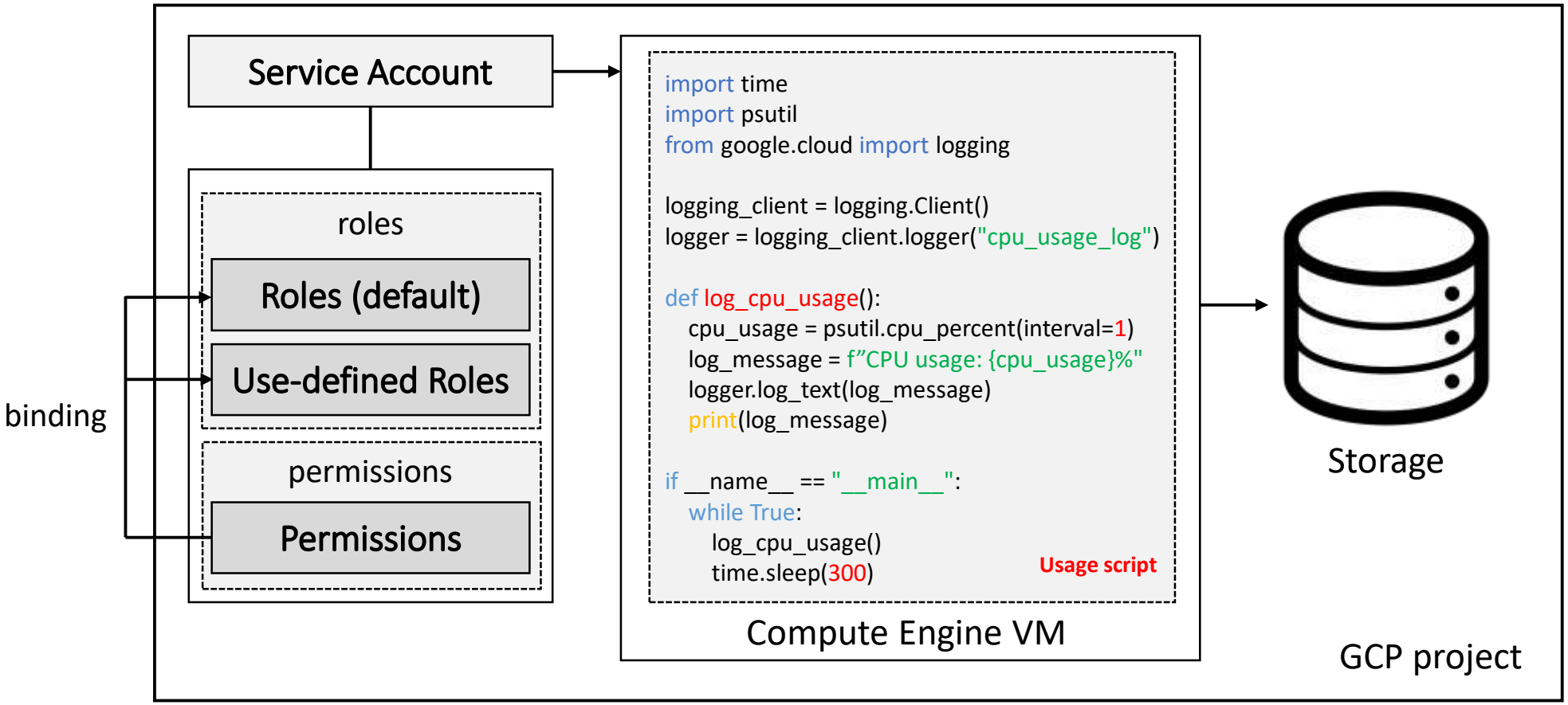
HYEOUNJUN PARK

Department of Computer Science & Engineering

Incheon National University

