IoTs Localization, Hardware Security and Trust: Threats, Countermeasures, and Design Tools

Itamar Levi and Yiftach Richter

The proliferation of Internet of Things (IoT) devices brings both benefits and hidden risks. IoT localization and hardware security have become critical concerns in the last decade as technology has become more interconnected, globally integrated and embedded around/over/inside us. With the rise of wireless devices, radio-enabled systems such as smartphones, tablets and drones, the need for accurate device localization has become increasingly important. However, this has also opened up new avenues for security attacks, with computing hardware now a vulnerable target for malicious actors. Attackers can exploit hardware weaknesses to obtain sensitive information, compromise system root-of-trust, steal intellectual property, and manipulate machine learning algorithms. Security professionals have been working hard to develop effective protection techniques and design tools to detect hardware vulnerabilities and strengthen hardware security. With ongoing efforts to improve hardware security, the industry can continue to innovate while ensuring that computing devices remain safe and secure.