Automated IoT Security

Oscar Garcia-Morchon[1] and Thorsten Dahm[2]

[1] Philips, oscar.garcia-morchon@philips.com
[2] Google, thorstendlux@google.com

The Internet of Things allows for human-to-thing and thing-to-thing communication by using standard Internet protocols. The security needs are well-recognized but the design space of IoT applications and systems – smart homes, smart buildings, critical infrastructure, connected healthcare – is complex and exposed to multiple types of threats. In particular, threats keep evolving at a fast pace while many IoT systems are rarely updated and still remain operational for decades.

When devices are deployed in a given environment, vulnerable devices can endanger the privacy of the users, the overall system where they are deployed, or even the whole Internet. For instance, a smart vacuum cleaner can forward video recordings in the house; hacked smart meters can force a smart power-grid to collapse; or hacked IP cameras can launch a DDoS attack. The problem is the limited integration of security processes in the device lifecycle. When a manufacturer makes a security design, the manufacturer does not know whether his security assumptions and designs will hold in all deployment scenarios; users often buy devices but they do not know whether they are secure or how they can be secured; system integrators have to operate devices from many multiple vendors with heterogeneous security.

The solution that we envision [1] is a comprehensive agile security framework to integrate existing security processes such as business impact analysis (BIA), risk assessment (RA), privacy impact assessment (PIA) or vulnerability assessment (VA) in the lifecycle of a smart object in an IoT application (see Figure 1). So instead of making risk or privacy assessments beforehand, we want to do them at deployment to adjust security settings to the specific environment; and keep doing them next to vulnerability assessment throughout the device lifecycle.

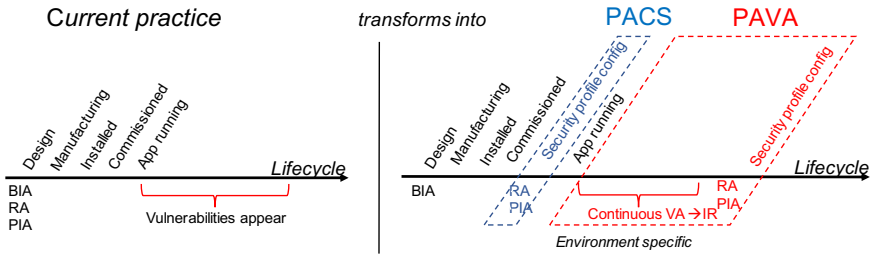

Fig. 1. Security processes integrated in the IoT device lifecycle.

As shown in Figure 2, the core of our agile security approach relies on two protocols: the Protocol for Automatic Security Configuration (PASC) and the Protocol for Automatic Vulnerability Assessment (PAVA). PASC is executed during the onboarding phase of a smart object in an IoT system and is in charge of automatically performing a risk assessment and assigning a security configuration – applicable to the device or the system – to defeat the identified risks. The assigned security configuration fits the specific environment and threat model of the application in which the device has been deployed. A simple way of doing this is by having the infrastructure learn the resources (e.g., communication patterns) required by the devices and limiting devices accesses to those resources. This can be realized by means of MUD files and a Software Defined Network architecture. PAVA is executed during the operation of the IoT object and ensures that vulnerabilities in the smart object and IoT system are discovered in a proactive way. This can be done by performing active tests in the deployed system and blocking any actions that go beyond the normal pattern agreed at deployment time.

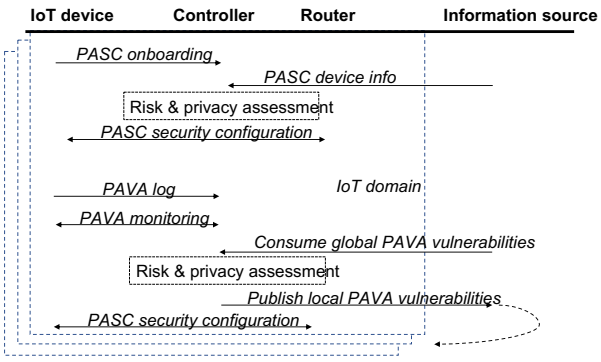

Fig. 2. PASC and PAVA Protocol Interactions.

Our architecture and protocols can simplify security work of manufacturers; empower users to secure their devices; and simplify the way system integrators operate large IoT systems. While PACS and PAVA work locally, events detected locally can also be published so that vulnerability information is globally available. A proof of concept of this architecture is DAQ [2].

References

1. Oscar Garcia-Morchon and Thorsten Dahm. *Internet Draft - Automated IoT Security.* `https://datatracker.ietf.org/doc/draft-garciamorchon-t2trg-automated-iot-security/` IRTF T2TRG, 2018.
2. `https://github.com/faucetsdn/daq`