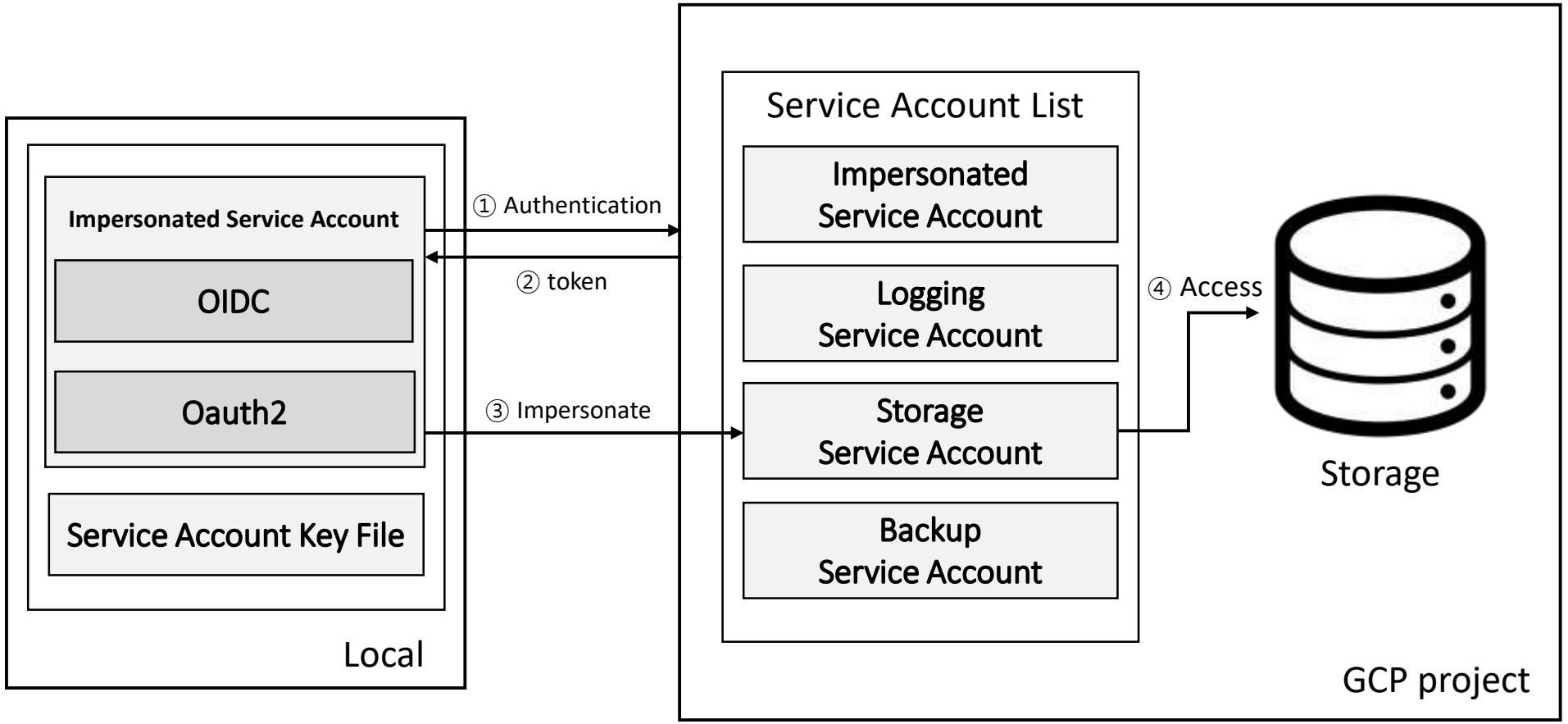
Service Account

- It is an assistant tool can access VMs or users to resources in GCP project.



