PROJECT DESCRIPTION

MULTIFACTOR AUTHENTICATION FOR E-COMMERCE

Online Authentication for the Retail Sector

William Newhouse
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Sarah Weeks
Blaine Mulugeta
Ken Sandlin
The MITRE Corporation

September 2016
consumer-nccoe@nist.gov

This revision incorporates comments from the public.

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 consumer-facing/retail sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the consumer-facing/retail sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by consumer-facing/retail sector organizations.

ABSTRACT

As greater security control mechanisms are implemented at the point of sale, retailers in the U.S. may see a drastic increase in e-commerce fraud, similar to what has been widely observed in the United Kingdom and Europe following the rollout of Europay, MasterCard, and Visa (EMV) chip-and-PIN technology approximately ten years ago. Consumers, retailers, payment processors, banks, and card issuers are all impacted by the security risks of e-commerce transactions. Retailers bear the cost for fraudulent, card-not-present (CNP) transactions, motivating them to reduce fraud in order to avoid damage to reputation and eliminate potential revenue losses, which have been estimated to be over $3 billion dollars.[1] Successfully reducing e-commerce fraud requires many, layered strategies, and includes an increased level of assurance in purchaser or user identity. In collaboration with stakeholders in the retail and e-commerce ecosystem, the NCCoE has identified that implementing multifactor authentication (MFA) for e-commerce transactions, tied to existing web analytics and contextual risk calculation (by the retailer and/or by a federated identity provider), can increase assurance in purchaser or user identity and thus help reduce the risk of false online identification and authentication fraud. The NCCoE understands that retail is a volume-reliant business and that consumers and retailers will adopt multifactor authentication mechanisms as long as they do not unnecessarily encumber the purchasing process or disrupt the user experience.

Building on this collaboration with the business community and vendors of cybersecurity solutions, the NCCoE will explore methods to effectively identify and authenticate purchasers during e-commerce transactions and develop an example solution composed of open-source and commercially available components. This project will produce a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to implement practices that effectively identify and authenticate purchasers during e-commerce transactions.

KEYWORDS

retail; multifactor; authentication; MFA; e-commerce; fraud; card-not-present; CNP; web analytics; risk calculation

DISCLAIMER

Certain commercial entities, equipment, 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 NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Table of Contents

1. Executive Summary

Purpose

The purpose of this project is to help retailers implement stronger authentication mechanisms (methods to ensure the card user is authorized to use the card by the card owner) for e-commerce transactions in card-not-present (CNP) scenarios. While at the present time of this publication chip credit cards in the U.S. are being processed as chip-and-signature rather than chip-and-PIN, the adoption of chip-and-PIN may be considered by some as an inevitability. As chip credit card usage increases, especially with PIN instead of signature at some point in the future, the ease with which fraudsters successfully commit fraud in card-present scenarios will decrease. Thus, this project aims to help prepare retailers in terms of proactively protecting themselves and their customers from the likely future increase in CNP e-commerce fraud in the U.S.

To achieve this purpose, the National Cybersecurity Center of Excellence (NCCoE) will develop an example multifactor authentication solution composed of standards-based commercial and open-source products currently available in the marketplace. The project process includes identifying stakeholders and systems participating in the CNP transactions, defining the interactions between the stakeholders and retailer systems, identifying mitigating security technologies, and ultimately providing an example implementation.

Multifactor authentication will also be central to a new National Cybersecurity Awareness Campaign launched by the National Cyber Security Alliance designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The National Cyber Security Alliance will partner with leading technology firms like Google, Facebook, Dropbox, and Microsoft to make it easier for millions of users to secure their online accounts, and financial services companies such as MasterCard, Visa, PayPal, and Venmo that are making transactions more secure.[2] Considering the anticipated rise of fraudulent activity due to stronger security mechanisms for card-present transactions, retailers should invest in understanding and implementing stronger authentication mechanisms for CNP purchases, while being sensitive to the user experience.

The publication of this project description is the beginning of a process that will identify project participants, cybersecurity vendors, and their relevant commercially available or open-source hardware and software components. These components will be used in a laboratory environment where the project team will build open, standards-based, modular, end-to-end reference designs that will address the CNP authentication problem. The approach may include architectural definition, logical design, build development, test and evaluation, and security control mapping. The output of the process will be the publication of a multi-volume NIST Cybersecurity Practice Guide that will help consumer-facing and retail organizations implement multifactor authentication for e-commerce transactions.

