Enabling User Control in IoT Device Traffic Management through Enhanced Open-Source MUD Manager Interface

Louis Hatton
University of York
lwh506@york.ac.uk

Poonam Yadav
University of York
poonam.yadav@york.ac.uk

Abstract

The Manufacturer Usage Description (MUD) [1] standard introduces a clear approach to enforcement of Internet of Things (IoT) device network traffic. It requires manufacturers to define the network behavior of their IoT devices within a MUD file, which is a JSON encoded YANG model containing access control lists (ACLs). These rules can be enforced at the network level by a network administrator or MUD manager to limit a device's network activities to the provided requirements. This allows the IoT devices to function normally without providing them unrestricted network access therefore introducing greater privacy and control over devices. In addition, when using a MUD manager this enforcement process is automatic and reduces the effort needed to secure IoT devices [2] especially in larger networks. However, for an end user it's difficult to understand or view the current state of the system with MUD files alone [3]. Furthermore, as MUD policies are defined by the manufacturers, the network requirements of the device may not match the policies or rules in place for the network they are connected to. Currently, users have no control over the policies being applied and have no way to override them without technical and complex changes. This application solves these problems. As an expansion to osMUD, an open-source MUD manager [4], the application adds a user interface and user policy manager to give users more control over which MUD policies are being enforced and for which device on the network. By connecting to the database which osMUD updates, the user can see a live view of the system with a list of all the devices currently being tracked by osMUD and interact with the individual MUD files attached to them. The user interface provides the user the ability to easily remove any policies as required to create a custom user defined policy. These user policies are handled by the user policy manager and sent directly to osMUD to be enforced on the network automatically. The application runs alongside osMUD with little changes required making it easy to install into a new or already existing MUD enforced network. In ad-

dition, the ability for quick iterations and changes to MUD files makes using and interacting with MUD easier for users which lowers the barrier to entry to running a MUD enforced network. This application is in an early-stage of development with new features, including automatically creating MUD files PCAPs and managing MUD file history per device, planned for the future.

References

[1] Eliot Lear, Ralph Droms, and Dan Romascanu. *Manufacturer Usage Description Specification*. RFC 8520. Mar. 2019. DOI: 10.17487/RFC8520. URL: https://www.rfc-editor.org/info/rfc8520.

[2] Ayyoob Hamza et al. "Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles". In: *Proceedings of the 2018 Workshop on IoT Security and Privacy*. IoT SP '18. Budapest, Hungary: Association for Computing Machinery, 2018, pp. 8–14. ISBN: 9781450359054. DOI: 10.1145/3229565.3229566. URL: https://doi.org/10.1145/3229565.3229566.

[3] Vafa Andalibi et al. "Is Visualization Enough? Evaluating the Efficacy of MUD-Visualizer in Enabling Ease of Deployment for Manufacturer Usage Description (MUD)". In: *Proceedings of the 37th Annual Computer Security Applications Conference*. ACSAC '21. ¡conf-loc¿, ¡city¿Virtual Event¡/city¿, ¡country¿USA¡/country¿, ¡/conf-loc¿: Association for Computing Machinery, 2021, pp. 337–348. ISBN: 9781450385794. DOI: 10.1145/3485832.3485879. URL: https://doi.org/10.1145/3485832.3485879.

[4] osmud.org. *Open Source MUD Manager*. URL: https://osmud.org/.