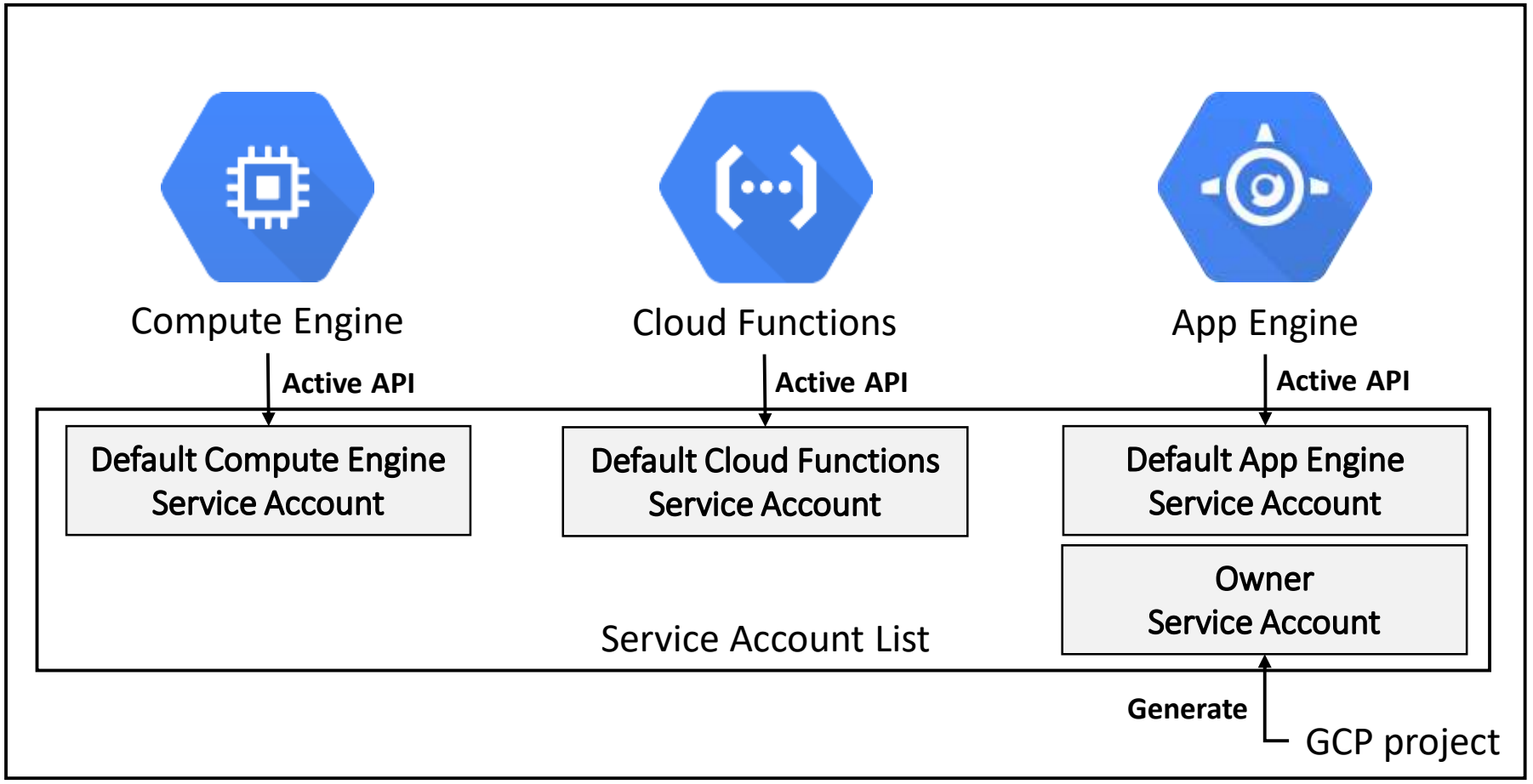
Impersonated Service Account

- External local environments can access resources using impersonated service account.



