Towards a Secure Cyberspace through Developing Security Safe-guards for IoT Devices

Moosa Yahyazadeh

Contact information: B1C MLH, The University of Iowa, Iowa City, IA 52242. moosa-yahyazadeh@uiowa.edu (✉)

Motivation & Problem Definition: IoT devices are pervasive and their popularity is on the rise. They are connected to each other for several benefits and can be readily accessed from the local network or managed through the Internet. These devices can directly communicate with each other (and they can also use a hub, as a base station,) to build the entire network using some underlying protocols like CoAP. Over the last few years, it can be seen that attackers have a tendency to target IoT devices for information leakage [2] [3] or using them in the subsequent attacks [1]. Given the circumstance that IoT devices often are placed in the proximity of its users, the consequence of IoT security vulnerabilities is often severe. Since these constrained nodes are usually low-power and low-resource, most of the times it is not possible for them to employ a full-fledged security solution and they usually prefer the functionality to the security. Therefore, manufactures prefer to use some open-source implementations of the protocols like CoAP or utilize some customized protocol adapted to work in the constrained environment. The open-source implementations often lack of comprehensive security analysis and are prone to some major vulnerabilities due to the fact that most of the time the specifications are stated in natural language and thus they could be either overestimated or underestimated. Therefore, wrong protocol design and implementation is a major problem in the IoT and can be considered as a significant source of threat in the network.

Approach, Objective, and Expected Results: IoT devices often exchanges some sensitive data and one needs to make sure the underling data protocol is secure. In this proposal, we will address wrong protocol design and implementation by tackling the problem through two main steps: (A) Security analysis of the protocol specification. In this step, we will show whether the properties in the CoAP specification is consistent and it will behave as it is expected. The consistency check is performed to show whether the properties of the protocol throughout its life-cycle are maintained based on the obliged requirements. To this end, we will leverage formal verification techniques (*e.g.*, model checking, SMT solvers) to prove the properties of the specification is consistent. (B) Security analysis of some implementations of the CoAP and MQTT protocols. The main goal of the step is that whether the implementations follow exactly what are stated in the specification. In the step we will be exploring the semantic bugs in the implementations in which (i) appropriate reactions cannot be taken place accordingly when a packet is received or (ii) the types of relevant packets cannot be recognized. The analysis will be done using software engineering techniques (*e.g.*, black box fuzzing, symbolic execution, differential testing) to carry out an in-depth security analysis of commonly used network protocols and find security relevant bugs.

References

[1] Chinese manufacturer recalls iot gear following dyn ddos. https://threatpost.com/chinese-manufacturer-recalls-iot-gear-following-dyn-ddos/121496/.

[2] Serious security flaws found in osram smart bulbs. http://www.zdnet.com/article/serious-security-flaws-found-in-osram-smart-bulbs/.

[3] Watch out, new parents—internet-connected baby monitors are easy to hack. http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/.