NIST SPECIAL PUBLICATION 1800-17A

Multifactor Authentication for E-Commerce

Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

Volume A:
Executive Summary

William Newhouse
Information Technology Laboratory
National Institute of Standards and Technology

Brian Johnson
Sarah Kinling
Jason Kuruvilla
Blaine Mulugeta
Kenneth Sandlin
The MITRE Corporation
McLean, Virginia

July 2019

This publication is available free of charge from https://doi.org/10.6028/NIST.SP.1800-17

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf

Executive Summary

- Retailers can implement multifactor authentication (MFA) to reduce the opportunity for a customer's online account to be used for fraudulent purchases.
- MFA is a security enhancement that allows a user to present several pieces of evidence when logging into an account. This evidence falls into three categories: something you know (e.g., password), something you have (e.g., smart card), and something you are (e.g., fingerprint). The presented evidence must come from at least two different categories to enhance security.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore MFA options available to retailers today, and documented the example implementations that retailers can consider for their environment.
- This NIST Cybersecurity Practice Guide demonstrates how online retailers can implement MFA to help reduce electronic commerce (e-commerce) fraud.

CHALLENGE

Smart chip credit cards and terminals work together to protect in-store payments. The in-store security advances were introduced in 2015, and those have pushed malicious actors who possess stolen credit card data to perform payment card fraud online. This guide describes implementing stronger user-authentication techniques to reduce the risk of e-commerce fraud. The guide documents a system in which risk determines when to trigger MFA challenges to existing customers.

SOLUTION

This project's example implementations analyze risk to prompt returning purchasers with additional authentication requests when risk elements are exceeded during the online shopping session. Risk elements may include contextual data related to the returning purchaser and the current shopping transaction. The example implementations will prompt a returning purchaser to present another distinct authentication factor—something the purchaser has—in addition to the username and password, when automated risk assessments indicate an increased likelihood of fraudulent activity.

The MFA capabilities for e-commerce used in this guide are based upon the Fast IDentity Online (FIDO) Universal Second Factor (U2F) authentication specification. The methods chosen in this guide provide examples that can be adopted by retailers to help reduce e-commerce fraud.

The NCCoE sought existing technologies that provide the following capabilities:

- integrate MFA into online shopping systems
- mitigate potential exposure to online fraud
- integrate into a variety of retail-information technology architectures
- provide authentication options to retailers:
    - capabilities that assess and mitigate a retailer's shopping-transaction risk factors

- alert retailer staff to potential threats, and adjust authentication mechanisms as needed

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to *Multifactor Authentication for E-Commerce* can help your organization:

- reduce online fraudulent purchases, including those resulting from the use of credential stuffing to take over accounts
- show customers that the organization is committed to its security
- protect your e-commerce systems
  - provide greater situational awareness
  - avoid system-administrator-account takeover through phishing
- implement the example solutions by using our step-by-step guide

SHARE YOUR FEEDBACK

You can view or download the guide at https://nccoe.nist.gov/projects/use-cases/multifactor-authentication-ecommerce. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at consumer-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200