Developing a Secure Application Programming Interface for Global Navigation Satellite System Authentication

An Application Programming Interface (API) is a set of protocols that enables data transmissions or exchanges between different devices, systems, and applications. The implementation of API allows Global Navigation Satellite System (GNSS) to send GPS data to others after user authentication is done through GNSS signals. However, GNSS technology is vulnerable to various cyber attacks, such as spoofing. GPS spoofing tricks the system into believing the attacker is a legitimate user by sending false GNSS signals and feeding the victim receiver counterfeit information. Spoofing attacks have brought grave consequences in important sectors such as civil aviation, finance, transport, and others in maintaining data integrity [1]. a previous project suggested a method for secure authentication by using a combination of cryptographic hash functions and secret keys shared only by the sender and receiver to generate Keyed-Hashing for Message Authentication Code (HMAC) and the HMAC received by the receiver will use the same cryptographic hash functions and keys to validate the HMAC to verify the sender identity [2]. Using cryptographic hash functions prevents individuals without the secret key from generating a valid HMAC, which makes spoofing harder. However, the hacker can still attack using other spoofing methods.

The cryptographic Hash Function works well against direct spoofing, where the attacker interferes directly with the legitimate signal at a close distance. However, in GNSS, There are other types of spoofing, such as replay spoofing and relay spoofing. Replay spoofing intercepts the GNSS signal and replays it at a different time resulting in navigation errors for the receiver, while relay spoofing intercepts the GNSS signal and transmits it to other intended devices resulting in communication issues. Replay/relay attacks proved their effectiveness against even a cryptographically secured GNSS authentication system [3]. Past research [4], [5] have demonstrated the possibility of real-time long-distance relay/replay spoofing on GNSS signals to be carried out by modifying the content of legitimate messages and retransmitting them as legitimate messages. This project aimed to prevent cyber attacks on GNSS signals. GPS spoofing in civil aviation, finance, and transport sectors could prove fatal. For example, military tasks and search and rescue missions can result in financial and human life losses.

This project explored the idea of using timestamps in HMAC computation because one of the approaches to detect relay/replay spoofing is through time intervals [6]. Timestamps in HMAC rely on time counters that increase depending on the algorithm and will only validate HMACs transmitted within the acceptable time range, in contrast to the previous work [2], which used cryptographic hashing to directly computes and validates HMAC at any given time.

The objective of this project was to develop a secure API Authentication using cryptographically secured GNSS with the implementation of timestamp-based HMAC. This project also hopes to provide an authentication scheme that prevents replay, relay, and direct spoofing. Furthermore, experiments have been conducted to ensure the user receives authentic navigation messages while undergoing direct, relay/replay spoofing attacks.

Citations:

[1] Cheng, X.-jun et al. (2009) “Analysis on forgery patterns for GPS civil spoofing signals,” 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 353–356. Available at: https://doi.org/10.1109/iccit.2009.88.

[2] Chu, Y.H. et al. (2022) “GPS signal authentication using a chameleon hash keychain,” Critical Infrastructure Protection XV, pp. 209–226. Available at: https://doi.org/10.1007/978-3-030-93511-5_10.

[3] Papadimitratos, P. and Jovanovic, A. (2008) “Protection and fundamental vulnerability of GNSS,” 2008 IEEE International Workshop on Satellite and Space Communications, pp. 167–171. Available at: https://doi.org/10.1109/iwssc.2008.4656777.

[4] Psiaki, M.L. and Humphreys, T.E. (2016) “GNSS spoofing and detection,” Proceedings of the IEEE, 104(6), pp. 1258–1270. Available at: https://doi.org/10.1109/jproc.2016.2526658.

[5] Papadimitratos, P. and Jovanovic, A. (2008) “Protection and fundamental vulnerability of GNSS,” 2008 IEEE International Workshop on Satellite and Space Communications, pp. 167–171. Available at: https://doi.org/10.1109/iwssc.2008.4656777.

[6] Haider, Z. and Khalid, S. (2016) “Survey on effective GPS spoofing countermeasures,” 2016 Sixth International Conference on Innovative Computing Technology (INTECH), pp. 573–577. Available at: https://doi.org/10.1109/intech.2016.7845038.