



SCOTT Newsletter July 2020



CONTENT

- Good news: another SCOTT session at an important conference!
- X-Burst explained in under 6 minutes!
- New YouTube Video available: Semantic Attribute-Based Access Control (SABAC) demonstrator
- SCOTT Safety & Security Technologies
- SCOTT featured as Project of the Week on cyberwatching.eu
- What's new from SCOTT Distributed Cloud Integration
- Low latency WSA systems supported by Edge Computing
- International Student Contest soon open!
- SCOTT work published in IEEE Journal
- How to harvest energy anywhere and run a wireless network with it

Welcome!

This is the July 2020 edition of the SCOTT newsletter, highlighting news & achievements from SCOTT during Q2 2020.

Please distribute this newsletter to all interested parties in your organization. We appreciate your feedback, please send comments or requests to scott@v2c2.at.

Enjoy the reading!



Good news: another SCOTT session at an important conference!

Apr 2, 2020

We are happy to announce that the SCOTT special session ("SS1:Trustworthiness and Security Focused Wireless Industrial IoT Networks") we have suggested and organized was accepted and in the WFCS conference program.

Due to the current global situation, the WFCS2020 was held virtually on 27 - 29 April 2020, see <https://www.cister-labs.pt/wfcs2020/>

The following papers were presented:

- TDOA-enhanced DistanceBounding in the Presence of Noise
- Lifetime Security Concept for Industrial Wireless Sensor Networks
- Tightening up security in lowpower deterministic networks
- Energy-efficient LinkCapacity Overprovisioning in Time Slotted Channel Hopping Networks

A big thank you to the organization team (Andreas, Kristina, Hans-Peter, Leander, Lukasz, Michael, Peter, Tomas)!



X-Burst explained in under 6 minutes!

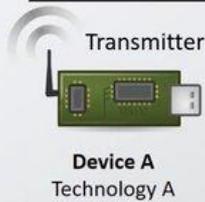
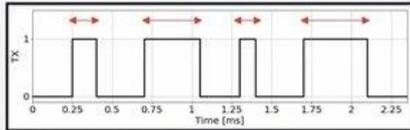
Apr 16, 2020

SCOTT partner TUG just released a video on YouTube explaining the X-Burst technology in under 6 minutes - see <https://youtu.be/7OgCQzbUQQE>. X-Burst is the innovative new technology providing Cross-Technology Broadcast Communication between off-the-shelf Wi-Fi, BLE and ZigBee Devices.

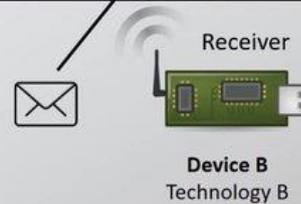
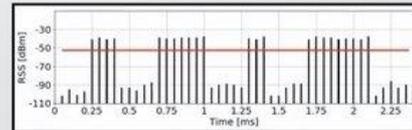
This video provides an introduction to the basic principles, and shows a demonstrator proving that off-the-shelf Wi-Fi, BLE, and IEEE 802.15.4 devices such as the Raspberry Pi 3B+, the TelosB mote, the TI CC2650 Launchpad, and the Zolertia Firefly can broadcast cross-technology frames to each other with an effective throughput above 1 kbps.

Let's Find a Common Ground!

- Encode data into sequence of durations
- Create **energy bursts** of given durations by transmitting regular packets of variable length



- Sampling the received signal strength
- Detect **energy bursts**



New YouTube Video available: Semantic Attribute-Based Access Control (SABAC) demonstrator

Apr 22, 2020

The Semantic Attribute-Based Access Control (SABAC) demonstrator presents a solution designed to ensure easy deployment of the systems created in SCOTT's Workpackage 9 Secure Connected Facilities Management. It will improve its performance, enhance the security of the whole system, and improve the interoperability. SABAC provides fine-grained access control, dynamic and context-aware access control by considering the context surrounding subjects (i.e., users or requesters) and objects (i.e., resources) & improves the interoperability by making decisions semantically and considering the semantic relationships for inferring new policies (i.e., implicit policies). Watch the great and informative video here: <https://www.youtube.com/watch?v=TVWY2v0ToJM>

Defining a SABAC Policy



which is combination of ABAC and semantic technol



SCOTT Safety & Security Technologies

May 18, 2020

Package WP23 on Safety and Security consists of a number of Building Blocks that address different aspects of safety and security. As a part of the work, key objectives of this Safety and Security Technology line are:

- Development of solutions to build trust in smart wirelessly connected devices, components and systems.
- Development of a flexible security and privacy architecture that allow pre-processing of data depending on the use case e.g. gateway support, end-device capability.
- Development of integrated safety and security development approaches.

