Man-in-the-Cloud Attack Analysis

Brendan Murphy

Harvard Extension School

Abstract

This paper explores a new cloud security threat scenario that researchers are calling a "Man-in-the-Cloud" (MITC) attack. This unique attack targets cloud storage service providers that have foregone security best practices and enabled users to authenticate using a synchronization token in place of the more secure username and password authentication procedure. My research shows that this threat scenario exploits OWASP Cloud Top 10 vulnerabilities and OWASP Mobile Top 10 vulnerabilities that are present in many cloud storage solutions. In order to mitigate against Man-in-the-Cloud attacks, users and organizations should employ the usage of Database Activity Monitoring (DAM) tools and File Activity Monitoring (FAM) solutions to monitor data flows from the cloud.

*Keywords*: Man-in-the-Cloud, Security, Cloud Security

Man-in-the-Cloud Attack Analysis

In a world where users expect a seamless experience accessing their personal data from any device, cloud storage service providers have responded with an innovative approach to data access. These cloud applications such as Google Drive and Dropbox have foregone security best practices and enabled users to authenticate using a synchronization token in place of more secure username and password combinations. This access procedure has been targeted by skilled hackers who are capable of stealing synchronization tokens in an effort to acquire sensitive user data. This new type of attack has been deemed a "Man-in-the-Cloud" (MITC) attack by security experts. This new threat scenario exploits OWASP Cloud Top 10 vulnerabilities and OWASP Mobile Top 10 vulnerabilities that are present in cloud storage solutions. In order to mitigate against Man-in-the-Cloud attacks, users and organizations should employ the usage of Database Activity Monitoring (DAM) tools and File Activity Monitoring (FAM) solutions to monitor data flows to and from the cloud.

There are two specific OWASP Cloud Top 10 vulnerabilities that the MITC threat scenario is able to successfully exploit. Firstly, MITC attacks present a challenge to R6: Service and Data Integration ("OWASP Cloud -10 Project ", n.d.). One of the key components of cloud data architecture is a secure pathway from the end user to the cloud data center. MITC attacks exploit a inherent security flaw that exists because, "Cloud computing models increase the risks associated with interception of data in transit, even though these risks are not unique to cloud. Cloud providers must ensure that they use SSL and/or tighter encryption protocols to secure data in transit." (Gupta, 2009; Christodorescu, Sailer, Schales, Sgandurra & Zamboni, 2009). Modern file synchronization services like Google Drive and Dropbox fail to implement tight security measures and allow users to access data with simple authorization tokens that are not as secure as other authorization methods.

MITC attacks also present a security risk to R1: Accountability and Data Ownership ("OWASP Cloud -10 Project ", n.d.). When users and organizations move their data into a cloud service provider, the question of who owns the data becomes a challenging inquiry to answer fairly. One must concede that when data is moved onto cloud-hosted services like Google Drive, users forego some ownership of that data and it becomes more challenging to protect. Each user is therefore at the mercy of the security principals and design patterns put in place by the cloud storage provider. This presents a risk to the cloud vulnerability principal of accountability and data ownership, and opens the door for exploits by pervasive and dedicated hacking parties.

There are three specific OWASP Mobile Top 10 vulnerabilities that the MITC threat scenario is able to exploit. Firstly, the usage of authorization tokens over traditionally secure authorization methods like username and password presents a violation of M3 - Insecure Communication: "This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc." ("Mobile Top 10 2016 ", 2016) Furthermore, the authorization token procedure violates two key principals of M4 - Insecure Authentication. These principals are: "Failing to identify the user at all when that should be required. Failure to maintain the user's identity when it is required." ("Mobile Top 10 2016 ", 2016) Lastly, although the cloud service providers would argue otherwise, it can be said that data hosted in the cloud presents a clear risk with regard to M2 - Insecure Data Storage. Although each cloud service provider would argue that their database is not prone to any data leakage, MITC attackers have demonstrated that this is not the case. Even Google, considered to be one of the most secure cloud companies in the world, suffered a large data breach in 2018 of its Firebase Cloud Service platform. This data leakage resulted in "over 3,000 mobile applications were left improperly secured, exposing a total of 113GB of data in 2300 unsecured Firebase databases. Exposed records included plaintext passwords, financial records and other personal information." (Kumar, 2018)

In order to mitigate against MITC, users and enterprises should employ the following cloud security solutions: Database Activity Monitoring (DAM) and File Activity Monitoring (FAM). Database Activity Monitoring tools "capture and record, at a minimum, all Structured Query Language (SQL) activity in real time or near real time, including database administrator activity, across multiple database platforms; and can generate alerts on policy violations." (Mogull, n.d.) This will help users and organizations identify the presence of data leaks and other attacks. In a similar sense, File Activity Monitoring will help these same users identify any possible MITC attacks and prevent the attacker from accessing key private data by monitoring data flows from the cloud. Neither of these solutions are the perfect defense against MITC attacks and users must remain vigilant when protecting personal data and keep a strong defensive mindset when sharing data with any cloud service provider.

In conclusion, the MITC attack is a frightening new attack vector that challenges the current understanding of private data storage on cloud hosting services. This threat has become more prevalent thanks to a growing attack surface as more users continue to synchronize their personal data with cloud storage providers. For now, it may be safer for personal users to avoid data synchronization tools unless they are under the umbrella of larger organization that can monitor data flows with an independent and reliable monitoring tool such as DAM or FAM. For now, users should carefully consider what data they are willing to share with the cloud until the industry has more time to catch up to this sophisticated attack scenario.

References

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). Cloud security is not (just) virtualization security: A short paper. Paper presented at the CCSW '09: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Chicago, Illinois, USA. 97-102

Gupta, R., Prasad, K. H., Luan, L., Rosu, D., & Ward, C. (2009). Multi-dimensional knowledge integration for efficient incident management in a services cloud. Paper presented at the SCC '09: Proceedings of the 2009 IEEE International Conference on Services Computing, 57-64

Kumar,M. (2018,June 21). Thousands of Mobile Apps Expose Their Unprotected Firebase Hosted Databases. Retrieved from https://thehackernews.com/2018/06/mobile-security-firebase-hosting.html

Mogull,R. (n.d.). Understanding and Selecting a Database Activity Monitoring Solution. https://www.securosis.com/assets/library/reports/DAM-Whitepaper-final.pdf

OWASP Cloud -10 Project. (n.d.). Retrieved from https://www.owasp.org/index.php/Category:OWASP\_Cloud\_%E2%80%90\_10\_Project

OWASP Mobile Top 10 -2016 (2016). Retrieved from https://www.owasp.org/index.php/Mobile\_Top\_10\_2016-Top\_10

Reeve, T. (2015, August 6). Man-In-The-Cloud Attacks Can Compromise Enterprise Cloud Storage. Retrieved from https://www.scmagazineuk.com/man-in-the-cloud-attacks-compromise-enterprise-cloud-storage/article/1479016