Webinar Recap: Implementing Multifactor Authentication for E-Commerce

NIST Releases Cybersecurity Guide to Help Reduce Online Retail Fraud

Over the past several months, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has been collaborating with retailers and technology vendors on a cybersecurity project using multifactor authentication (MFA) to help reduce the risk of online fraudulent purchases. The project resulted in the recently published draft of cybersecurity practice guide, NIST Special Publication 1800-17, *Multifactor Authentication for E-Commerce*.

The draft guide may be published, but our work is just beginning. Recently, the project's lead engineer participated in an R-CISC community webinar, during which he reviewed the contents of the guide.

A First for the NCCoE

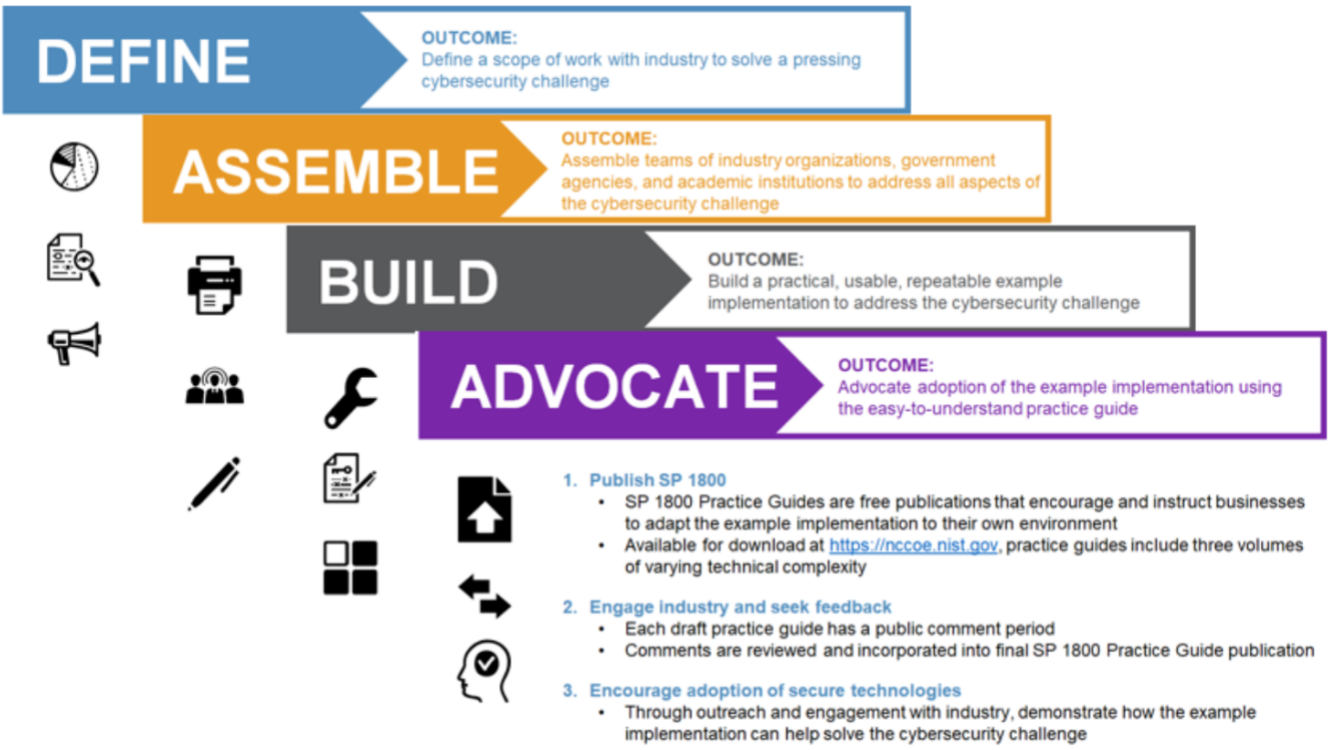
The *Multifactor Authentication for E-Commerce* Practice Guide was the NCCoE's first retail sector project. With so many challenges facing this sector, we made improving the security of online purchases a top priority. Here's why: According to a recent independent analysis, e-commerce fraud increased by 30 percent in 2017, compared with 2016, as malicious actors shift from using stolen credit card data in stores at the checkout counter to using stolen credit card data for fraudulent online shopping. Because online retailers cannot utilize all the benefits of improved credit card technology, the NCCoE focused upon helping online retailers implement stronger user authentication methods.

Meeting the Challenge

To address the challenge of reducing online fraudulent purchases, the NCCoE engaged in a four-step process to:

1. Define the scope of work required to address the cybersecurity challenges within the retail industry
2. Assemble a team of government, industry, academic and other stakeholders to find a solution to the challenge
3. Build an example implementation that industry can use to mitigate their cybersecurity risk
4. Advocate for industry to adopt the example implementations to improve their cybersecurity and better protect their customers from online fraud

In posting the draft publication describing our example implementations, we are in the "advocate" part of the process.

