PROJECT DESCRIPTION

AUTHENTICATION FOR LAW ENFORCEMENT VEHICLE SYSTEMS

Donald Tobin
National Cybersecurity Center of Excellence

DRAFT
September 2016
lev-nccoe@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) 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. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a particular problem that is relevant across the Law Enforcement community. NCCoE cybersecurity experts will address this challenge through collaboration with members of the community and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by Law Enforcement organizations.

ABSTRACT

Law enforcement vehicles often serve as mobile offices. In-vehicle laptops or other computer systems are used to access a wide range of software applications and databases hosted and operated by federal, state, and local agencies, with each typically requiring a different username and password. This operational environment presents unique security challenges. Officers must frequently leave the vehicle unattended, perhaps on short notice, and must be able to gain access to systems quickly once they return or possibly while the vehicle is in motion. These needs discourage the use of screen locks and traditional single sign-on solutions. This project will demonstrate an integrated set of authentication mechanisms, improving system security, usability, and safety. This project will also explore additional capabilities, such as proximity authentication, derived Personal Identity Verification (PIV) credentials, integration with FirstNet, and integration with vehicle drive-away protection and Computer Assisted Dispatch systems to indicate whether the officer is in the vehicle. This project will result in a freely available NIST Cybersecurity Practice Guide that will enable members of the community to more easily and effectively incorporate proximity access and reduced-sign-on technologies.

KEYWORDS

law enforcement; proximity authentication; reduced sign on; automotive; vehicle upfit systems

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology or the National Cybersecurity Center of Excellence, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: lev-nccoe@nist.gov

Public comment period: *September 12, 2016 to October 12, 2016*

Table of Contents

1. Executive Summary

Purpose

Traditional security practices for securing computers and applications in an office setting are not necessarily as effective in a vehicle-based operational environment. The police vehicle environment presents two unique challenges. First, as with other mobile environments, it is more vulnerable to being physically compromised. Second, the demands of security controls, such as multiple complex passwords, might interfere with safe vehicle operation.

An officer's daily tasks require the use of a diverse suite of applications, each with a separate set of login credentials. The absence of an integrated authentication mechanism can negatively affect both security and the law enforcement mission. When leaving their vehicles unattended, officers are forced to choose between logging out of sensitive systems, potentially increasing response time, and remaining logged into those systems, thereby decreasing security. For example, even the simple practice of locking or unlocking a laptop screen can impede an officer's ability to confront an approaching suspect.

Poor implementation of authentication security controls can also increase risks to the computer systems and databases that these controls are intended to protect. With many diverse logins, officers may resort to using password managers, spreadsheets, and paper notes to record passwords. Alternatively, relying only on a screen lock to protect multiple logged-in application sessions does not prevent these sessions from being hijacked, possibly by a hacker compromising the vehicle laptop directly or via an in-vehicle Wi-Fi system.

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 are easier to adopt as they may already be supported by most commercial applications and can offer a wide variety of development programming interfaces to ease integration with custom applications. Modern standards-based approaches also support sharing of strong authentication with applications in a secure manner without requiring a trusted relationship between applications. These capabilities are useful when integrating RSO across jurisdictions, such as federal law enforcement information providers and state or local providers.

The project described in this document aims to address these concerns by demonstrating an integrated authentication architecture compatible with the law enforcement vehicle operational environment. By integrating simplified identity and authentication technologies, such as proximity, biometrics, tokens, or other similar technologies, with readily available RSO tools, law enforcement organizations can enhance mission effectiveness, improve officer safety, and reduce risk to sensitive back-end databases and systems. This project will result in a publicly available NIST

Cybersecurity Practice Guide, a detailed guide of the practical steps needed to implement our cybersecurity reference design that addresses this challenge.

Scope

This project will meet the goals above by integrating commercially available, standards-based security products into a representative architecture, which we will build in our laboratory. This architecture will include a representative vehicle, one or more proximity identification/authentication solutions, and an in-vehicle computer or laptop with datalink. If technologies permit, the vehicle may also be modified to implement drive-away deterrence. The architecture will also include all necessary back-end systems to support authentication, a Computer Assisted Dispatch system or mock-up to support presence indication, and real or representative applications an officer would typically access during day-to-day operations.

