CHIST-ERA Call 2015

Project: COCOON

Coordinator: University of Reading

Participants: Dr. Etienne B. Roesch (University of Reading), Dr. George Loukas (Unoiversity of Greenwich), Prof. dr. Thomas Gross (ETH Zurich), Dr. Johnny Fontaine (Ghent University), Dr. Antal Haans (TU/e)

Summary:

In Cocoon, we interweave innovations in two distinctly different disciplines to understand and improve security of home IoT technology: emotion psychology and cyber security. We produce an understanding of the psychology of IoT users, assess risks in current and future IoT systems, and formulate provisions for the design and integration of user-centric IoT in tomorrow's homes. Home is a safe haven to experience privacy and control, personal autonomy and integrity. IoT technology is expected to merge physical and virtual worlds, creating smart home environments that enhance wellbeing. As the physical and the virtual grow closer, concerns for security, privacy and trust grow in similar measures. Addressing these concerns requires technological dispositions and interventions aligned with the individuals. Our objectives are twofold: 1) To examine the emotional investment of IoT users in the comfort of their home, which will condition their usage technology, drive their reactions when security is breached, and will determine their ability to recover. Large-scale qualitative and quantitative studies, and a four-month experiment conducted in 20 volunteering households will not only yield the first comprehensive theoretical framework of the emotional status of IoT users in cases of both normal usage and when their smart home is compromised, but will also inform the development of a novel intrusion detection system (IDS) by recasting the user as an integral part of the system. 2) To put mainstream off-the-shelf IoT technology to the test, and derive empirical opportunities for creating IDS and data security visualization that are appropriate for given occupants' profiles, based on real-time analytics of data from such a heterogeneous set of technologies. Intrusion experiments in self-contained laboratory environments will permit the examination of the effects in a typical smart home. The IDS will be based on real-time big data stream mining classification techniques tailored for resource-constrained IoT environments.