Scope

The scope of this example solution includes the implementation of risk calculation, web analytics, and common multifactor authentication mechanisms during e-commerce transactions for a repeat customer (RC) of a simulated retailer website. The project scope may or may not include identity federation. For the purposes of this project, guest checkout purchasing flows, blockchain and distributed ledger technologies, micropayments, and security challenges specific to mobile payments and mobile shopping are out of scope but may be considered for future work for the NCCoE in the consumer-facing/retail space.

Assumptions

This example solution of multifactor authentication for e-commerce transactions provides numerous security benefits including increased confidence in user identity and reduced risk. The NCCoE understands that a retail business would weigh the cost of investment in a multifactor authentication solution with its potential benefits, which include protection of reputation and trust from the consumer, as well as reduced fraud losses.

The security of existing systems and networks is out of scope for this project. A key assumption is that all potential adopters of this project or any of its components already have in place some degree of system and network security, as well as many, layered e-commerce fraud reduction measures. Therefore, we intend to focus on the effort of complementing existing system and network security and e-commerce fraud reduction strategies with risk calculation, web analytics, and multifactor authentication.

Background

The NCCoE, working with retail organizations and other e-commerce payment stakeholders, including information sharing and analysis centers (ISACs) and the Retail Cyber Intelligence Sharing Center (R-CISC), has identified the potential need and benefits of a multifactor authentication for e-commerce solution. The need arises from the recognition that malicious actors are likely increasingly motivated to exploit security vulnerabilities in CNP retail transactions in response to the adoption of EMV chip credit cards in the U.S.

The NCCoE also held a workshop to identify key issues that affect multifactor authentication for e-commerce. The conversations held and insight derived from that workshop have informed the direction of this project and this project description.

2. SCENARIOS

Scenario 1: Repeat customer, repeated context – MFA Not Activated

While getting his child ready for bed, the RC of an online retailer finds the supply of disposable diapers is low. The RC logs into the online retailer's website to order

disposable diapers. He authenticates with a user ID and password and finds the diapers in the favorites section. In seconds, the RC places the same order for diapers that he has placed in the past, and is not prompted for any additional authentication.

In the background, automated risk and web analytics on the retailer's system are comparing the RC's current behavior and the context of his website access to stored data. The online retailer grades this purchase as low risk because of the nature of the product, a known internet protocol (IP) address associated with the customer, typical geolocation, and consistency with past patterns of online purchases. In this scenario, the stepped up additional authentication was not activated.

Scenario 2: Repeat customer, new context – MFA Activated

While on travel for business across the country from her residence, a RC of an online retailer remembers that this day would be the deadline to buy a gift online for a friend's birthday. She opens the laptop she usually uses exclusively for work and navigates to the retailer's website. The RC authenticates with a user ID and password and browses several categories of expensive items that she usually does not browse. After some time browsing, the customer finds a product to purchase and puts it in her virtual shopping cart. She then follows the prompts to choose shipping and stored payment methods. After entering these choices, the user is prompted with a message stating that the retailer requests she enter an additional authenticator[3] before completing the transaction. The user completes the multifactor authentication process and completes the transaction.

In the background, automated risk and web analytics on the retailer's system are comparing the RC's current behavior and the context of her website access to stored data. The online retailer grades this purchase as high risk because of the nature of the product, an unknown IP address associated with the customer, atypical geolocation, and deviance from past patterns of online purchases. In this scenario, the stepped up additional authentication was activated.

Scenario 3: Fraud perpetrator – MFA Activated

After illegally receiving the credentials of a legitimate RC of an online retailer, a fraud perpetrator (FP) in a country different from the RC navigates to the retailer's website with the intention of committing e-commerce fraud and receiving goods paid for by the RC. The FP does not browse but goes straight to an expensive electronic item, adds the item to his shopping cart, and begins the checkout process. During checkout, the FP chooses stored payment information, but edits the shipping address to one not previously associated with the RC. After entering these choices, the FP is prompted with a message requesting that he enter a multifactor authentication ID as an additional step before completing the transaction. The FP attempts to spoof the ID a number of times before another message appears indicating that the transaction has been terminated and the account has been locked.

In the background, automated risk and web analytics on the retailer's system are comparing the FP's current behavior and the context of her website access to stored data. The user's device, behavior, IP address, geolocation, and shopping choices do not align sufficiently per the retailer's risk threshold and pose a relatively high fraud risk, so the FP is prompted for additional authentication. Because the retailer has implemented a limit to additional multifactor authentication attempts, after a few attempts the user account is locked until the retailer's fraud detection team can contact the account owner. In this scenario, the stepped up additional authentication was activated.