To the extent practical, we may demonstrate integration with non-production test/development instances of applications hosted by law enforcement partners.

Assumptions/Challenges

Windows-based laptops

This project assumes the use of commodity-based laptop or mobile computer systems operating Microsoft Windows, which are the most common within the law enforcement community. While the concepts within the project would still apply, integration with systems based on other technologies, such as Google Android or Apple iOS tablets, would require additional effort on the part of the integrator.

Differing back-end applications

Many law enforcement applications are hosted by different federal, state, and local agencies, resulting in integration challenges that will be unique to each agency seeking to adopt the results of this project. However, our focus on standards-based solutions should facilitate this integration.

Limited market space

The market space for solutions optimized around an in-vehicle workforce or that interface with vehicles and related systems is limited. However, we believe that a wide variety of standards-based proximity authentication mechanisms used in other environments can easily be adapted to meet the requirements of this project.

Background

The NCCoE, working with federal, state, and local law enforcement, identified the need for an identity management solution for the in-vehicle operational environment. Additional Law Enforcement Organizations (LEOs), including other state police agencies, professional associations, and federal departments have provided input to this project description. Through public comments, NIST is eager to receive input from a broad array of stakeholders including LEOs, officers, technology vendors, and the public at large.

2. Scenarios

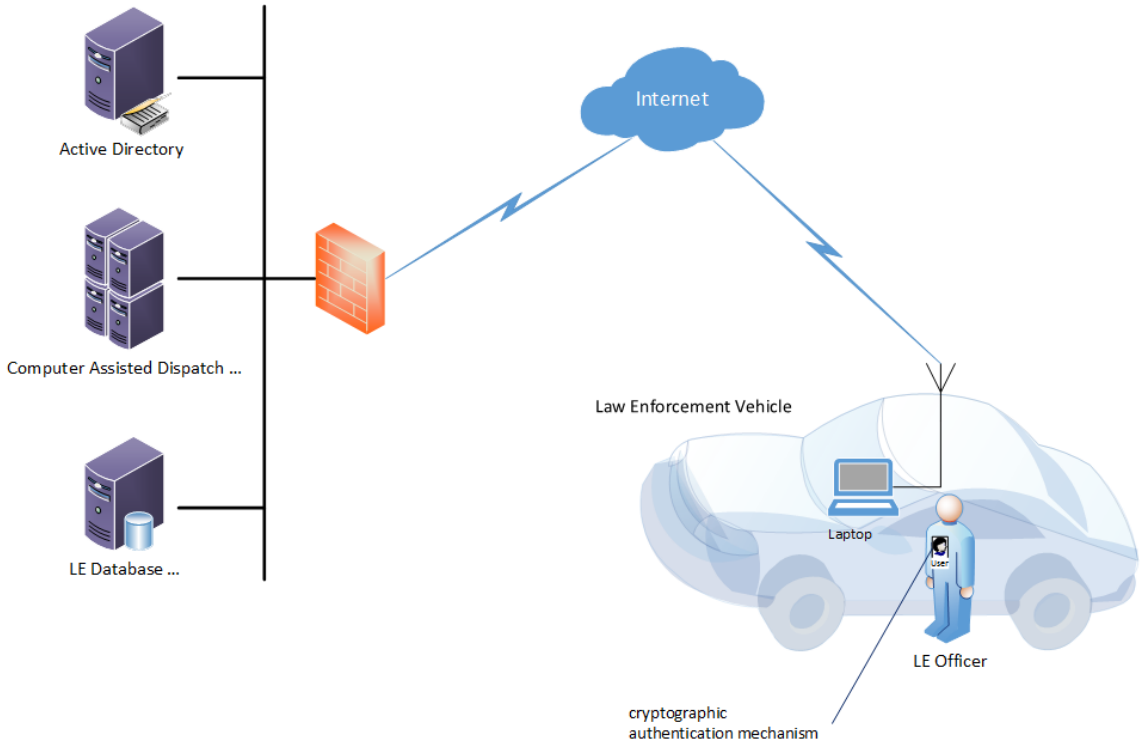
Scenario 1: Officer Start-of-Shift Sign-On

At the start of a shift, the officer initially authenticates to a laptop using a smart card token, biometric, or other mechanism. An RSO solution acting as a trust store authenticates the officer to additional remote applications as each is opened.

