Google Cloud Platform(GCP)에서 가장된 서비스 계정의 위험에 관한 연구

박현준[1], 이승수[2]
[1]인천대학교 컴퓨터공학부 학부생
[2]인천대학교 컴퓨터공학부 교수
isc10093@inu.ac.kr, seungsoo@inu.ac.kr

Study on the Risks of Impersonated Service Accounts in Google Cloud Platform (GCP)

Hyeon-Jun Park[1], Seungsoo Lee[2]
[1]Dept. of Computer Science and Engineering, Incheon National University
[2]Dept. of Computer Science and Engineering, Incheon National University

요 약

멀티 클라우드 및 하이브리드 클라우드 환경의 확산은 클라우드 인프라의 복잡성을 증가시키는 만큼, 보안 관리의 중요성 역시 높아지고 있다. 특히, 여러 가지 보안 설정 중에서, 본 논문은 GCP(Google Cloud Platform)에서 서비스 계정의 가장(impersonate)을 통한 프로젝트 마비 공격의 위험성을 분석한다. 공격자는 IAM 정책을 변경하거나 삭제하여 프로젝트의 정상적인 기능을 마비시킬 수 있으며, 이러한 상황이 발생하면 서비스 복구에는 상당한 시간이 소요될 수 있다. 이러한 공격을 방지하기 위해 다단계 인증(Multi-Factor Authentication, MFA) 등과 같은 보안 대책도 제시한다.

1. 서론

멀티 클라우드와 하이브리드 클라우드 환경이 점점 더 많은 조직에서 채택됨에 따라, 클라우드 인프라의 복잡성은 더욱 증가하고 있다. 서비스 계정(service accounts)은 이와 같은 클라우드 환경에서 중요한 관리 도구로 활용되며, 효율적인 리소스 관리와 보안을 유지하는 데 핵심적인 역할을 한다. 예를 들어, 서비스 계정을 가상 머신에 할당하여 스크립트를 통해 로그 수집, 모니터링, 스토리지 접근, 보안 정책 관리 등의 다양한 클라우드 작업을 자동화할 수 있다. 이러한 자동화는 인적 오류를 줄이고, 운영 효율성을 높이는 동시에 클라우드 리소스 관리의 복잡성을 감소시킨다. 이때, 특정 작업이나 애플리케이션의 실행을 위해 서비스 계정을 가장(impersonate)하는 것이 필요할 때도 있다. 이는 외부 애플리케이션 통합 또는 특정 리소스에 대한 제한적 접근을 허용하기 위한 상황에서 유용하다. 하지만, 이러한 가장이 악의적으로 사용되거나 서비스 계정이 잘못 관리될 경우, 프로젝트 전체를 마비시킬 수 있는 심각한 보안 위협이 발생할 수 있다 [1].

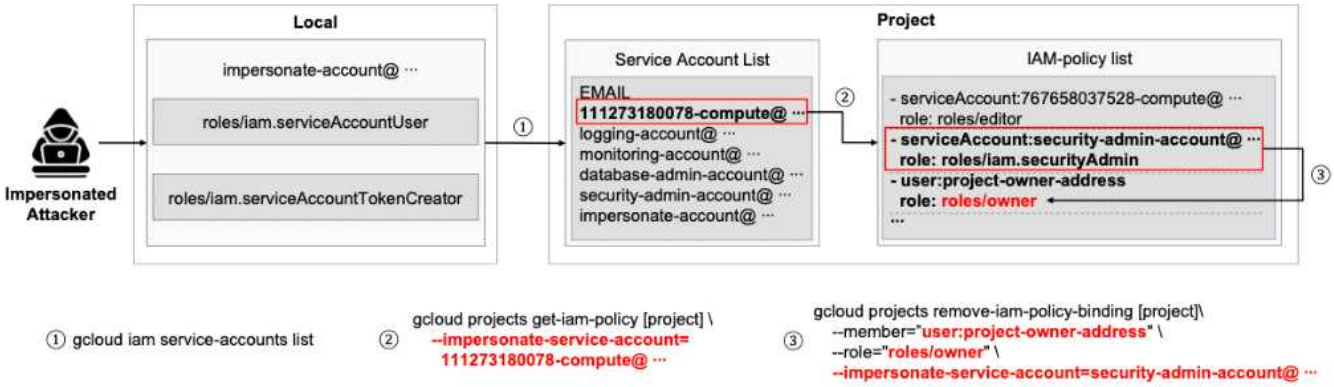
본 논문에서는 Google Cloud Platform (GCP) 환경에서 서비스 계정을 통해 발생할 수 있는 프로젝트 마비 공격의 메커니즘을 분석하고, 이러한 공격이 미치는 영향을 언급한다. 이를 통해, 멀티 클라우드와 하이브리드 클라우드 환경에서의 보안 관리의 중요성을 강조하고, 보안 강화를 위한 실질적인 대책을 제시한다.

