Proposal Title

Towards a Secure Cyberspace through the Development of Security Safe-guards for IoT Devices

Introduction and Motivation

We are living in a place surrounded by a lot of information generated by sensors and appliances that we are dealing with in every day and the Internet of things (IoT) is meant to be connect those devices to each other for several benefits. So, they can be readily accessed from the local network or managed through the Internet. These devices can also communicate to each other (and of course to a hub, as a base station,) to build the entire home network and one of the most popular protocol specialized for using in the constrained nodes and networks (which are usually low-power, low-resource with high-potential to packet loss) is the Constrained Application Protocol (CoAP). Over the last few years, it can be seen that attackers have a tendency to aim IoT devices for information leakage or using them in the subsequent attacks. Here are some major attacks reported:

- Chinese DDOS attack based on IoT devices [1]
- Smart bulb vulnerability [2]
- Baby monitors hacked [3]

Problem

Basically, we have identified that there could be three potential source of threads to the network from the communication perspective.

1. **Secure Bootstrapping**
   For the first time setup the nodes in the network, they should be able to agree on some configuration that they want to use for the further communications, like sharing the common key for encrypting their connection. But with respect to the fact the nodes are resource-constrained, they usually can not efficiently perform the task and thus try to use some simple approaches like hard-coding the key and possibly share it in plain text for the initialization purpose.

2. **Wrong protocol design and implementation**
   There could be some security issues to the communication between the nodes in the network because they usually use some open-source implementations of CoAP or other CoAP-based protocol that may not conform the protocol specifications. The indoor communications are also very important because they can be still threated by nearby attacker to for example breach the smart lock and trespass to a house.

3. **Unauthorized Access to IoT devices**
   This is stem from the fact that these are limited resources devices and implementing full–fledged authentication system may not be feasible. Hence, the gateway should employ some technique to recognize an unauthorized access and then filter out from the network.

Approach

In this proposal, we will address problems (1) and (2). We will tackle problem (1) through two steps: (A) We will leverage formal verification techniques (e.g., model checking, satisfiability modulo theory solvers) and software engineering techniques (e.g., black box fuzzing, symbolic execution) to carry out an in-depth security analysis of commonly used network protocols (e.g., CoAP) and find security relevant bugs. (B) Based on the respective RFC standards, develop formally verified reference implementation of few of these network protocols, CoAP being the principal one. One insight is that the properties we are interested in proving are safety properties which is much simpler to handle than its liveness counterpart. We plan to carry out a modular verification based on the assume-guarantee paradigm where we will write function contracts for each function. We will then use tools such as Boogie, Dafny to first ensure that each function indeed satisfies its contract based on the assumption on the input. Once each such function has been verified to satisfy their contracts, we will try to prove the global properties.

Approaching problem (2) will be divided into two steps: (1) Evaluation of existing bootstrapping and authentication techniques; (2) Based on the finding, design and implement a new bootstrapping protocol with formally verified security assurance. For proving the security assurance of these protocols we plan to leverage current technologies including ProVerif, Cryptol, etc.

Challenges

Challenges in Problem (1)

- Written in system level language like C/C++ which are known to be difficult to verify and test.
- Protocol specification is written in natural languages which could be both under-specified and ambiguous.
- Reference implementation has to be platform-agnostic (e.g., network stack).

Challenges in Problem (2)

- Reasoning about protocols with cryptographic primitives in the computational model is significantly harder than in the symbolic model.
- Developing a framework for evaluating different bootstrapping protocols uniformly is a difficult problem.

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/.