3. High-Level Architecture

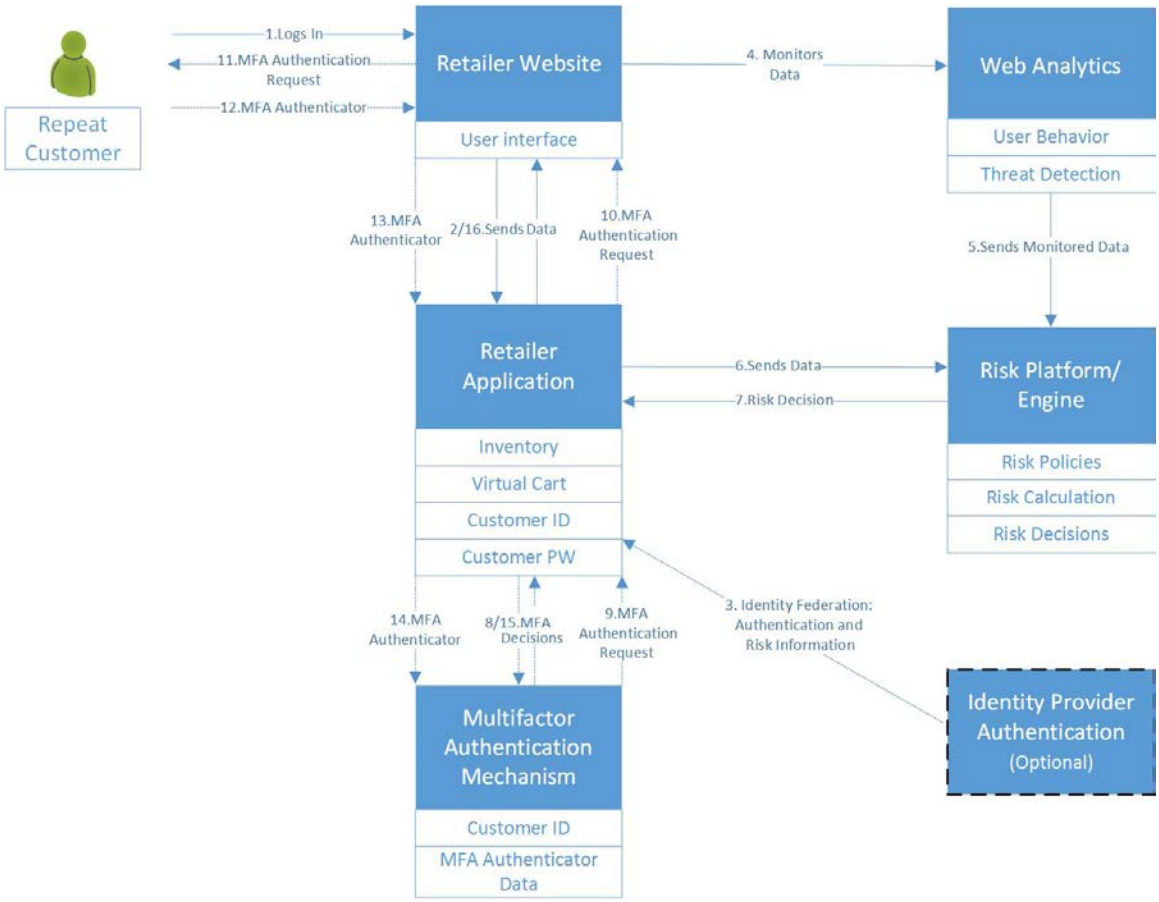

Figure 1: High-level Architecture

Component List

A multifactor authentication solution for e-commerce transactions includes but is not limited to the following components:

- Online/e-commerce shopping cart and payment system (in-house or outsourced)
- Multifactor authentication mechanisms (types of which to be determined)
- Risk calculation platform/engine

- Web analytics engine
- Logging of risk calculation and web analytics data
- Data storage for risk calculation and web analytics data
- Identity federation mechanism (optional)

Desired Requirements

- Authentication mechanisms that meet business security and regulatory requirements
- Automated web analytics including monitoring of user behavior and contextual details
- Automated logging of web analytics and risk calculation data
- Automated data storage of web analytics and risk calculation data
- Ability to establish and enforce risk decisions including performing risk calculations
- Automated alerting of suspected fraudulent activity
- Ease of use for the consumer, no substantial increase in friction during the e-commerce transaction
- Identity federation (optional)