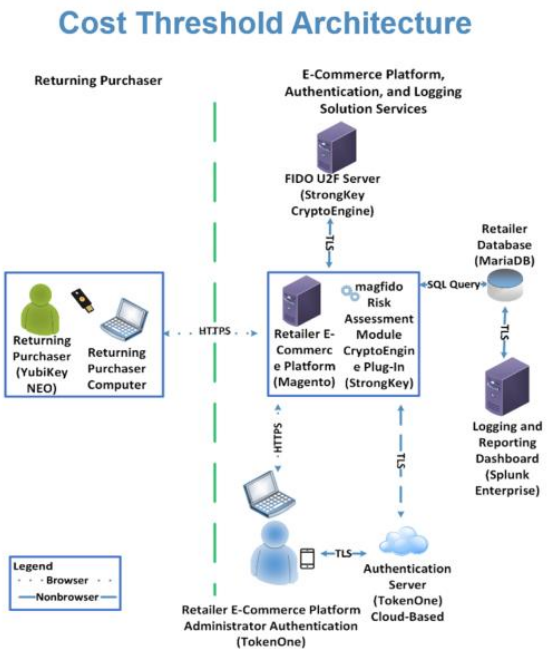


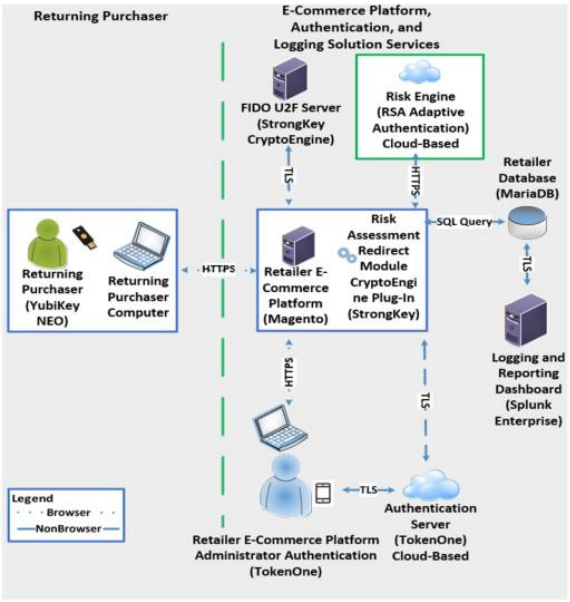
About the Guide

The guide is published in three volumes:

- **Volume A** – an executive summary of the guide to help senior executives and other decision-makers understand what the challenges are, the example implementations and benefits of implementing MFA.
- **Volume B** - provides a more detailed explanation to Chief Information Security Officers or other senior technical staff\ of our approach to addressing the cybersecurity challenge, including the architecture components and how they are mapped to the NIST Cybersecurity Framework.
- **Volume C** is meant for engineers and others who may be involved in implementing MFA, and offers a step-by-step approach to help them replicate our example implementations. Retailers can either use all or parts of the example implementations to meet their unique needs.

The guide explores several risk-based scenarios that use MFA to increase assurance of purchaser identity and reduce fraudulent online purchases. In the project's example implementations, if certain risk elements (contextual data related to the transaction) are present during an online shopping session, it could indicate an increased likelihood of fraudulent activity. The purchaser will then be prompted to present another distinct authentication factor—something the purchaser has—in addition to the username and password to prove their identity





The images above show how MFA can be triggered using a *Cost Threshold* architecture and a *Risk Engine* architecture. The cost threshold example implementation requests additional authentication when a shopping cart dollar amount is exceeded during a purchase. Because fraudulent activity may still occur in purchases below this threshold, the *Risk Engine* example implementation can examine many system and external elements related to a shopping session. The risk engine leverages machine learning to develop a risk score, obtained from an outside service with which the risk engine communicates, to determine whether to prompt a user for additional MFA.

In both the cost threshold and risk engine example implementations, the retailer's e-commerce platform system administrator's account is protected with one-time pad authentication principles. This increases the security of the overall system by prompting the system administrators to use their smartphone-based MFA capability before making changes to the e-commerce platform. Additionally, returning-purchaser account-lockout techniques are demonstrated that can limit credential stuffing and takeovers of customer accounts.

The example implementations also describe and document situational awareness within the overall system that tracks the important processes, including logging system functions such as authentication activity, and providing dashboard displays of this information for system owners.

Both industry and federal security standards and best practices were used to develop two reference designs leveraging commercially available technologies. The draft guide also maps capabilities to NIST guidance and control families, including the NIST Cybersecurity Framework.

What Say You?

During the recent R-CISC webinar, Implementing Multifactor Authentication for E-Commerce, participants responded to a series of questions regarding their experience with MFA. Below is what we learned:

1) **Do you already offer Multifactor Authentication for customers? (select one)**
    - Yes – **33%**
    - Will offer it within 6 months – **0%**
    - No – **67%**

2) **What might keep you from implementing Multifactor Authentication? (select all that apply)**
    - Cost – **57%**
    - Existing fraud reduction tactics – **29%**
    - Project success risk – **43%**
    - Could turn away customers due to increased complexity during the purchaser checkout process – **86%**
    - Your organization's technical expertise on MFA implementations – **29%**

3) **What 2nd authentication factor does your organization prefer? (select all that apply)**
    - Hardware token-Customer brings their own device – **50%**
    - Hardware token-Retailer supplied device – **25%**
    - Mobile application – **50%**
    - Text (Short Message Service-SMS) – **25%**
    - Email – **0%**

Tell Us What You Think!

The NCCoE believes the draft guide helps meet a critical cybersecurity and economic need, but we want to hear from you. **Please share your thoughts on this step-by-step guide to help enhance it.** Download the draft guide and provide your feedback on the NCCoE comment page. **The public comment period closes on October 22, 2018.**

And to learn more about the work of the NCCoE Retail team and to contribute new ideas for improving the cybersecurity of the retail sector, please consider joining our Retail Community of Interest. If interested, send an email to consumer-nccoe@nist.gov.