The authorization frameworks mentioned above offer no control over permission sequences constraints. In capability-based systems such as ICAP and OAuth, capabilities may carry a list of granted permissions. These permissions do not have any usage constraints. Recent work in [30] presents a capability system (HCAP) that supports history-based access control. Compared to HCAP, our work has several advantages when enforcing a finite permission sequence. First, any communication between resource servers is not required. Second, HCAP uses the timestamp to invalidate the old capability, which requires a synchronized clock. We do not have this assumption in our capability system. Third, HCAP capabilities carry part of the request security automaton (a security automaton specifies the enforceable security policy), and the RS is required to simulate the state transition in the security automaton. Our capabilities carry the finite permission sequence, and the RS simply needs to maintain an internal counter. The lightweight capabilities and fast capability verification pave the way for faster deployment of our capability-based system for ecosystems such as IoT. Finally, the capability in HCAP includes a Message Authentication Code using the shared secret. This security tag is only verifiable by the target resource server. In this work, the signatures in capabilities are public-key-based thus are public-verifiable. It is worth noting that HCAP does not support "context" of access.

9 CONCLUSION

The effectiveness of applying capability-based systems to access control in many domains depends on its ability to enforce complex policies, including orderings among permissions and environmental situations. However, efficient enforcement of these conditions in a distributed capability system is challenging since policy decision and enforcement are carried out in different entities. We motivate this research to provide a capability-based system with the fine-grained delegation of authority and efficient enforcement of conditional constraints.

We described a capability-based system, which supports enforcement of permission sequence and context constraints. Capabilities in our model allow the resource owner to have control over orderings among permissions and specify any external conditions in the policies. Cryptographic means in the capability system provide advanced security features and efficient capability revocation. We formally proved the safety property of the proposed system. We integrated our system with OAuth 2.0 and demonstrated that the performance of our system is competitive. Future work will focus on enforcing the other history-based policies using minimum state. Furthermore, we will consider an honest but curious RS and ensure that the RS can not passively/actively learn more information about the user and their surrounding environment.

10 ACKNOWLEDGEMENTS

This research is in part supported by Natural Sciences and Engineering Research Council of Canada and Telus Communications, under Industrial Research Chair Grant scheme.

REFERENCES

[1] Auth0. jsonwebtoken. https://www.npmjs.com/package/jsonwebtoken. Accessed on Jan 2022.
[2] BeyondTrust. What Is Least Privilege and Why Do You Need It? https://www.beyondtrust.com/blog/entry/what-is-least-privilege. Accessed on Feb 2022.
[3] A. Birgisson, J. G. Politz, U. Erlingsson, A. Taly, M. Vrable, and M. Lentczner. Macaroons: Cookies with contextual caveats for decentralized authorization in the cloud. 2014.
[4] E. Y. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague. OAuth demystified for mobile application developers. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 892–903. ACM, 2014.
[5] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari. IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. *IEEE Sensors Journal*, 15(2):1224–1234, 2015.
[6] D. Clarke, J.-E. Elien, C. Ellison, M. Fredette, A. Morcos, and R. L. Rivest. Certificate chain discovery in SPKI/SDSI. *Journal of Computer security*, 9(4):285–322, 2001.
[7] J. B. Dennis and E. C. Van Horn. Programming semantics for multiprogrammed computations. *Communications of the ACM*, 9(3):143–155, 1966.
[8] D. Fett, R. Küsters, and G. Schmitz. A comprehensive formal security analysis of OAuth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1204–1215, 2016.
[9] L. Gong. A secure identity-based capability system. In *Proceedings. 1989 IEEE Symposium on Security and Privacy*, pages 56–63. IEEE, 1989.
[10] S. Gusmeroli, S. Piccione, and D. Rotondi. A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, 58(5-6):1189–1205, 2013.
[11] D. Hardt. The OAuth 2.0 authorization framework. https://tools.ietf.org/html/rfc6749, 2012.
[12] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, et al. Guide to attribute based access control (ABAC) definition and considerations (draft). *NIST special publication*, 800(162), 2013.
[13] M. Jafari. Using JSON to Model Complex OAuth Scopes. https://medium.com/@jafarim/using-json-to-model-complex-oauth-scopes-fa8a054b2a28. Accessed on Jan 2022.
[14] M. Jones, P. Tarjan, Y. Goland, N. Sakimura, J. Bradley, J. Panzer, and D. Balfanz. JSON Web Token (JWT). https://tools.ietf.org/html/rfc7519, 2012.
[15] S. P. Kaluvuri, A. I. Egner, J. Den Hartog, and N. Zannone. SAFAX–an extensible authorization service for cloud environments. *Frontiers in ICT*, 2:9, 2015.
[16] A. Labs. The Untold Story of the Target Attack Step by Step. https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf. Accessed on Feb 2022.
[17] L. Lamport. Proving the correctness of multiprocess programs. *IEEE transactions on software engineering*, (2):125–143, 1977.
[18] S. Li. A Capability-based System to Enforce Context-aware Permission Sequence. Master's thesis, Science, 2020.
[19] T. Lodderstedt. Transaction Authorization or why we need to re-think OAuth scopes. https://medium.com/oauth-2/transaction-authorization-or-why-we-need-to-re-think-oauth-scopes-2326e2038948. Accessed on Jan 2022.
[20] E. Maler, D. Catalano, M. Machulak, and T. Hardjono. User-managed access (UMA) profile of OAuth 2.0. https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html, 2018.
[21] J. Mott. Crypto-js. https://code.google.com/archive/p/crypto-js. Accessed on Jan 2022.
[22] H. Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.
[23] S. Ravidas, P. Karkhanis, Y. Dajsuren, and N. Zannone. An authorization framework for cooperative intelligent transport systems. In *International Workshop on Emerging Technologies for Authorization and Authentication*, pages 16–34. Springer, 2019.
[24] R. Schuster, V. Shmatikov, and E. Tromer. Situational Access Control in the Internet of Things. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1056–1073. ACM, 2018.
[25] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi. OAuth-IoT: An access control framework for the Internet of Things based on open standards. In *2017 IEEE Symposium on Computers and Communications (ISCC)*, pages 676–681. IEEE, 2017.
[26] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig. Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth). https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-27, 2019. IETF Internet Draft. Accessed on Nov 2021.
[27] M. Shehab and F. Mohsen. Towards enhancing the security of OAuth implementations in smart phones. In *2014 IEEE International Conference on Mobile Services*, pages 39–46. IEEE, 2014.
[28] M. Suárez-Albela, P. Fraga-Lamas, and T. Fernández-Caramés. A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices. *Sensors*, 18(11):3868, 2018.
[29] S.-T. Sun and K. Beznosov. The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 378–390, 2012.
[30] L. Tandon, P. W. Fong, and R. Safavi-Naini. HCAP: A History-Based Capability System for IoT Devices. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, pages 247–258. ACM, 2018.