LONDON METROPOLITAN UNIVERSITY

A framework for lightweight polymorphic security system for IoT devices

Dion Mariyanayagam, Pancham Shukla, Bal Virdee

Abstract:

One of the many things COVID-19 has taught humanity is that the internet is not just a commodity but a vital service integral to the modern world. As we become ever more connected, there is a growing need to secure data and communication streams. If data is valued, then it should be protected. Some of the least secure devices in modern electronic systems are the Internet of Things (IoT) devices – partly due to their low processing power and always-on functionality.

We find IoT devices in many sectors such as commercial, consumer, government and military and large-scale industry. The key question is how we can protect such a diverse range of IoT devices with a multitude of footprints, functional characteristics and vulnerabilities.

Polymorphism is the notion of changing one's form. In biological organisms, polymorphic (mutating or changing) viruses trick the natural security mechanisms by changing their unique signatures (e.g. DNA or proteins). In computing, antivirus software systems are adapted to detect and remove constantly changing software viruses. However, polymorphism at the firmware level and over the wireless medium is neither well understood nor explored for IoT devices.

This paper proposes a novel and bio-inspired framework for securing distributed IoT

devices often assumed to be working at the intersection of engineering, computing, and cybersecurity domains. The proposed framework attempts to exploit the notion of polymorphism in resource-constrained (e.g., memory, power, bandwidth) IoT devices. The system's core aim is to detect, reject, and block foreign agents individually or collaboratively and in real-time within a client and server model by changing the access credentials and encryption keys as soon as an unauthorised client is detected. The framework proposed for the light-weight polymorphic security system for IoT devices is designed to remain operationally compartmentalised, functionally integrated, and objectively unified.