

AUTHENTICATION FOR LAW ENFORCEMENT VEHICLE SYSTEMS

The National Cybersecurity Center of Excellence (NCCoE) is helping the law enforcement community address the challenge of securing in-vehicle systems through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Authentication for Law Enforcement Vehicle Systems* project description, including background and challenge, goals, and potential benefits. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge, please contact us at lev-nccoe@nist.gov.

BACKGROUND

A law enforcement officer's daily tasks require the use of a diverse suite of applications, each with its own set of login credentials. When leaving their vehicles unattended, officers are forced to make a choice. Logging out of multiple, sensitive systems could increase response time. Even the simple practice of locking or unlocking a laptop screen can impede an officer's ability to confront an approaching suspect. However, remaining logged in, even behind a screen lock, is a major security risk. A screen lock does not necessarily prevent multiple logged-in application sessions from being hijacked, possibly by a hacker compromising the vehicle laptop directly or via an in-vehicle Wi-Fi system.

CHALLENGE

Traditional practices for securing computers and applications in an office setting are not ideal for a vehicle-based operational environment. A police-vehicle environment presents two unique challenges: it is more vulnerable to being physically compromised than computers in an office setting, and the demands of security controls, such as multiple complex passwords, might interfere with safe vehicle operation. If implemented poorly, authentication security controls can actually increase risks to the computer systems and databases that these controls are intended to protect. The absence of an integrated authentication mechanism negatively affects both security and the law enforcement mission.

GOALS

Integrated reduced-sign-on (RSO) enables multiple applications to share a single authentication action taken by the user, eliminating the need for the user to log in more than once. Standards-based approaches to RSO may already be supported by most commercial applications and can offer a wide variety of development programming interfaces to ease integration with custom applications. The Authentication for Law Enforcement Vehicle Systems project aims to demonstrate, using standards-based commercially available products, an integrated authentication architecture compatible with the law enforcement vehicle operational environment. The NCCoE research will address two scenarios: the officer sign-on at the start of a shift, and the automatic deactivation of the session that occurs when an officer exits a law enforcement vehicle.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCoE
Visit <http://nccoe.nist.gov>

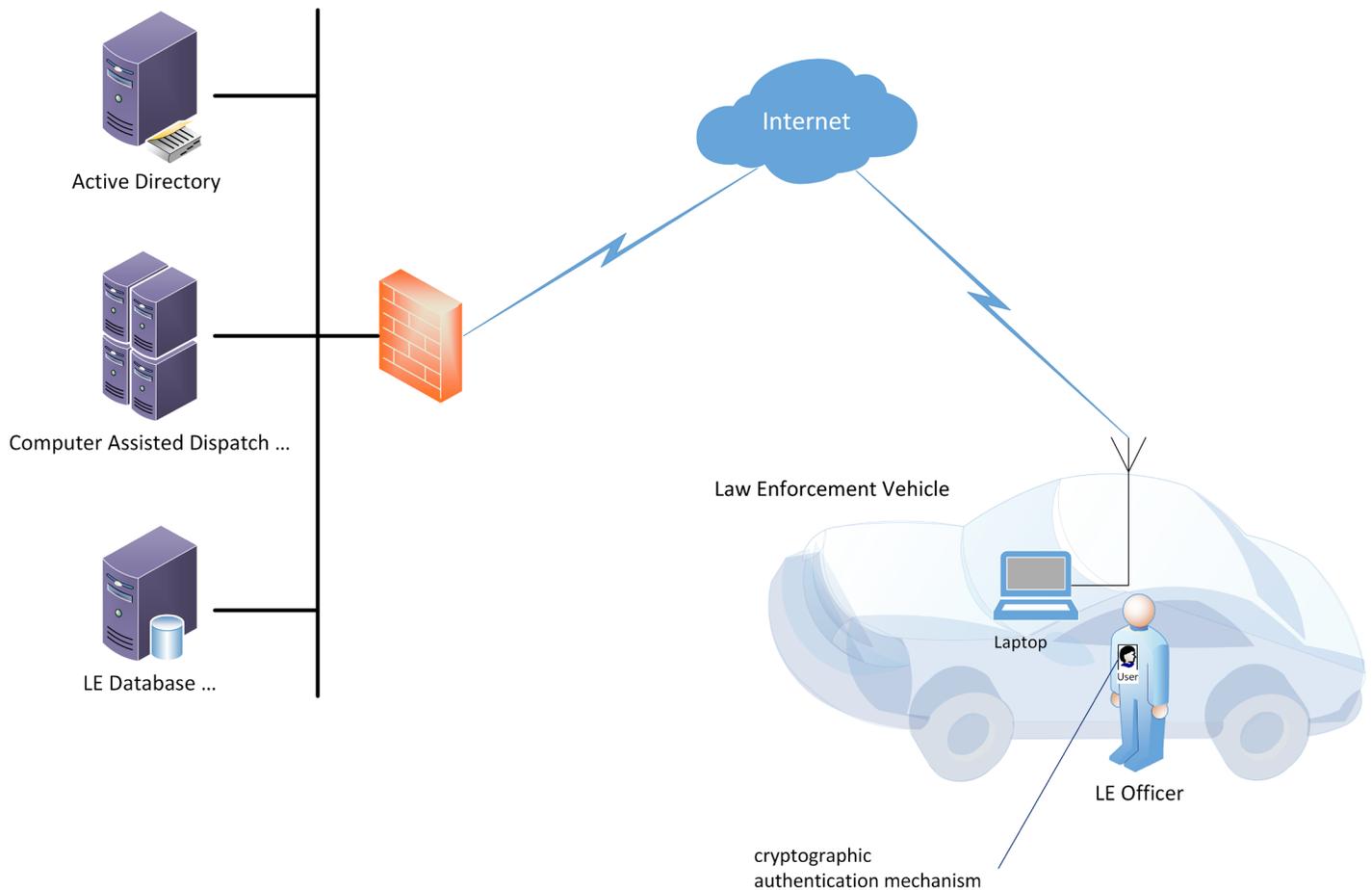
CONTACT US
nccoe@nist.gov
301-975-0200

BENEFITS

The potential mission benefits of the authentication solution explored by this project include:

- enhanced mission effectiveness by restoring sessions rapidly to all required systems when the officer enters the vehicle
- reduced risk to sensitive back-end databases and systems by providing for automatic screen and application locking of in-vehicle systems when an officer exits the vehicle
- improved officer safety by allowing the officer to maintain situational awareness of the vehicle and environment rather than logging in again to multiple systems
- stronger standards-based authentication through FIPS 201 PIV compliant tokens

HIGH-LEVEL ARCHITECTURE



DOWNLOAD THE PROJECT DESCRIPTION

Visit https://nccoe.nist.gov/projects/use_cases/authentication-law-enforcement-vehicle-systems to learn more about this project.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you have questions about this project or would like to join the Law Enforcement Community of Interest, please contact us at lev-nccoe@nist.gov.