National Cybersecurity Center of Excellence

Multifactor Authentication for e-Commerce Project

Cloud Identity Summit
June 19, 2017

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Overview

- U.S. adoption of credit cards equipped with computer chips helps retailers achieve greater protection against fraud in stores, but potentially pushes fraud into card not present e-commerce transactions.
- Reducing e-commerce fraud requires implementing security standards and processes to achieve an increased level of assurance in purchaser or user identity.

Project Goals

- Implement multifactor authentication (MFA) for e-commerce transactions, tied to existing web analytics and contextual risk calculation to increase assurance in purchaser or user identity.
- Help retailers implement stronger authentication mechanisms using standards-based, commercially available or open source products.

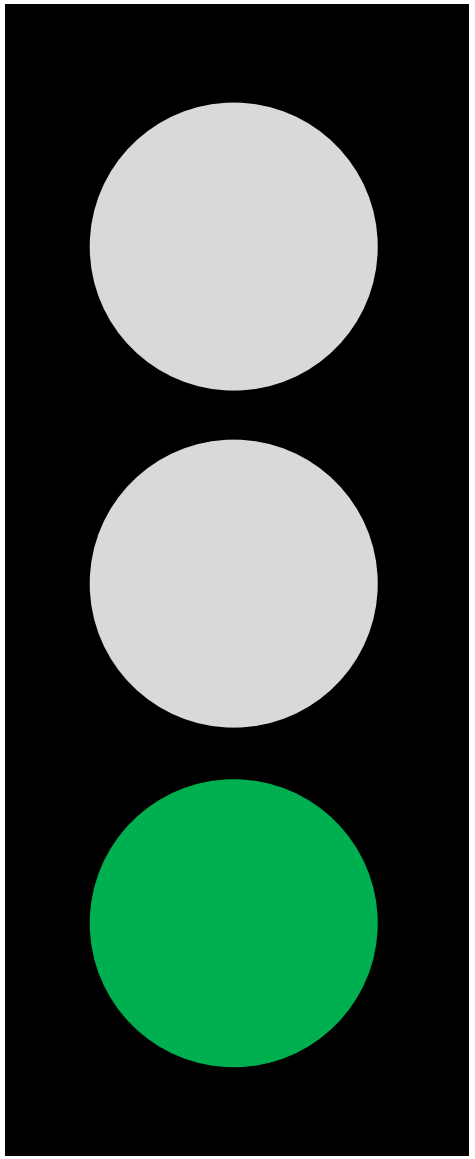
Origin

- NISTIR 8050 Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy

Repeat Customer, Repeat Context

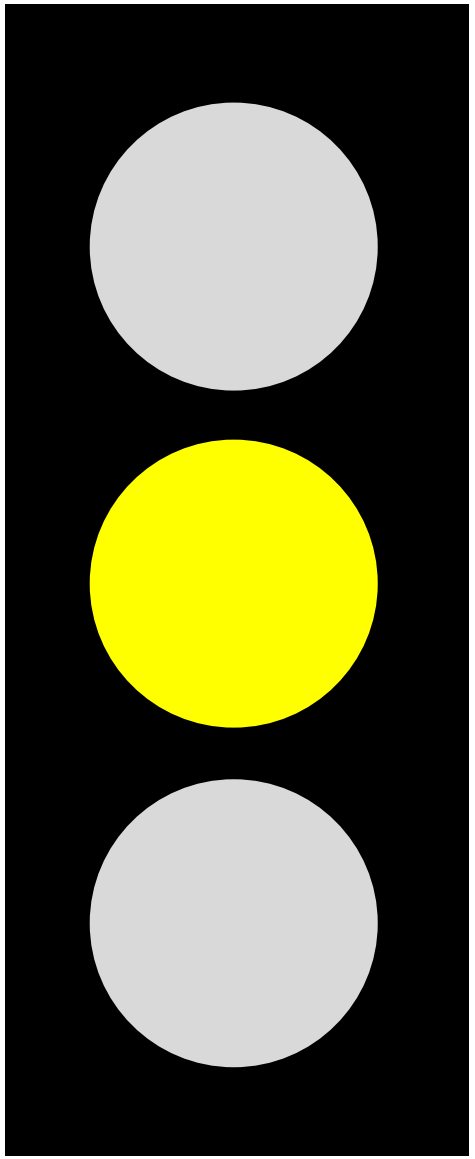
- User shops from home computer or with personal mobile device with an already registered username and password and orders an item from their favorites list.
- The online retailer grades this purchase as low risk because of the nature of the item, a known IP address or device associated with the customer, typical geolocation, and consistency with past patterns of online purchases.

