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
The MITRE Corporation

DRAFT
May 5, 2016
consumer-nccoe@nist.gov

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 United States may see a drastic increase in e-commerce fraud, similar to what has been widely observed in the UK and Europe following the rollout of 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 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] Part of e-commerce fraud reduction includes an increased level of assurance in purchaser or user identity. In collaboration with stakeholders in the retail and e-commerce ecosystem, the National Cybersecurity Center of Excellence (NCCoE) has identified that implementing multifactor authentication for e-commerce transactions, tied to existing web analytics and contextual risk calculation, can help reduce the risk of false online identification and authentication fraud. Consumers and retailers will adopt multifactor authentication mechanisms as long as they do not unnecessarily encumber the purchasing process or if they are applied evenly across the entire sector.

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 publically 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; retail; 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.

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: consumer-nccoe@nist.gov

Public comment period: *May 5, 2016 to June 3, 2016*

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, using standards-based commercially available and open source products. 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 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 and hardware and software components for use in a laboratory environment to 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.

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 known user of a simulated retailer website. For the purposes of this project, guest check-out purchasing flows, certificate-based authentication, and biometric authentication mechanisms are out of scope.

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 benefits of using a multifactor authentication solution will outweigh any additional costs and risks that may be introduced.

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. Therefore, we focused on the effort of complementing existing system and network security with risk calculation, web analytics, and multifactor authentication. The goal of this solution is to not introduce additional vulnerabilities into existing systems.

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), identified the need for 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 card-not-present (CNP) retail transactions in response to the adoption of EMV chip credit cards in the United States. The NCCoE 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

While getting her child ready for bed a repeat customer of an online retail customer finds the supply of disposable diapers is low. The customer logs into the online retailer's website to order disposable diapers. She authenticates with a user ID and password. She finds the diapers in the favorites section. In seconds she places the same order for diapers that she has placed in the past. The online retailer grades this purchase as low risk because of the nature of the product, a known IP address associated with the customer, geolocation, and past patterns of purchases within the website. The customer is not prompted for any additional authentication.

Scenario 2: Repeat customer, new context

While on travel for business across the country from her residence, a repeat customer 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 for work and navigates to the retailer’s website. The customer inputs a username and password to enter the site and browses several categories of expensive items that she usually does not browse. After some time browsing, the customer finds a product to purchase as a gift 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 a multifactor authentication ID (either pre-distributed, dynamically sent to a known phone number or email address, or other multifactor mechanism such as biometric authentication) 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 this known user's current behavior and the context of her website access to stored data. Because the user's device, behavior, IP address, geolocation, and shopping choices do not align sufficiently per the retailer's risk threshold and poses a relatively high fraud risk, the user is prompted for additional authentication.

Scenario 3: Fraud perpetrator

After illegally receiving the credentials of a legitimate, repeat customer (RC) for an online retailer, a fraud perpetrator (FP) in another country from the repeat customer 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 malicious actor is prompted with a message requesting that he enter a multifactor authentication token ID (either pre-distributed or dynamically sent via phone or email to known numbers and addresses) as an additional step before completing the transaction. The malicious actor 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 this known user's current behavior and the context of his website access to stored data. Because the user's device, behavior, IP address, geolocation, and shopping choices do not align sufficiently per the retailer's risk threshold and poses a relatively high fraud risk, the user is prompted for additional authentication. Because the retailer has implemented a limit to authentication attempts, after a few attempts the user account is locked until the retailer's fraud detection team can contact the account owner.

3. High-Level Architecture

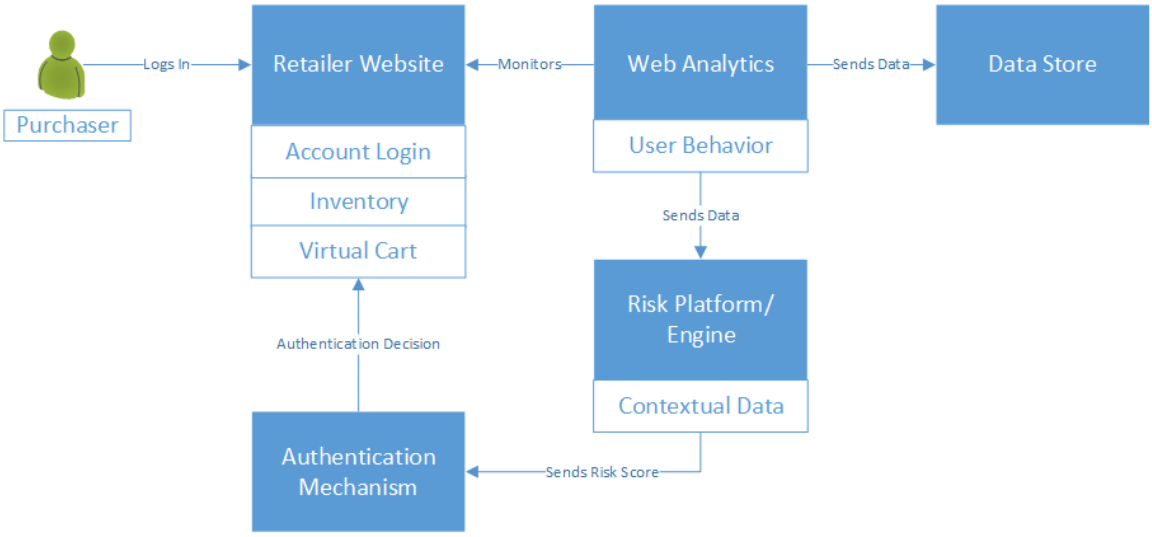

Diagram 1: High-level Architecture

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
- Risk calculation platform/engine
- Web analytics engine
- Logging of risk calculation and web analytics data
- Data storage for risk calculation and web analytics data

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

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 3.1, April 2015, PCI Security Standards Council,
  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.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

163 Table 1: Security Control Map

164 ## 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] 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

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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

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

165