4. Relevant Standards and Guidance

- ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems
  http://www.iso.org/iso/home/search.htm?qt=27001&sort=rel&type=simple&published=on
- ISO/IEC 29115, Information Technology – Security Techniques – Entity authentication assurance framework
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138
- ISO/IEC 29146, Information Technology – Security techniques – A framework for access management, https://www.iso.org/obp/ui/#iso:std:iso-iec:29146:ed-1:v1:en
- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure
  http://www.nist.gov/itl/cyberframework.cfm
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
  http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
- NIST SP 800-63-2, Electronic Authentication Guide
  http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

- NIST SP 800-73-4, Interfaces for Personal Identity Verification (3 Parts) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf
- Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2, April 2016, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

5. Security Control Map

Table 1 maps the characteristics of the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and other NIST activities. The solution characteristics offered in the table are the ones expected to be explored in this project. This mapping exercise, which is likely to expand as the project progresses, is meant to demonstrate the real-world applicability of standards and best practices.

Solution Characteristic	NIST CSF Category	Informative References
Authentication mechanisms	PR.AC-1 PR.AC-3 PR.AC-4	**NIST SP 800-53 Rev. 4** AC-1, IA Family; AC-17, AC-19, AC-20; AC-2, AC-3, AC- 5, AC-6, AC-16 **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.6.2.2, A.13.1.1, A.13.2.1; A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
Automated web analytics	DE.AE-1 DE.AE-2 DE.AE-3	**NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4; AU-6, CA-7, IR-4, IR 5, IR-8, SI-4; **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
Automated logging	PR.PT-1	**NIST SP 800-53 Rev. 4** AU Family, IR-5, IR-6 **ISO/IEC27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
Automated data storage	PR.DS-1 PR.DS-3	**NIST SP 800-53 Rev. 4** SC-28; CM-8, MP-6, PE-16 **ISO/IEC27001:2013** 7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3
Ability to establish and enforce risk decisions	ID.RA-3 ID.RA-4 ID.MS	**NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, PM-12, PM-16, SA-14, SI-5

Table 1: Security Control Map

APPENDIX A – REFERENCES

[1] Payment Card Fraud Management: Essential Tools for U.S. Card Issuers, Julie Conroy, Aite Group, April 2, 2015, http://aitegroup.com/report/payment-card-fraud-management-essential-tools-us-card-issuers

[2] Fact Sheet: Cybersecurity National Action Plan, Office of the Press Secretary, The White House, February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[3] Draft NIST Special Publication 800-63-3, Digital Authentication Guideline: Public Preview, Paul A. Grassi and James L. Fenton, National Institute of Standards and Technology, https://pages.nist.gov/800-63-3/sp800-63-3.html

[4] U.S. e-commerce grows 14.6% in 2015, Stefany Zaroban, Internet Retailer Magazine, February 17, 2016, https://www.internetretailer.com/2016/02/17/us-e-commerce-grows-146-2015

[5] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[6] Bring on Cyber Monday: E-Commerce Merchants and Fraud, RSA Monthly Online Fraud Report – October 2014, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-102014.pdf

[7] E-Commerce Fraud Trends 2014: Securing the Online Shopping Cart, RSA Monthly Online Fraud Report – July 2014, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0714.pdf

[8] E-Commerce Transactions – A New Roadmap for Authentication in Europe, Christoph Baert, Paul Baker, and Cathy Mulrow-Peattie, MasterCard Inc., http://newsroom.mastercard.com/wp-content/uploads/2015/07/A-New-Roadmap-for-Authentication-in-Europe.pdf

[9] Preparing for Chip-and-PIN Cards in the United States, Mark Scott, New York Times, December 2, 2014, http://bits.blogs.nytimes.com/2014/12/02/preparing-for-chip-and-pin-cards-in-the-united-states/?_r=1

[10] Card-Not-Present Fraud: A Primer on Trends and Authentication Processes, A Smart Card Alliance Payments Council White Paper, Smart Card Alliance Payments Council, February 2014, http://www.smartcardalliance.org/resources/pdf/CNP-WP-012414.pdf

[11] Card-Not-Present Fraud Working Committee White Paper: Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, Version 1.0, EMV Migration Forum: Card-Not-Present Fraud Working Committee, April 2015, http://www.emv-connection.com/wp-content/uploads/2015/04/CNP-Solutions-White-Paper-FINAL.pdf

[12] Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization (ISO), http://www.iso.org/iso/catalogue_detail?csnumber=54534