Recent and publicized results from this work package include the work and demonstration of Remote Attestation (with talks on that topic available at the Code::Dive conference <https://codedive.pl/index/speaker/name/gabriela-limonta> and <https://codedive.pl/index/speaker/name/ian-oliver>), as well as the previously promoted Security Scan methodology document for basic checking of a network architecture's following of state of the art security procedures and protocols. More information can be found in a Whitepaper available here: <https://scottproject.eu/download/whitepaper-security-scan-methodology-for-cloud-connected-iot-devices/>

Learn more about SCOTT using <https://scottproject.eu/>

GABRIELA LIMONTA



Gabriela is a researcher in the CyberSecurity Research group at Nokia Bell Labs. She specializes in using trusted computing technologies to create a Trustworthy Telco Cloud and using root cause analysis techniques to diagnose and mitigate trust failures. She joined Bell Labs in 2019 and she's been working at Nokia since 2016. In her free time, she enjoys knitting.

PRESENTATIONS

WHAT DOES IT MEAN TO TRUST YOUR BOOT PROCESS?
(2019)



SCOTT featured as Project of the Week on cyberwatching.eu

May 19, 2020

We are proud to announce that SCOTT is featured as **Project of the Week** on cyberwatching.eu! Check it out on <https://cyberwatching.eu/services/catalogue-of-services/project-week-scott>



What's new from SCOTT Distributed Cloud Integration

May 25, 2020

SCOTT's WP24 is dedicated to **Distributed Cloud Integration**, connecting IoT via vehicular and 5G networks. Here the focus is on

- remote management, configuration, and seamless heterogeneous communication of wireless devices
- Provisioning of guidelines for Application Layer Protocols on cloud architectures
- analytics platforms
- mobile Edge Computing for Security and Privacy
- secure cloud-based services for mobility applications
- Adoption of ABAC models using semantic technologies
- cloud technologies for 5G network slicing

Interested? Recent research results include

1. A Vehicle Telematics Service for Driving Style Detection: Implementation and Privacy Challenges, VEHITS 2020, <http://www.insticc.org/node/TechnicalProgram/VEHITS/2020/presentationDetails/93294>
2. Cross-Federation Identities for IoT Devices in Cellular Networks, ETFA 2019, <https://ieeexplore.ieee.org/document/8868982>

3. Towards a Generic IoT platform for Data-driven Vehicle Services, ICVES 2018, <https://doi.org/10.1109/ICVES.2018.8519505>



Low latency WSAAN systems supported by Edge Computing

May 28, 2020

SCOTT partner TU Delft (TUD) has produced a little video explaining their work in WP24 for **low latency WSAAN systems**: <https://youtu.be/WEh2nDZi7x8>. Connected vehicles need to react to imminent threats fast enough. Therefore, they leverage edge computing to perform the bare minimum analysis to detect threats that require immediate action. TUD developed a set of small robot cars to test out and showcase this work. A partially completed version of TUD's testbed is shown in the video. More on SCOTT can be found at <https://scottproject.eu>



International Student Contest soon open!

Jun 4, 2020

SCOTT organizes the **International Student Contest** "Secure and Trustable Wirelessly Connected IoT", organized and sponsored by NXP, AVL, VIF, UIO, GUT, Pomorskie Voivodship (Poland), Interizon ICT Cluster, and AP/MTT/AES Joint Chapter, IEEE Poland

1st PLACE: 1300€ 2nd PLACE: 1000€ 3rd PLACE: 700€ Additional SPECIAL PRIZES for finalists: 500 € each, cool gadgets and books and internship opportunities

Tell us about your bachelor or master thesis, PhD dissertation or any kind of student project and win awesome prizes! Think of wearables used in healthcare and smart living, think of your smart home appliances, future smart cities, connected cars, or all the machines collaborating in a modern production facility (talk Industry 4.0). They are all part of "The Internet of Things" (IoT), which revolutionizes our everyday life, one of the most important drivers of digital transformation. But are the IoT devices secure? Can you trust them? The European research project SCOTT (Secure COnnected Trustable Things) consortium organizes a competition for students and recent graduates. If your bachelor or master thesis, PhD dissertation or student project of any kind addresses issues like security, safety, trust, and dependability applicable to wired and wireless communication or can be used in interesting IoT applications, send us its description, applicability fields, together with your CV.