Scenario 2: Screen Lock

When the officer exits the vehicle, a proximity token with a reader, door switch, or similar system automatically locks the laptop screen and possibly suspends access to remote applications. When the officer returns, a simplified authentication, such as a biometric or proximity token with a reader, could automatically unlock the laptop and restore access to remote applications. If the officer has been gone for a longer period of time, a stronger form of authentication could be required.

3. High-Level Architecture



Component List

An integrated RSO solution for the law enforcement vehicle operational environment includes but is not limited to the following components:

- Law Enforcement Vehicle, consisting of:
  - a console-mounted laptop

- proximity, biometric, token, or other simplified authentication solution(s)
- cellular or other wireless data connectivity

- representative back-end systems consisting of:
  - a connection to the internet or other network that enables access from the in-vehicle laptop
  - a perimeter router and firewall representative of a common security perimeter
  - an authentication and directory service (e.g. Active Directory)
  - multiple representative applications, such as:
    - an e-mail service
    - a Computer Assisted Dispatch application
    - a case management system
    - a state or national criminal information system (e.g. National Crime Information Center)
- integrating software/components, including:
  - reduced sign-on software components
  - standards-based tools to support cryptographic credentials
  - tools to integrate with selected simplified authentication solutions

Desired Requirements

To address the scenarios noted above, this project will use a collection of commercially available technologies to demonstrate the following security and functional characteristics:

- provide for automatic screen locking and possible application locking of an in-vehicle system when the officer exits the vehicle
- restore sessions rapidly with minimal interaction when the officer returns to the vehicle
- allow integration with readily available single sign-on tools to enable the officer to log in to multiple applications with a single set of credentials
- demonstrate the use of a FIPS 201 PIV-compliant token
  - provides strong, standards-based identity verification and authentication
  - enables secured access to modern applications
  - more securely enables backwards-compatible RSO solutions for legacy systems
- authenticate quickly and safely while the vehicle is in motion

In addition, if technologies identified for the project permit, the project will also:

- integrate with Computer Assisted Dispatch or fleet management tools to enable dispatch to know if the officer is in the vehicle, informing the best means to contact the officer and improving officer safety

- enable drive-away protection to deter unauthorized operation of the vehicle

4. Relevant Standards and Guidance

- Fast IDentity Online (FIDO) Alliance Universal 2nd Factor (U2F)
- FIDO Universal Authentication Framework (UAF)
- Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 Standard: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
- Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) v2.0: https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- RFC 6749 - The OAuth 2.0 Authorization Framework: https://tools.ietf.org/html/rfc6749
- User-Managed Access (UMA) Profile of OAuth 2.0: https://tools.ietf.org/html/draft-hardjono-oauth-umacore-13
- OpenID Connect Core v1.0: http://openid.net/specs/openid-connect-core-1_0.html
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.24, May 2015 (https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TN9iAAG&field=File__Body__s)
- Federal Information Processing Standards (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST, August 2013 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf)
- NIST Special Publication 800-63-2, Electronic Authentication Guideline, NIST, August 2013 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)
- NIST Special Publication 800-73-4, Interfaces for Personal Identity Verification, NIST, May 2015 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf)
- NIST Special Publication 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST, May 2014 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)
- NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST, December 2014 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf)

- ISO/IEC 15693 B Identification cards -- Contactless integrated circuit cards -- Vicinity cards
- ISO/IEC 14443 A,B Identification cards -- Contactless integrated circuit cards -- Proximity cards

5. Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 1: Security Control Map

Requirement	NIST CSF Category	Informative References	
Automatic screen and application locking of an in-vehicle system when officer exits vehicle	PR.AC-2 PR.PT-4 RS.RP-1 RC.RP-1 DE.CM-3	**COBIT 5** **ISA 62443-2-1:2009** **ISA 62443-3-3:2013** **NIST SP 800-53 Rev. 4** **CCS CSC**	APO13.01, BAI01.10, DSS01.04, DSS02.05, DSS03.04, DSS05.05, DSS05.02 4.3.3.3.2, 4.3.3.3.8, 4.3.4.5.1, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 6.2, SR 7.1, SR 7.6, A.1, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.12.4.1, A.13.1.1, A.13.2.1 1.2.3, A.16.1.5 AC-2, AC-4, AC-17, AC-18, AU-12, AU-13, CA-7, CM-10, CM-11, CP-2, CP-8, CP-10, IR-4, IR-8, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, SC-7 7, 8, 18
Minimal interaction for rapid session restoration	PR.AC-1 PR.AC-2 PR.AC-3 PR.PT-4 RS.RP-1 RC.RP-1	**COBIT 5** **ISA 62443-2-1:2009** **ISO/IEC 27001:2013**	APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS06.03 4.3.3.3.2, 4.3.3.3.8, 4.3.3.5.1, 4.3.3.6.6 A.6.2.2, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1

		NIST SP 800-53 Rev. 4	AC-2, AC‑17, AC-19, AC-20, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		CCS CSC	16
		ISA 62443-3-3:2013	SR 1.13, SR 2.6
RSO tools integration to provide a single set of credentials for multiple applications	ID.GV-1 PR.AC-1 PR.AC-3	**COBIT 5**	APO01.03, APO13.01, DSS01.04, DSS05.03, EDM01.01, EDM01.02,
		ISA 62443-2-1:2009	4.3.2.6, 4.3.3.5.1, 4.3.3.6.6
		ISA 62443-3-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.6
		ISO/IEC 27001:2013	A.5.1.1, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, A.6.2.2, A.13.1.1, A.13.2.1
		NIST SP 800-53 Rev. 4	controls from all families
		CCS CSC	16
		ISA 62443-3-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
FIPS 201 Personal Identity Verification compliant token to provide strong, standards-based identity verification and authentication to enable secured access to applications	PR.AC-1 PR.AC-2 PR.AC-4 PR.DS-6	**COBIT 5**	DSS01.04, DSS05.04, DSS05.05, DSS06.03
		ISA 62443-2-1:2009	4.3.3.3.2, 4.3.3.3.8, 4.3.3.7.3, 4.3.3.5.1,
		ISO/IEC 27001:2013	A.6.1.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, SR 2.1, SR 3.1, SR 3.3, SR 3.4, SR 3.8
		NIST SP 800-53 Rev. 4	AC-2, AC-3, AC-5, AC-6, AC-16, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, SI-7
		CCS CSC	12, 15, 16
		ISA 62443-3-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 2.1, SR 3.1, SR 3.3, SR 3.4, SR 3.8

Authenticate quickly and safely while the vehicle is in motion	PR.AC-1 PR.AC-2 PR.AC-4	**COBIT 5**	DSS01.04, DSS05.04, DSS05.05, DSS06.03
		ISA 62443-2-1:2009	4.3.3.3.2, 4.3.3.3.8, 4.3.3.5.1
		ISO/IEC 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		NIST SP 800-53 Rev. 4	AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		CCS CSC	16
		ISA 62443-3-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

182

APPENDIX A - ACRONYMS AND ABBREVIATIONS

FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standards
LEO	Law Enforcement Organizations
LEV	Law Enforcement Vehicle
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PIV	Personal Identity Verification
RSO	Reduced Sign-on
SAML	Security Assertion Markup Language
U2F	Universal Second Factor
UAF	Universal Authentication Framework
UMA	User Managed Access
XACML	eXtensible Access Control Markup Language

185 ## APPENDIX B - GLOSSARY

Backwards-compatible	able to be used with an older piece of hardware or software without special adaptation or modification
Datalink	an electronic connection for the exchange of information
Derived PIV Credential	an X.509 derived PIV authentication certificate, which is issued in accordance with the requirements specified in this document where the PIV authentication certificate on the applicant's PIV card serves as the original credential. The derived PIV credential is an additional common identity credential under HSPD-12 and FIPS 201 that is issued by a federal department or agency and used with mobile devices
Legacy System	an old method, technology, computer system, or application program

186