**Developing Secure Application Programming Interface for Global Navigation Satellite System Signal Authentication against Relay/Replay Attack**

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 another device or user. However, GNSS technology is vulnerable to various types of cyber attacks. Cyber attacks in GNSS include jamming and spoofing. GPS spoofing tricks the system into believing the attacker is a legitimate user and feeds the victim receiver counterfeit information. Spoofing attacks may have grave consequences in sectors such as civil aviation, finance, transport, and many more in maintaining data integrity [1]. Previous projects have suggested a method for secure authentication by using a combination of cryptographic hash functions with secret keys shared only by the sender and receiver to validate Keyed-Hashing for Message Authentication Code (HMAC) through signal authentication. Using cryptographic hash functions prevents individuals without the secret key from generating a valid HMAC, which makes spoofing harder [2].

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 involves intercepting the GNSS signal and transmitting it to different intended devices resulting in communication issues. Replay/relay attacks showed the feasibility and effectiveness against even a cryptographically secured GNSS authentication [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 legitimate messages and retransmitting the messages as legitimate messages.

This project aimed to prevent cyber attacks on GPS data that impact finance loss and human life in important sectors such as civil aviation, finance, transport, and tasks such as military defense and search and rescue. 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, which is different from using cryptographic hashing to directly computes and validates HMAC at any given time done in previous work [2].

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 direct and relay/replay spoofing. Furthermore, experiments have been conducted to ensure the user receives authentic genuine 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.