OUTCOME: Completed purchase, MFA not activated



Repeat Customer, New Context

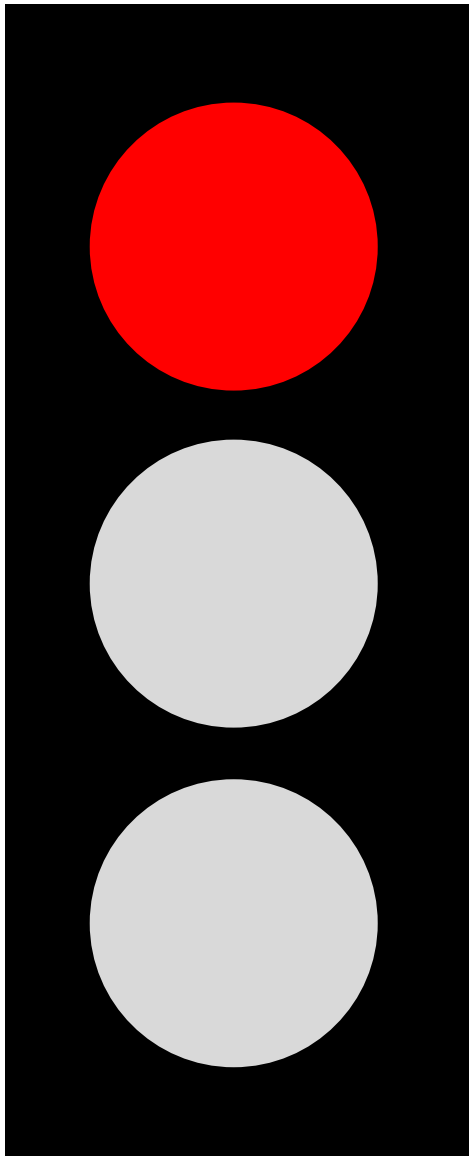
- User shops on work laptop or unknown mobile device with already registered username and password while travelling and browses several categories of expensive items before selecting one to purchase.
- User is prompted for additional authenticator.
- User successfully completes the transaction.
- The online retailer grades this purchase as moderate 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.



OUTCOME: MFA activated – successful authentication – completed purchase

Fraud Perpetrator Example

- User from a different network address range from the established consumer account location accesses the account.
- User does not browse and immediately adds an expensive item to their shopping cart.
- User selects stored payment information, but edits the shipping address to one not previously associated with consumer account.
- User is prompted for additional authenticator. After several failed attempts, the account is locked.
- The online retailer grades this purchase as high risk because of the user's device, behavior, IP address, geolocation, and shopping choices do not sufficiently align per the retailer's risk threshold.

