JEREMY WATSON, UNIVERSITY COLLEGE LONDON
EMIL LUPU, IMPERIAL COLLEGE

PETRAS – CYBER SECURITY OF THE INTERNET OF THINGS

A research hub to fill knowledge gaps and promote safe and secure use of the Internet of Things

At the beginning of 2016, the PETRAS Hub consortium of nine leading UK universities was awarded £9.8m by the Engineering and Physical Science Research Council (EPSRC). PETRAS brings the universities together with around 50 user partners representing both the private and public sectors.

STRATEGIC REVIEW OF IOT

Following a strategic review by the UK Government, *'The Internet of Things: making the most of the Second Digital Revolution'* was published in 2014. It emphasised the economic importance of the Internet of Things (IoT), which would only be realised by ensuring its cyber security and trustworthiness while not standing in the way of vibrant technical and business development. The government response was to create the £40m IoTUK initiative, which funds the PETRAS hub amongst other initiatives.

PRINCIPLES OF THE PETRAS HUB

The review highlighted a knowledge and capability gap in the ability to look at IoT (or indeed other) cyber security from an integrated socio-technical viewpoint. Collaborative thinking across social and physical science disciplines was needed from project identification to execution. This principle has guided the vision for PETRAS.

PETRAS stands for Privacy, Ethics, Trust, Reliability, Acceptability and Security – headings that have relevance to both technical and social science. They are all important in ensuring the successful adoption of the Internet of Things. The PETRAS hub is founded on these six themes, and emphasises in equal measure, the physical and social science aspects of the adoption of new IoT technology. The academic partners are made up of a cross-disciplinary Hub team of UCL, Imperial College, Oxford, Leicester and Warwick, augmented by four Spoke contributors at Surrey, Southampton, Cardiff and Edinburgh, who provide specialist contributions. Additionally, PETRAS boasts a large cohort of user and research partners in the private sector (ranging across banking, through healthcare to mobile telecommunications), the public and NGO sectors. 'Impact Champions' working in the PETRAS management team ensure good bidirectional connections between these and the academic partners.

PLANNED PROJECTS

In order to best represent and investigate the opportunities and challenges of the wide span of IoT applications, the partners have created a project structure which feeds into the generic themes of interest; Privacy & Trust, Safety & Security, Harnessing Economic Value, Standards, Governance & Public Policy, and Adoption & Acceptability. A number of projects will provide evidence under these headings; these we have grouped by type or sector into areas of applications or 'Constellations'. Around 20 initial projects cover the constellation themes. PETRAS has been designed so that further internal calls for projects can be shaped to fill the research gaps identified with user partners and then consolidate the research outcomes into concrete demonstrators. PETRAS plans to become the go-to place for research in cyber security of the IoT in the UK by creating an inclusive technical and social platform for innovation that will continue beyond the end of the funded period.

Examples of projects within these constellations include: **Transport & Mobility** where projects will include smart street planning, pricing and road maintenance, and security and privacy solutions for communicating autonomous and semi-autonomous cars and infrastructures. The **Health & Care** constellation will include modelling and analysis for body sensor networks, security mechanisms for miniaturised low power chips, and an investigation of the factors of user trust in medical applications of IoT. **Design & Behaviour** explores the role Design plays in influencing the adoption of IoT. In particular, how Design and Engineering can actively encourage or discourage behaviours, so that Privacy and Trust are enhanced and adoption is promoted. Projects under the **Infrastructure** heading look, from a policy angle, at approaches in various countries and across borders to manage IoT threats and increased attack surfaces. These projects include tools to analyse threats in many contexts. **Identification** constellation projects deal with the trustworthiness of identification systems and evaluating identification technologies, protocols, and procedures alongside privacy strategies, to identify robust solutions that deliver a balance between identifiability and privacy of IoT technology. **Supply & Control Systems** projects cover secure IoT-augmented control systems for industry and buildings, and exploring the economic value of IoT data in cyber physical supply chains. The **Ambient Environments** constellation investigates the impact of security on adaptability within cross-layered network wide protocols for low powered IoT devices. A combination of 'In the Wild' experiments on the Olympic Park and focus groups will explore the boundaries of privacy, trust and personalisation.

Further information can be found on the PETRAS web-site: www.petrashub.org