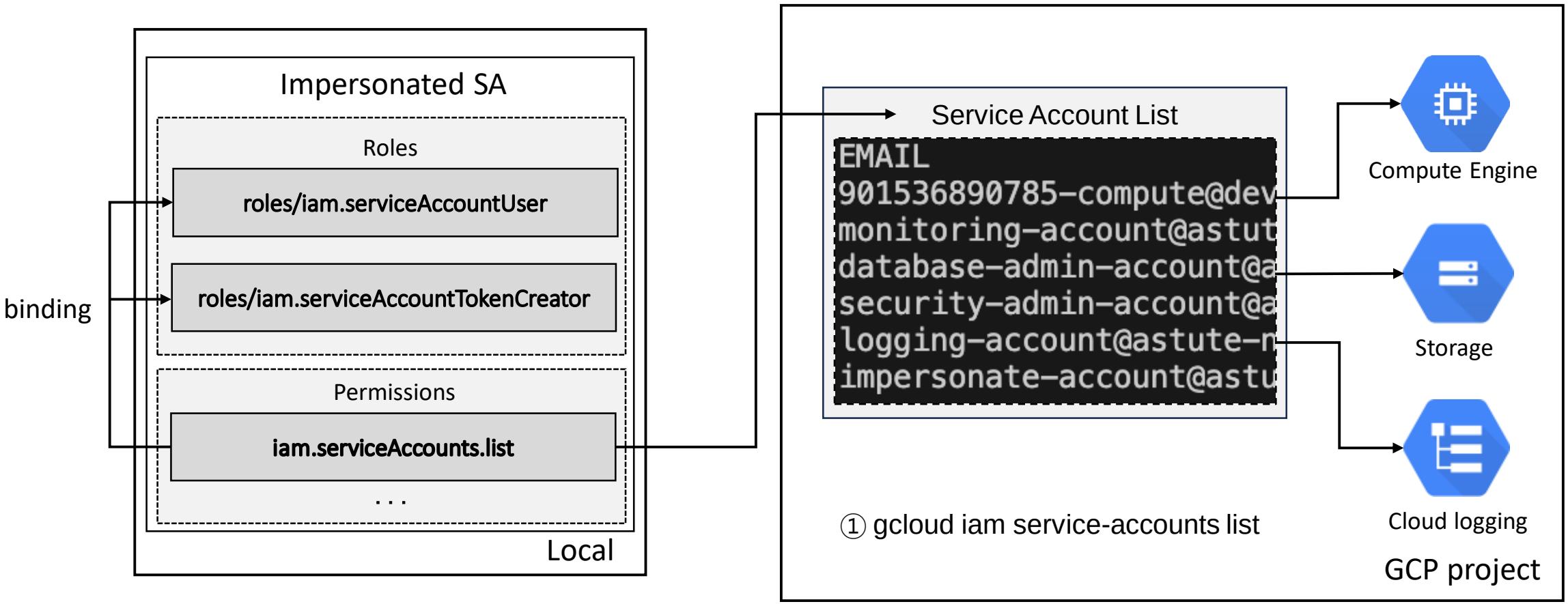
Default Service Account

- Generate default service accounts when APIs are turned on in the project.



