



NSF Convergence Accelerator's 2022 Cohort Phase 1 Award

Project Title

Feasible Cooperative Zero Trust Framework for 5G

Awardee

BlackBerry Corporation

Award/Contract

49100422C0021

Award Contract Type

R&D

Award Date

July 25, 2022

Principal Investigator

Andrew Walenstein

awalenstein@blackberry.com

Co-Principal Investigator

Bryan Cunningham

Ian Harris

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

Millions of Americans connect daily to 5G cellular networks through their devices; however, most are unaware that their connections depend on stacks of software running on legions of networking components. Their security and privacy therefore directly depends on the trustworthiness of this infrastructural software, and yet network customers can do very little themselves to verify the trustworthiness. The user must trust the processes, standards, and regulations used by the network operators and their regulators. As a result, network customers cannot currently extend principles of "Zero Trust" (ZT) to the network; namely, they cannot meaningfully observe and establish a reasoned basis for trust in the software critical to their security and privacy.

Our convergence accelerator team will combine expertise in software security analysis, human-centered design, networking, cybersecurity, standards, laws, and regulations to establish a novel technical foundation for ZT cybersecurity solutions in the context of multi-stakeholder, high-security 5G networks. Called "Cooperative Zero Trust," (CZT) multiple parties— notably, clients and network operators —will use it to work jointly on continuously assuring trustworthiness of the 5G infrastructure software involved in a client's network. To develop CZT the team will: (1) develop novel theoretical and technical foundations for CZT solutions and frameworks, including a trustworthy and efficient technical foundation for inserting software monitoring into 5G infrastructure, (2) utilize human-readable technical requirements documents to develop new automated indicators of software trust that are intelligible and actionable, and (3) pave the way for widespread adoption of CZT security technologies by ensuring their pragmatic workability within existing regulatory environments, and designing incentive structures through legal and regulatory framework development, including aligned draft laws and standards.