2. 프로젝트 마비 공격

2.1. 위협 상황

본 논문에서는 GCP 환경에서 여러 클러스터나 가상머신을 운영할 때, 기본적으로 생성되는 Compute Engine 서비스 계정이 활성화된 상태를 가정한다. 이 서비스 계정은 클러스터 노드와 같은 중요한 리소스를 관리하기 위해 필요하며, 프로젝트의 다양한 리소스에 접근할 수 있는 역할인 **roles/editor**가 부여되어 있다.

또한, 서비스 계정 가장을 통해 공격자가 프로젝트의 서비스 계정에 접근할 수 있는 상황을 가정한다. Google 문서에 따르면, 서비스 계정 가장을 하기 위해 **roles/iam.serviceAccountUser**와 **roles/iam.serviceAccountTokenCreator**라는 역할이 필요하다. 특히, **roles/iam.serviceAccountUser** 역할 안에 포함된 **iam.serviceAccounts.list**의 권한은 공격자가 프로젝트 내에 존재하는 모든 서비스 계정 목록을 조회할 수 있다.



(그림 1) Overview of Project Frozen Attack

마지막으로, 프로젝트에 속한 모든 리소스에 대한 접근 제어를 체계적으로 관리하고, 보안 정책의 일관성을 유지할 수 있는 **roles/iam.securityAdmin** 역할을 가진 서비스 계정이 활성화된 상태를 가정한다. 이 권한은 프로젝트 내의 모든 IAM 정책을 설정하고 관리할 수 있으며, 이를 통해 프로젝트에 속한 모든 IAM 정책을 변경하거나 삭제할 수 있다.

2.2. 공격 메커니즘

프로젝트 마비 공격의 개요는 그림 1과 같으며, 공격의 전반적인 흐름은 다음과 같다. (1) 공격자는 먼저 **iam.serviceAccounts.list** 권한을 사용해 프로젝트 내 모든 서비스 계정의 목록을 조회한다. 이 중 Compute Engine과 관련된 서비스 계정(예: **111273180078-compute@...**)을 볼 수 있다.

(2) 이어서, 공격자는 해당 Compute Engine 서비스 계정을 가장하여 프로젝트의 IAM 정책을 조회한다. 특히 **roles/iam.securityAdmin** 역할을 가진 서비스 계정(예: **security-admin-account@...**)은 프로젝트 내 모든 IAM 정책을 관리할 수 있는 강력한 역할로, 공격자가 이 계정을 가장하면 프로젝트의 중요한 정책들을 변경하거나 삭제할 수 있다.

(3) 최종적으로, 공격자는 **security-admin-account** 계정을 가장하여 프로젝트를 만들 때 자동으로 소유자에게 부여되는 **roles/owner** 역할을 삭제한다. 이로 인해 소유자는 프로젝트에 대한 전체적인 제어권을 상실하게 되며, 프로젝트의 정상적인 기능이 마비된다. 제어권을 다시 확보하기 위해서는 조직 관리자에게 문의하여 **roles/owner** 역할을 복구해야 하며, 이 과정에는 예상치 못한 시간이 소요될 수 있고 그동안 서비스가 중지되어 이를 이용하는 사용자들에게 심각한 영향을 미칠 수 있다.

2.3. 해결 방안

서비스 계정 가장을 통한 보안 위협을 완화할 수 있는 방법 중 하나는 다단계 인증(Multi-Factor-Authentication, MFA)을 도입하는 것이다 [2]. 특히 IAM 정책을 삭제하거나 수정할 때, 서비스 계정을 가장하여 이러한 작업을 시도할 경우, MFA를 통해 로그인과 같은 추가적인 인증을 요구함으로써 보안을 강화할 수 있다.

3. 결론

본 논문에서는 GCP 환경에서 서비스 계정 가장을 통한 보안 위협과 프로젝트 마비 공격 시나리오를 분석했다. 서비스 계정의 부적절한 관리나 악용은 프로젝트의 소유자 계정 삭제 등으로 이어져, 서비스 운영에 심각한 영향을 미칠 수 있다. 이러한 위험을 완화하기 위해 다단계 인증과 같은 보안 조치를 도입하는 것이 필요하다.

ACKNOWLEDGEMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 학석사연계 ICT핵심인재양성사업의 연구결과로 수행되었음(IITP-2024-RS-2024-00437024).

참고문헌

[1] netscope, "Over-Privileged Service Accounts Create Escalation of Privileged and Lateral Movement in GCP", 2021. [Online]. Available: https://www.netskope.com/blog/over-privileged-service-accounts-create-escalation-of-privileges-and-lateral-movement-in-google-cloud

[2] Otta, Soumya Prakash, et al. "A systematic survey of multi-factor authentication for cloud infrastructure." *Future Internet* 15.4 (2023): 146.