Attribute-based authentication protocol with FaR Hash

Shashank Tripathi
Research and Transfer Centre CyberSec,
Hamburg University of Applied Sciences

36th Crypto Day, 14/15 March 2024

The expanding realm of the Internet of Things (IoT) introduces a unique set of challenges in maintaining secure and reliable communication across a vast network of connected devices. Traditional methods of authentication largely depend on the use of secrets such as passwords and keys. The proposed protocol couples the identities closely with authenticity tokens, designed not to be readable or reversible. This method significantly enhances security by mitigating the risk of table-based attacks through the implementation of k-anonymity Sweeney (2002). Such a strategy allows for the remote creation and verification of tokens at access gateways. These tokens uniquely represent a user's identity and can be verified universally using the corresponding method. This mechanism ensures that only legitimate users can access their accounts.

To ensure k-anonymity FaR hash (Tripathi and Skwarek, 2023) (fuzzyfiable and robust) based design has been employed. It is a type of hash calculated with multiple types of attributes of the subject under consideration. The proposed authentication protocol — FaR-Auth utilizes this property of FaR hash and combines attribute-based key cryptography with challenge-response pairs as behavioural attributes for device authentication. Utilizing discrete logarithmic functions (Odlyzko, 2000), the protocol utilizes attributes such as physically unclonable functions (PUFs) (Herder et al., 2014) or communication packet analysis (Shahid et al., 2018) to authenticate a device. The authentication process involves two main entities: the client and the verifier, which can be decentralized or distributed across multiple systems. The steps include initiating communication upon a trigger and exchanging keys based on behavioural attributes. By making use of discrete mathematical functions, both parties get symmetric keys independently. This approach enhances security by utilizing unique behavioural attributes and supports decentralization.

By utilizing behavioural attributes to generate a FaR hash and then deriving keys from prime numbers identified through the Miller-Rabin primality test (Chaitin and Schwartz, 1990), FarAuth introduces an additional layer of security. The protocol's foundation on the discrete logarithm problem and its use of prime numbers for cryptographic operations place it within a robust theoretical framework of security; especially for the IoT devices which face limitations in computational and storage capabilities. The FarAuth protocol can be useful as it doesn't require storing secrets but rather relies on a device's behaviour. The present work will aim to share the implementation results and future goals.

crypto day matters 36 (2024)
Beiträge vom 36. Kryptotag, 14.-15. MÃ¤rz 2024, Regensburg.
doi:10.18420/cdm-2024-36-03

References

Chaitin, G. J. and Schwartz, J. (1990). A note on monte carlo primality tests and algorithmic information theory. *Pap. Algorithmic Inf. Theory*, 8:197.

Herder, C., Yu, M.-D., Koushanfar, F., and Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141.

Odlyzko, A. (2000). Discrete logarithms: The past and the future. *Towards a Quarter-Century of Public Key Cryptography: A Special Issue of DESIGNS, CODES AND CRYPTOGRAPHY An International Journal. Volume 19, No. 2/3 (2000)*, pages 59–75.

Shahid, M. R., Blanc, G., Zhang, Z., and Debar, H. (2018). Iot devices recognition through network traffic analysis. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 5187–5192.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, 10(05):557–570.

Tripathi, S. and Skwarek, V. (2023). Fuzzified advanced robust hashes for identification of digital and physical objects. *arXiv preprint arXiv:2303.17499*.