USE CASE | Consumer/Retail

MULTIFACTOR AUTHENTICATION FOR E-COMMERCE

Online Authentication for the Retail Sector

The National Cybersecurity Center of Excellence (NCCoE) is helping enterprises ensure the security of their online transactions through collaborative efforts with industry and the Information Technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Multifactor Authentication for e-Commerce* 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 of securing e-commerce transactions, please contact us at consumer-nccoe@nist.gov.

BACKGROUND

When chip-and-PIN technology was introduced in the UK and Europe approximately ten years ago, malicious actors turned to e-commerce fraud due to increased security at the point of sale. As retailers in the United States implement the same security measures, there may be a similar increase in fraudulent, card-not-present (CNP) e-commerce transactions. Consumers, retailers, payment processors, banks, and card issuers are all impacted by the security risks of e-commerce transactions. However, retailers bear the cost for such 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. Part of e-commerce fraud reduction includes an increased level of assurance in purchaser or user identity.

THE CHALLENGE

Retailers are worried that multifactor authentication mechanisms will encumber the purchasing process resulting in loss of sales. Any solution must be user-friendly enough to appeal to the general public, while also integrating with the retailer's existing anti-fraud infrastructure. The challenge lies in identifying sufficiently secure multifactor authentication mechanisms that work in the fast-paced e-commerce environment.

GOALS

In collaboration with stakeholders in the retail and e-commerce ecosystem, the 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.

This project aims to help retailers implement stronger authentication mechanisms to ensure the user is authorized to use the card for e-commerce transactions in CNP scenarios, using standards-based commercially available and open source products. The project process includes identifying stakeholders and systems participating in CNP transactions, defining the interactions between the stakeholders and retailer systems, identifying mitigating security technologies, and ultimately providing an example implementation.

BENEFITS

The potential business benefits explored by this project include:

- increased level of security and assurance for CNP e-commerce transactions
- security alerts through web analytics and risk engine
- ability to automate risk decisions to mitigate risks in real-time
- ability to implement risk based multifactor authentication
- reduced risk of fraudulent CNP e-commerce transactions

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

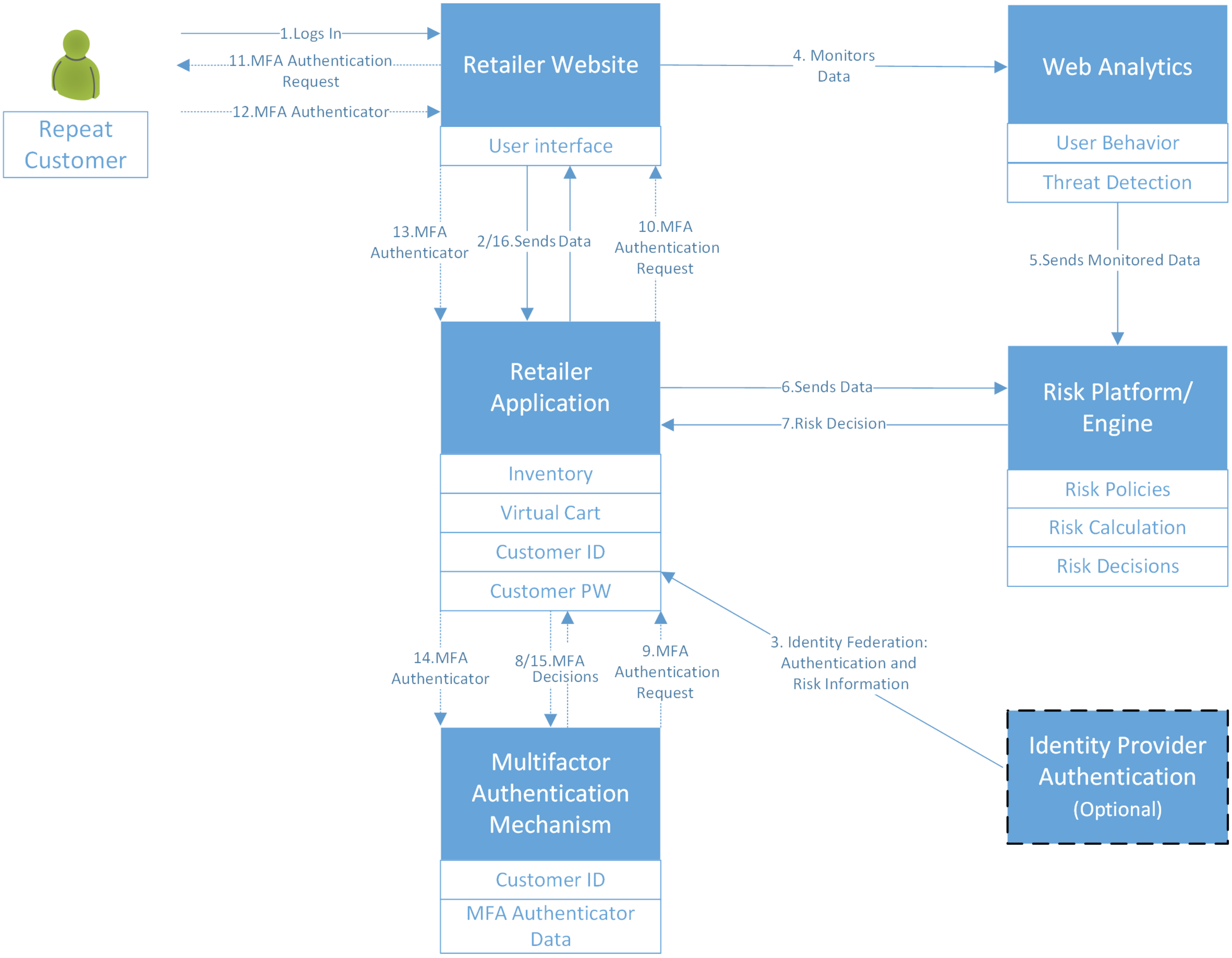
CONTACT US
nccoe@nist.gov
301-975-0200

COMPONENTS

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)

ARCHITECTURE



DOWNLOAD THE PROJECT DESCRIPTION

Visit https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce 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 Consumer/Retail Community of Interest, please contact us at consumer-nccoe@nist.gov.

September 2016