Media Operations Use Case for an Augmented Reality Application on Edge Computing Infrastructure

draft-ietf-mops-ar-use-case-13

Renan Krishna, Akbar Rahman

MOPS WG IETF 118 Prague November 2023

Draft's Table of Contents

Section 6 has been added

Table of Contents

New Update

Section 6 : Security Considerations

Many Thanks for Stephan Wenger for shepherding this document!

Communication from Stephan:
"For formal reasons, you will also need a section "Security Considerations". That one is harder, as ***you (and the WG) are expected to think about security even for an informational document covering ops aspects.****"*

In Section 6, , we briefly present the operational security considerations of our use case. A more detailed analysis of these considerations can be found in the references.
There are two dimensions of the operational security to deploy the presented use case:
(i) XR-device related operational security issues and
(ii) Edge server related operational security issues.

Section 6.1 XR-device related operational security issues

- The XR devices could be stolen or tampered with and so the operator of the use case should not rely on the integrity of these devices [DIST].
- The XR devices are already running computationally intensive tasks that drain battery power and so the operator must carefully select an appropriate cryptographic system for communication that takes these issues into consideration.
- Finally, the operator must avoid deploying security protocols that rely on the XR devices being continuously connected to the edge server.

Section 6.2 Edge Server related operational security issues

- The operational security considerations for Edge server of the presented use case are **similar to those for cloud data centres**. The National Institute of Standards and Technology (NIST) [NIST1] details the operational issues of security for such data centres. The edge servers in the presented use case run as a private cloud of the operator. **Operators will need to consider physical security of the servers, disks, routers, cables, power etc**.
- Additionally, the XR software being deployed for the use case will need to be **audited for software error categories** [CWE] such as insecure interaction between components, risky resource management, and porous defences.
- Finally, **security maintenance** of the XR system running on the edge servers will require [NIST2] monitoring and analysing logging information, performing regular back-ups, recovering from security compromises, regular testing of system security and using processes to patch and update all critical software, and to monitor and revise the configuration as needed.

Comments and Suggestions are invited!

References

[CWE] "CWE/SANS TOP 25 Most Dangerous Software Errorss", Common Weakness Enumeration, SANS Institute, 2012.

[DIST] Coulouris, G., Dollimore, J., Kindberg, T., and G. Blair, "Distributed Systems: Concepts and Design", Addison Wesley, 2011.

[NIST1] "NIST SP 800-146: Cloud Computing Synopsis and Recommendations", National Institute of Standards and Technology, US Department of Commerce, 2012.

[NIST2] "NIST SP 800-123: Guide to General Server Security", National Institute of Standards and Technology, US Department of Commerce, 2008.