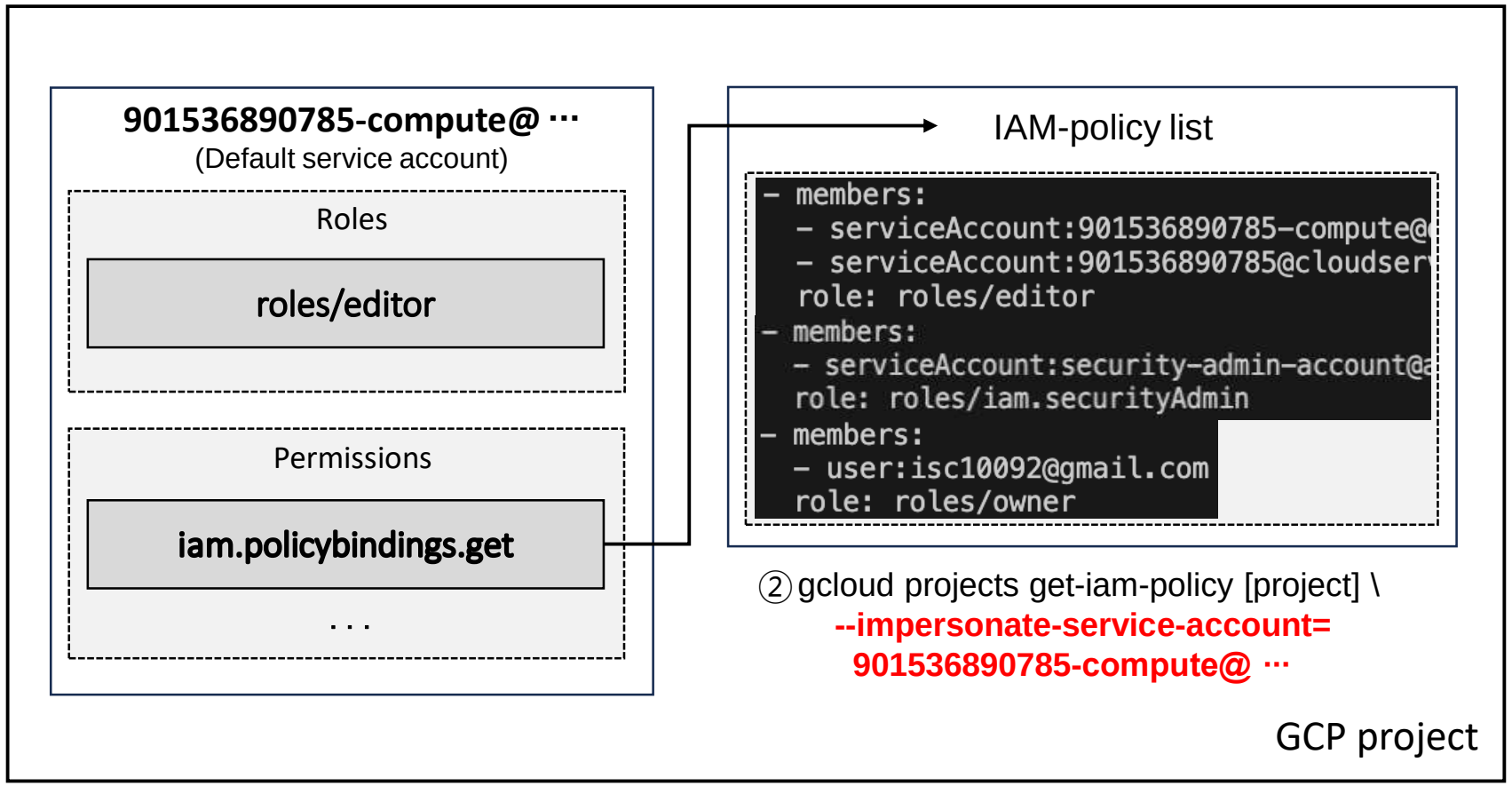
Attack Flow

1. View the list of service accounts in project through CLI using impersonated service account.



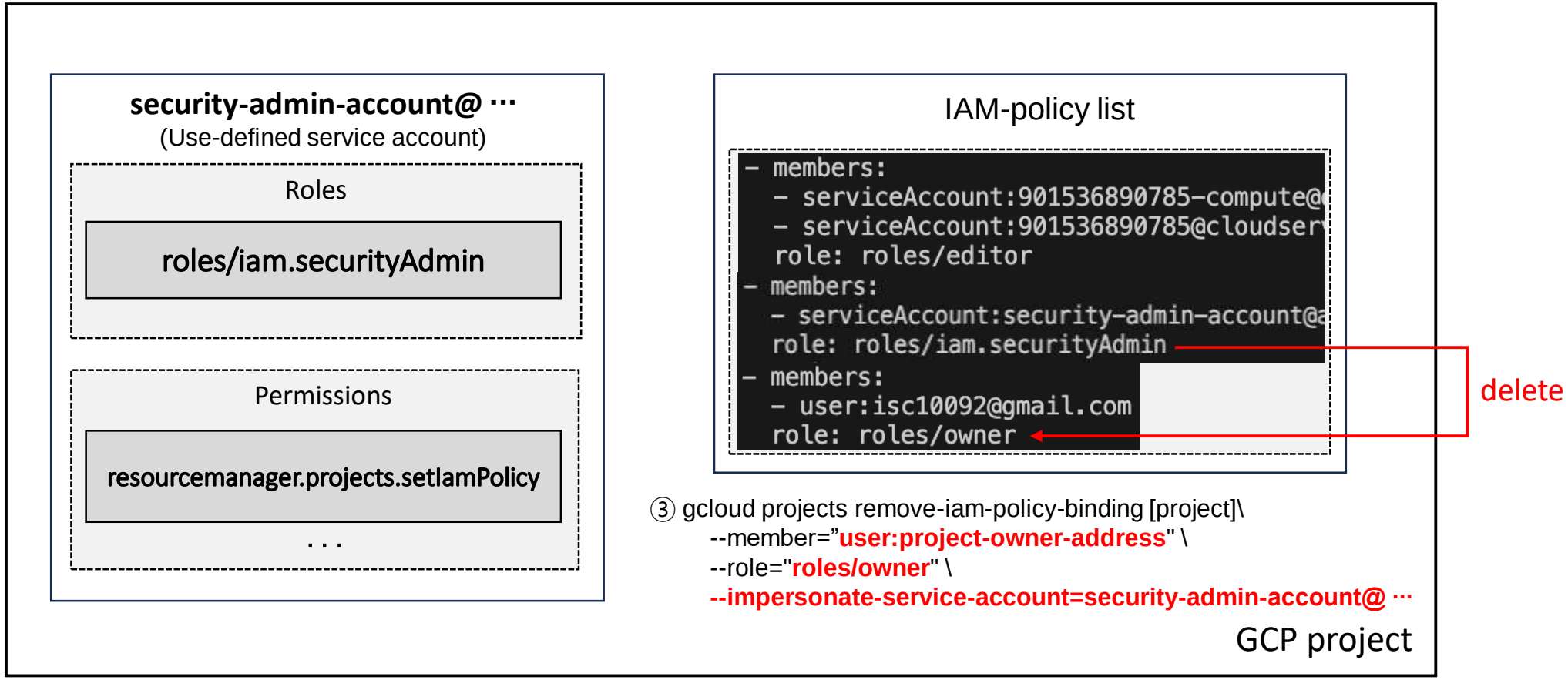
Attack Flow

2. Get bound policies to important roles through impersonating compute engine service account.



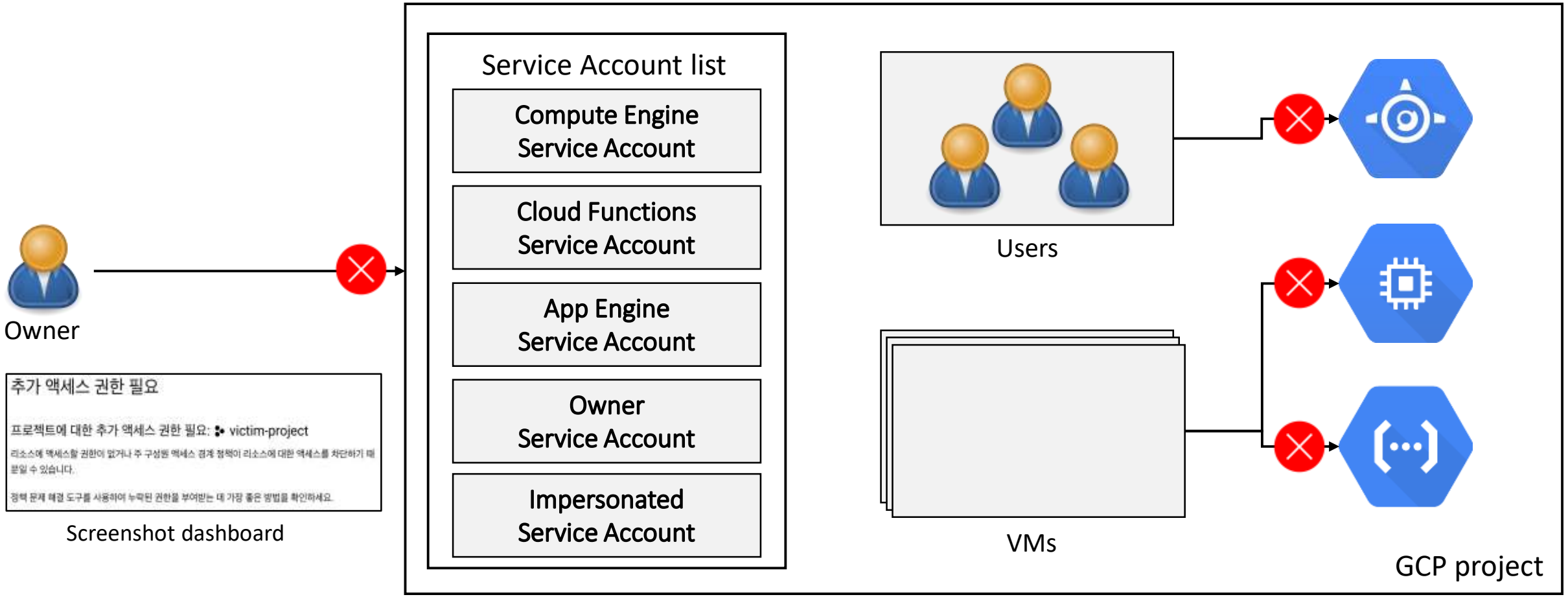
Attack Flow

3. Finally, delete important service account such as project owner.



Result of Attack

- If the attack is successful, the project is dysfunctional.



Conclusion

- In this paper, we analyzed **security threats** and **project frozen attack scenario** through **impersonated service account** in GCP environment.

- As a **countermeasures**, when deleting a **high-privileged** service account, a **warning message** or **two-factor authentication** through login can be introduced.

- **Don’t use default service accounts**, instead, create and use a **customized service account** by following the **rules of least privilege.**

- In future work, **compare security risks of service account** across various cloud platforms, such as AWS, and Azure, would provide broader insights into the importance of cloud security.