9.8 The Internet of INSECURE Things

Date: Thursday 30 March 2017
Time: 08:30 - 10:00
Location / Room: Exhibition Theatre

Organiser:
Marcello Coppola, STMicroelectronics, FR

Today everything from the door locks, a heating system or vehicle can be connected to internet opening the endless possibilities of future innovative technologies. As more low-power and internet-connected gadgets and sensors are integrated to our lives, an increase in demand for developing secure and trustworthy IoT-based systems is becoming the key element to make winning products.

Although, there has been a steady increase in improving the security, still proper authentication and encrypted communications are not common; making the overall Internet as a network of insecure things. This session proposes a journey through several speeches to show the advances in technologies that master the security aspects of IoT.

The session starts with an in-depth overview of security challenges and the trends in the IoT ecosystem against cyber-threats. Then, introduces the STM32 and the secure IoT platforms based on STM32 called SECube. Finally, the session provides some real use cases for smart vehicle, where IoT have a big impact on the type of applications and services that can be deployed using the association between vehicle and the homes of their owners. Last but not least, all the pre-registered attendees are eligible to get one of IoT platforms presented by the speakers via the www.secube.eu web site.

Time	Label	Presentation Title Authors
08:30	9.8.1	**CHALLENGES FOR SECURE IOT** **Speaker**: Paolo Prinetto, Politecnico di Torino, IT
08:45	9.8.2	**MITIGATING THE RISKS IN IOT WITH AN EFFECTIVE SECURITY OFFER** **Speaker**: Michele Scarlatella, STMicroelectronics, FR ***Abstract*** *The IoT will change our lives, bringing huge benefits and making a positive impact on society and the economy, but it requires trusted systems with efficient security and privacy mechanisms from devices to the Cloud. For years digital security technologies have proven their efficiency in telecom, banking and ID applications. Technical solutions exist and can be reused as a toolbox to provide security and privacy for the IoT.* *In this session we will describe how STMicroelectronics' scalable security offer based on STM32 microcontrollers and STSAFE secure microcontrollers make it possible to build secure IoT solutions with the right level of robustness, The STMicroelectronics scalable offer for IoT security can also be adapted to efficiently combat various threats. STMicroelectronics, a global semiconductor leader supplying the market with the most advanced technologies and solutions and a 20-year presence in security, is committed to contributing to a more secure connected world.*
09:00	9.8.3	**UNIVERSITY EXPERIENCES USING A SECURE IOT PLATFORM BASED ON STM32** **Speaker**: George Kornarors, Univ. of Applied Sciences of Crete, GR ***Abstract*** *In this session practical design methods and experiences are presented centered on STM32 devices. Gateways and connected IoT devices networks need to be secured as well as the devices themselves. Suitable safeguards must be integrated to prevent network interfaces and emdedded firmware updates from becoming security holes themselves; these safeguards refer to securing the data stored by the device, secure communication and protecting the device from cyber-attacks Software and hardware development approaches are outlined along with practical experiences that meets the appropriate security level of modern IoT platforms.*
09:15	9.8.4	**SECUBE™: THE SECURE COMMERCIAL IOT PLATFORM** **Speaker**: Antonio Varriale, Blu5 Labs Ltd, MT ***Abstract*** *The SEcube™ (Secure Environment cube) platform presented in this session is an open source security-oriented hardware and software platform constructed with ease of integration and service-orientation in mind. It is based on a single-chip design embedding three main cores: a highly powerful processor, a Common Criteria certified smartcard, and a flexible FPGA. The software components include several libraries of ready-to-use components that provide developers with different entry levels to adoption. This way, security experts can avail of the open source character and verify, change or write from scratch the entire system, starting from the elementary low-level blocks. At the same time developers who use the predefined primitives can experience the SEcube™ as a high-security black box suitable for security-oriented services in several fields, like IoT, Automotive, etc.*
09:30	9.8.5	**SECURE COMMUNICATION IN AUTOMOTIVE** **Speaker**: Giovanni Gherardi, Energica Motor Company, IT ***Abstract*** *The growth and diffusion of high technology consumer communication devices and the following tech skills in average user are pushing industry to put connectivity/network functions in devices. Automotive industry is riding as well this wave. Vehicles are nowadays implementing new "Cyber Physical Features" by collecting information from the physical system and processing it via interconnected cyber systems, creating thus new challenges for safety and security. In addition, an increasing number of vehicles are nowadays connected to the Web, and the capillarity of interconnected IoT devices are drawing the future for the customer expectations in term of innovative services. Historically, security was first of all achieved with isolation of subsystems and, nowadays, with the growing number of interconnected systems that are indirectly interconnected with IoT services highlight how component level countermeasures are important but not enough to enforce protection in a modern vehicle. A multi-level, coordinated, system wide approach is necessary such as isolation of safety critical systems, secure gateways, virtualization, trusted software injection and execution, but not only. It requires also a re-design of vehicle data transport infrastructure with new communication standards with the adoption of secure protocols like sCAN.*

Time	Label	Presentation Title Authors
10:00		End of session **Coffee Break** in Exhibition Area On all conference days (Tuesday to Thursday), coffee and tea will be served during the coffee breaks at the below-mentioned times in the exhibition area. Tuesday, March 28, 2017 ○ Coffee Break 10:30 - 11:30 ○ Coffee Break 16:00 - 17:00 Wednesday, March 29, 2017 ○ Coffee Break 10:00 - 11:00 ○ Coffee Break 16:00 - 17:00 Thursday, March 30, 2017 ○ Coffee Break 10:00 - 11:00 ○ Coffee Break 15:30 - 16:00

Source URL: https://past.date-conference.com/date17/conference/session/9.8