49th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Mr. Arnoldo Esteban Cervantes García
Pinnacle Aerospace, Mexico, arnoldo.cervantes@sonorasoft.com

REINFORCING CRITICAL AUTHENTICATION SYSTEMS AGAINST UNAUTHORIZED USERS

Abstract

The purpose of this research is to find different ways to strengthen the defenses of the authentication systems used to access to privileged areas where an unauthorized access can be catastrophic, from accessing to confidential information, to remotely controlling some critical piece of hardware. This is necessary because today's computational resources are powerful enough, such that even some inexpensive hardware using a multi-core graphic card can be used to penetrate in an application by brute force or even to provoke a denial of service, just because the authentication system is not taking the necessary measures to minimize those problems and even when this system is following multiple industry standards. Our proposal is to use a behavioral biometrics authentication system, combined with an algorithm to degrade the retry rate after a configurable amount of failed attempts and a slow hashing algorithm. The objective of the biometric authentication system is to add an implicit two factor authentication to improve the security of the account. The algorithm to degrade the retry rate avoids giving unlimited tries in a fixed amount of time to an attacker trying a brute force attack or even a denial of service, since the degraded response time will become a bottleneck against brute force attacks and it will also minimize the risk of a denial of service by sending thousands of login requests per second to abuse of the hashing algorithm's computational cost. Finally, the slow hashing algorithm will make each request slower, since it will take a longer amount of time compared with other fast hashing algorithms (like the SHA family), which will become a bottleneck for a possible attacker trying multiple passwords, but it will be a negligible amount of time for a legitimate user. This research will help to improve the defenses on critical systems where it is crucial that no unauthorized users can access to it.