Innovate UK

Results of Competition: Demonstrators Addressing Cyber Security Challenges in the Internet of Things

Competition Code: 1901_SDTAP_CRD

Total available funding is £6,000,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
CISCO INTERNATIONAL LIMITED	i-TRACE - IoT Transport Assured for Critical Environments	£997,570	£498,785
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY		£275,062	£137,531
NORTHUMBRIAN WATER LIMITED		£395,383	£197,692
SENSEON TECH LTD		£346,382	£242,467
University of Warwick		£520,804	£520,804

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Funders Panel Date: 08/07/2019

Project description - provided by applicants
i-TRACE innovates through the use of an ML and blockchain-based cybersecurity approach using enhanced gateways for IoT. It will tackle the challenge of securing constrained devices highly prevalent in IoT particularly in distributed and dispersed networks (utilities, transport, smart city etc). While reducing power use and enabling 'fit and forget' deployment these devices then lack the capacity to use typical security techniques such as signature-based approaches. i-TRACE will implement an approach that introduces a device authentication/authorization mechanism. The gateway router will be able to regularly determine the identity of the devices and detect tampered devices. If a hacker introduces a malware/virus which might potentially corrupt the data which the sensor is sending to the GW router, it would be able to detect the device has been compromised. The data sent from the device will also be secured by using fairly lightweight encryption algorithm. The data will then make its way to the cloud server and be signed with a blockchain and stored in the secure data lake along with the provenance metadata. The end user will be able to read and detect the authenticity of the data whenever it needs by crosschecking the messages with the blockchain to obtain the ground truth. Since blockchain is immutable and tamper-proof, it is secure in principle and cannot be altered. This data will also be analysed by a ML system to run state-of-the-art threat analysis algorithms. This will identify & prioritise anomalies/outliers for action by security analysts. i-TRACE will demonstrate its approach in a high social impact sector: the water industry. London is in the top 10 cities in the world most at risk of running out of freshwater. Our current use is 150 litres per person per day; to be sustainable, we need to reduce this to 118 litres. A third of this saving needs to come from more efficient use -- reducing consumption -- but while reducing the cost of water for households. i-TRACE will demonstrate its approach to enable a secure yet low-cost, long-life approach to smart water meters. This in turn will enable approaches to household behaviour change. The i-TRACE Partnership includes relevant cross sector expertise to enable successful innovation delivery. Partners include: Cisco International Limited | Northumbrian Water Limited | BT plc | Senseon Tech Ltd | University of Warwick (Warwick Manufacturing Group).

Innovate UK

Results of Competition: Demonstrators Addressing Cyber Security Challenges in the Internet of Things

Competition Code: 1901_SDTAP_CRD

Total available funding is £6,000,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
ULTRASOC TECHNOLOGIES LIMITED	The world's first on-chip and in-life monitoring solution to rapidly detect cyber security threats in Connected and Autonomous Vehicles (CAVs)	£1,960,362	£1,313,443
COPPER HORSE LIMITED		£249,804	£167,369
Coventry University		£298,077	£298,077
University of Southampton		£159,995	£159,995

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Connected and Autonomous Vehicles (CAVs), as part of the **Internet of Things** **(IoT), represent a major cyber security challenge.** In 2015, Charlie Miller, a security researcher at Twitter, and Chris Valasek, director of Vehicle Security Research at IOActive, exposed the security vulnerabilities in automobiles by hacking into a Fiat-Chrysler Jeep Cherokee remotely, controlling the cars' various controls from the radio volume to the brakes and steering wheel. Since then, nearly all OEMs have suffered similar cyber-attacks. **The socio-economic impacts of** **cyber security attacks** **are tremendous, with** **the automotive industry estimated to lose £26 billion annually** **by 2023 \[Upstream Security\].** Systems-on-chip (SoCs) integrate all computing components that power today's CAVs operating within a digitally connected societal framework via the Internet of Things (IoT). A clear market need exists to monitor SoCs 'in-life' (i.e. in an operating environment rather than in the lab), and this is further mandated by current international standards (ISO 26262 "Road Vehicles - Functional Safety") and forthcoming standards (ISO 21434 "Road Vehicles - Cybersecurity engineering"). However, existing software monitoring solutions: * Take hundreds of milliseconds to detect anomalies, which is inadequate for safety-critical applications. **At ~70 mph, a CAV will travel 22 meters in 700 milliseconds, which could be critical to avoid an accident.** * Disturb the normal operation of the SoC. * Are highly visible and more prone to hacking. * Are unable to monitor the entire SoC. Today, no hardware-based, in-life SoC monitoring solution exists. UltraSoC provides on-chip monitoring solutions to monitor the health of SoCs during the design phase and our customers include major firms such as Intel, HiSilicon (Huawei), C-SKY (Alibaba) and more. **However,** **unlike our competitors, our IP is runtime configurable, vendor-neutral, and being hardware-based allows us to** **detect anomalies at 'clock-speed' (i.e. in microseconds), which is 1,000x faster than software.** **Being embedded into the SoC itself during the design phase gives us** **a unique opportunity to exploit our existing IP to monitor SoC health in-life.** However, reliably monitoring SoCs in-life poses significant technical challenges, especially to discriminate normal and abnormal system behaviour in constantly changing operating environments. **This project will develop the world's first on-chip and in-life monitoring solution to detect system anomalies at clock-speed, be vendor-neutral, non-intrusive, runtime configurable and far less prone to hacking.** This will ensure IoT systems function as they were designed, protecting citizens and infrastructure.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Demonstrators Addressing Cyber Security Challenges in the Internet of Things

Competition Code: 1901_SDTAP_CRD

Total available funding is £6,000,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
NQUIRINGMINDS LIMITED	CyberStone: Collaborative Secure IOT Gateway	£837,697	£586,388
CISCO INTERNATIONAL LIMITED		£1,173,650	£586,825
TECHWORKSHUB LTD.		£496,400	£496,400
University of Oxford		£218,085	£218,085

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Objective CyberStone will develop a secure, intelligent, collaborative IOT gateway to address the IOT cyber security challenge. Its key components are * Secure: the gateway will embody security best practice. This encompasses secure boot, secure storage, software component attestation, network segmentation, managed IOT updates, remote management of router capabilities, roots of trust and secure device and user identities. * Intelligent: CyberStone will by dynamic. Using secure edge based processing it will analyse IOT device behaviours and dynamical infer risk using a mix of strategies from statistics to full blown AI. The processing will include cloud based security services, that complement the local analytics * Collaborative: the IOT risk is shared across players. A collaborative ecosystem of information sharing is needed to both detect and mitigate risks. CyberStone will define collaborative information sharing protocols, IOT fingerprinting techniques and technical integration layers to make wide scale deployment and impact possible **Why the gateway** Why address the issue at the gateway? For both deep technical and entirely pragmatic purposes securing the IOT endpoint is impossible. The horse has already bolted. The IOT gateway is an essential component of most IOT deployments, but provides a unique management node, to monitor, analyse, and mitigate risk across heterogeneous IOT devices and networks. Equally, any deep IOT security endpoint innovation will require an IOT gateway innovation to be practically deployable **The team** CyberStone is an active collaboration between: NquiringMinds - a leading UK AI and Cyber SME, Cisco - one of the worlds foremost router and gateway suppliers, The Internet of Things Security Foundation - a UK based trade association, with international reach, focusing entirely on IOT security and University of Oxford Cyber Security Centre , one of the UKs leading academic cyber centres of excellence