



**Securing the Internet of Things with  
Security-by-Contract**

av

**Alberto Giarretta**

**Akademisk avhandling**

Avhandling för filosofie doktorsexamen i datavetenskap,  
som kommer att försvaras offentligt  
Fredag den 29 januari 2021 kl. 13.00,  
Hörsal L2, Örebro universitet/Universitetssjukhuset Örebro

Opponent: Docent Shahid Raza  
RISE Research Institutes of Sweden och  
Uppsala Universitet, Sverige

Örebro universitet  
Institutionen för naturvetenskap och teknik  
701 82 ÖREBRO

# Abstract

Alberto Giarretta (2021): Securing the Internet of Things with Security-by-Contract  
Örebro Studies in Technology 90.

Smart homes, industry, healthcare, robotics; virtually every market has seen the uprising of Internet of Things (IoT) devices with different degrees and nuances. IoT devices embody different desirable characteristics, such as mobility, ubiquity, variety, and affordability. All combined, these features made so that IoT devices reached 35 billion units in the world. However, the sudden uprising of market demand put enormous pressure on manufacturers. The necessity of delivering to customers as many devices as possible, in the shortest time possible, leads manufacturers to overlook features that are not perceived critical by the users, such as resiliency to cyberattacks. This led to severe security issues. The prime example is Mirai, a malware that infected hundreds of thousands of IoT devices in 2016 and used them to strike lethal Distributed Denial of Service (DDoS) attacks.

In the first part of this thesis, we present the state of the art regarding IoT devices security resilience. In particular, we provide relevant examples of breaches, an analysis of the relationship between IoT and Cloud from a security point of view, and an example of an IoT device penetration test. Then, we focus on the usage of IoT devices in DDoS-enabled botnets and we provide an extensive study of DDoS-enabling malwares, discussing their evolution and their capabilities.

In the second part, we contextualise the gathered knowledge and we show that the highlighted problems stem from two main causes: insecure configurations and insufficient secure configurability. We also show that, to address these two issues, it is necessary to equip IoT devices with precise and formal descriptions of their behaviour. Therefore, we propose  $S \times C4IoT$ , a security framework for IoT devices that combines Security-by-Contract ( $S \times C$ ) paradigm and Fog Computing paradigm. First, we provide a thorough breakdown of our proposal. We start from high-level lifecycles that describe how devices participate to  $S \times C4IoT$ . Then, we discuss the pillars that compose the framework (e.g., security contracts and security policies), together with their formal descriptions. Last, we provide precise algorithms for achieving security-policy matching capabilities, as well as routines for allowing the framework to deal with dynamic changes while maintaining consistency.