IoTA: IoT Assurance (Host 2017 Hardware Demo Submission)

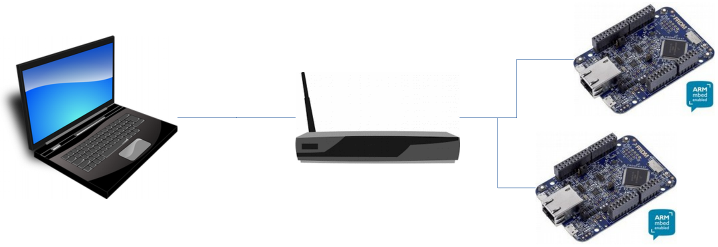
John Clemens (JHU/APL), Raj Pal (DoD), Branden Sherrell (JHU/APL)

Research Summary

Cyber-physical interactions driven by data are increasingly important in today's hyper-connected world. Given that, it is imperative that mechanisms for collecting the data are trusted. However, first line data collectors often use constrained platforms that lack the resources for traditional integrity assessment.

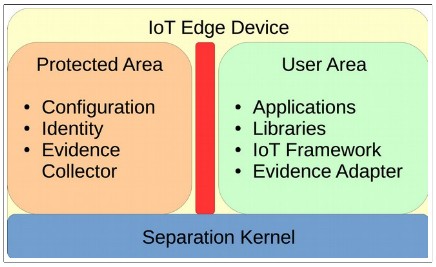
JHU/APL and DoD are researching ways to bring trustworthy Measurement and Attestation (M&A) to resource-constrained devices. Previous research [1][2] enumerated the set of properties necessary for any framework making integrity assessments of individual systems. However, implementing these properties can be expensive in both time and computational resources. We have developed a prototype framework for trustworthy M&A on constrained platforms, and will demonstrate evidence collection and evaluation using multiple measurement collectors within the constraints of a modern IoT system. This includes discussion of the overhead incurred to the original application and trade-offs necessary to implement the demonstration. This is a continuation and demonstration of the research briefly presented in [3].

Demonstration



The demonstration will consist of at least two FRDM-K64F development boards running ARM's mBedOS, a modified version of the ARM uVisor separation kernel, an example first-line data collection application, and the endpoint portion of our prototype M&A framework. The example application communicates with a laptop computer which both consumes the example data and provides the M&A server. The M&A server includes a web interface allowing the user to request an integrity evaluation of any of the currently connected devices. The user can watch in real time as the following steps occur: 1) the framework establishes a secure connection to the device to be measured, 2) the device generates evidence from at least two different collectors pre-installed on the device, and 3) the collected evidence is evaluated by the server.

Both success and failure cases will be demonstrated. The user can also observe the (lack of) impact on the primary application on the device. The accompanying poster will display measurements of code size and time overhead for the measurement, as well as the general architecture of the framework, implementation trade-offs, and future research directions.



References

[1] Coker, G., Guttman, J., Loscocco, P., Sheehy, J., & Sniffen, B. (2008, October). Attestation: Evidence and trust. In *International Conference on Information and Communications Security* (pp. 1-18). Springer Berlin Heidelberg.

[2] Loscocco, P. A., Wilson, P. W., Pendergrass, J. A., & McDonell, C. D. (2007, November). Linux kernel integrity measurement using contextual inspection. In *Proceedings of the 2007 ACM workshop on Scalable trusted computing* (pp. 21-29). ACM.

[3] Clemens, J., Pal, R., & Philip, P. (2016, October). Extending Trust and Attestation to the Edge. In *Edge Computing (SEC), IEEE/ACM Symposium on* (pp. 101-102). IEEE.