We are interested in accomplished projects targeting industrial domains like automotive, aeronautics, building, health, robotics, smart manufacturing, etc. that can be a part of the future secure and wirelessly connected world. The contest finalist will have an opportunity to present their projects before representatives of the leading European companies and universities in September 2020.

To apply go to <https://scottproject.eu/>

Topics: The contest will be focusing on (but not limited to) the following topics:

- Advanced wireless sensor networks (WSN) and IoT concepts for industrial use cases in domains like automotive, aeronautics, building, health, robotics, smart manufacturing, with the focus on one or more of the following attributes: security, safety, reliability, trustability.
- Theoretical aspects of security, privacy, safety and trust for IoT.
- Innovative energy-constrained and autonomous IoT components.
- Dependable WSN with enhanced energy efficiency, robustness and quality-of-service.
- Physical layer and out-of-band security in WSN applications.
- Routing and scheduling algorithms for reliable real-time WSNs.
- Secure identification, authentication, authorization and communication in WSN.
- Trust anchors and trust indicators for secure IoT systems.
- Edge and Cloud computing services for safe and secure connected mobility applications.
- Secure localization using radio technology.
- UWB solutions for distance bounding and positioning.
- Secure car access technologies.
- Secure and robust Integration of IoT systems with edge/cloud services.
- Connected vehicles (e.g. cars, trucks, ...) interacting with personal mobile devices and systems of passengers, road participants, other vehicles and cloud services.



SCOTT work published in IEEE Journal

Jun 9, 2020

SCOTT is proud to announce another high-rank publication: Georgi Nikolov and his co-authors from the Cork Institute of Technology (CIT) published "ASR - Adaptive Similarity-Based Regressor for Uplink Data Rate Estimation in Mobile Networks" in the IEEE Journal on Selected Areas in Communications June 2020 special issue on Advances in Artificial Intelligence and Machine Learning for Networking (DOI: 10.1109/JSAC.2020.3000414). Publishing in such high prestigious journal is just another testament of the great work all the partners are doing in SCOTT. Find out more about SCOTT at <https://scottproject.eu/>



How to harvest energy anywhere and run a wireless network with it

Jun 23, 2020

SCOTT Technologies for Autonomy and Energy Efficiency of Wireless Sensor Networks

SCOTT's WP25 aims to improve autonomy of devices and energy efficiency of Wireless Sensor Networks (WSNs) through the development of a set of Building Blocks that will help to achieve the following objectives of the Technology Line:

- Development and integration of energy harvesting and energy storage technologies applicable in different contexts and industrial domains.
- Development of novel, energy efficient hardware and software components for WSNs.
- Development of methods for integration and testing of energy-constrained WSNs.

Some of the main research results from this WP are:

- Security enhancement of a WSN prototype for automotive test-beds considering tight energy and low computational resources constraints.
- A local oscillator signal generation sub-system designed within strict power consumption constraints, as part of an integrated UWB SoC to be used for the purposes of distance bounding in secure car access system solutions (see picture).
- An energy prediction algorithm to predict energy income on devices operating with a minimum amount of energy, by adjusting the time slots for data transmission, in order not to deplete the energy stored (see picture). This algorithm has been integrated into a harvester device developed for environments where the energy source is either not predictable or steady but with very low voltage generation.
- An energy supply system for electronic equipment used in on-track segments, which harvests energy from two primary mechanical sources (track deformation and air

displacement when a train is passing by, see picture) and from solar photovoltaic panels as a third source.

- A concept study of security aspects for in-vehicle WSNs considering the energy constraints of devices powered by batteries, energy harvesting system, or a combination of both.
- An investigation of how fault level injection techniques can contribute to a fast release of large and complex systems.
- Technologies supporting efficient and secure network deployment, runtime operation, and maintenance of in-vehicle networks, for the layers above the physical layer.

