NSF Convergence Accelerator's 2022 Cohort Phase 1 Award

Project Title
SMART-5G: Secure Multichannel Automated opeRations Through 5G Networks

Awardee
IBM
Consulting Federal

Award/Contract #
49100422C0022

Award Contract Type
R&D

Award Date
July 15, 2022

Principal Investigator
Seraphin B. Calo
scalo@us.ibm.com

Co-Principal Investigator
Elisa Bertino
Thomas F. LaPorta

NSF Funded Directorate
Directorate for Technology, Innovation and Partnerships

NSF Funded Program
NSF's Convergence Accelerator

NSF Program Director
Ibrahim Mohedas
Track G: Securely Operating Through 5G Infrastructure
Convergence Accelerator
Directorate of Technology, Innovation and Partnerships
imohedas@nsf.gov

PROJECT ABSTRACT
The objective of the SMART-5G project or Secure Multichannel Automated opeRations Through 5G Networks, is to develop a suite of technologies, tools and operational principles which will allow for the secure operation of military communications on civilian 5G infrastructure. We will employ the capabilities of Multi-access Edge Computers or MEC, for secure communication. By leveraging military-provided servers that are deployed within the 5G network infrastructure plus servers at the tactical edge and in the backend infrastructure, we show how a more secure operational environment can be obtained with a variety of techniques including: application of AI to network traffic inspection, policy-driven separation of traffic along a low-bandwidth secure communication path and a high-bandwidth insecure communication path, virtual multi-function authentication leveraging mobile edge computing mechanisms, and self-generation of security policies for automated operations.

To support the scenarios to be developed as part of the convergence research project, the team will develop a suite of technologies to enable military personnel to operate through the insecure 5G network without compromising security requirements, and group these technologies into three different, but inter-related thrusts: multi-channel exploitation, network situation awareness, and automation of security workflows. Multi-channel exploitation includes the use of multiple channels with different performance and security properties to provide the required environment for mission-critical applications. Network situation awareness provides information to users through monitoring and analysis of the traffic and activities in the 5G network; and, automation of security workflows use automation of security protocols to improve responsiveness to threats.

This multidisciplinary effort brings together research fields such as computer science, machine learning, network operations and management, and social science. Potential threats that can be launched through social engineering will be identified, and countermeasures proposed for detection and mitigation.