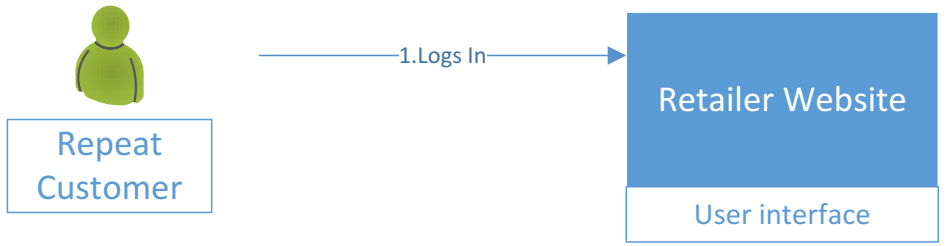


OUTCOME: MFA activated - unsuccessful authentication – purchase denied

Solution Component Walkthrough

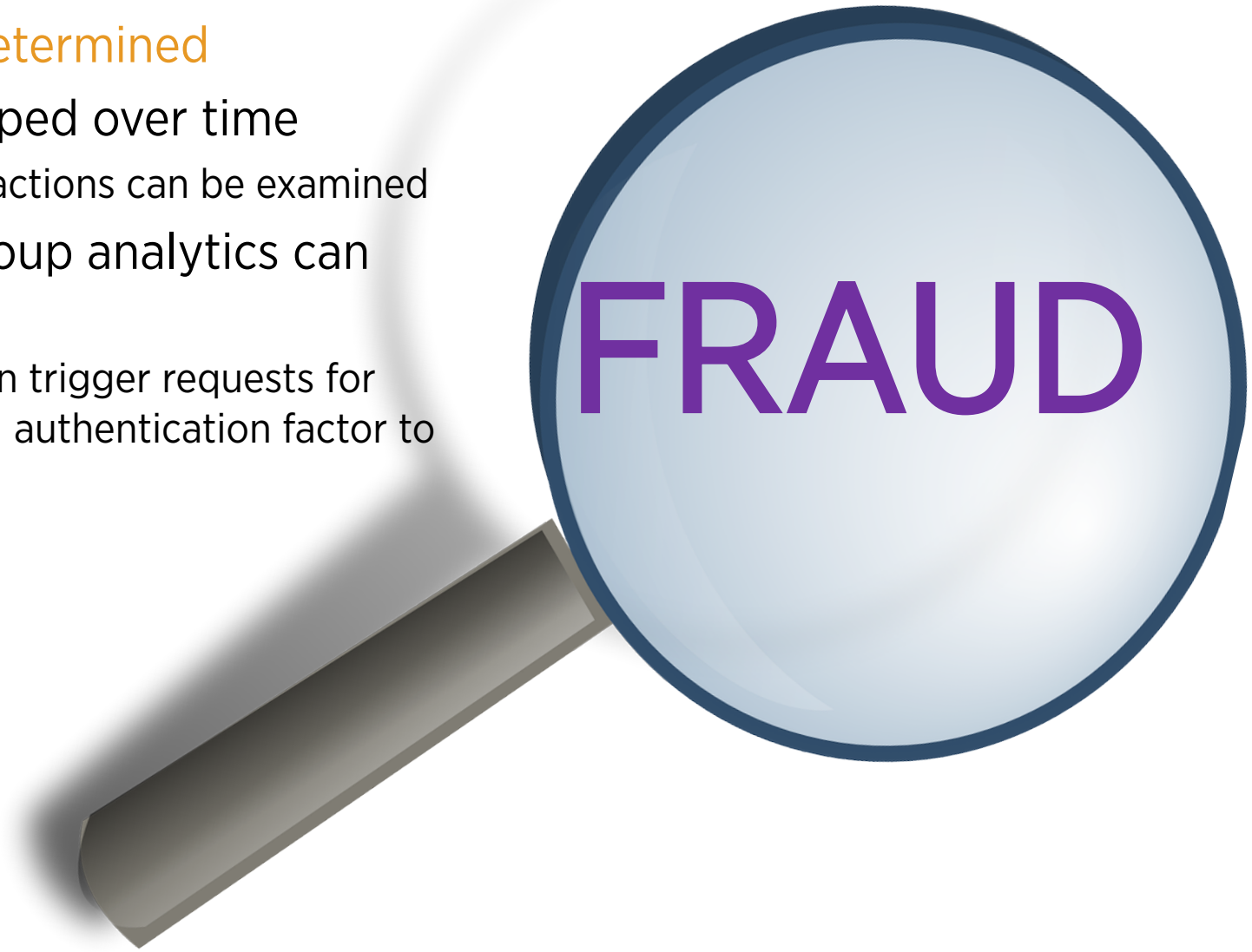
User and e-Commerce Platform Interaction

- Customer shops with e-Commerce platform
  - Either by visiting a retail website or using a mobile retail application
- Customer browses inventory, adds items to cart
  - Checks out with credit card
- Customer interaction information ingested by web analytics engine
  - Web analytics is a component of the overall risk engine
  - Information can be used to establish and recognize a baseline for legitimate customer interactions



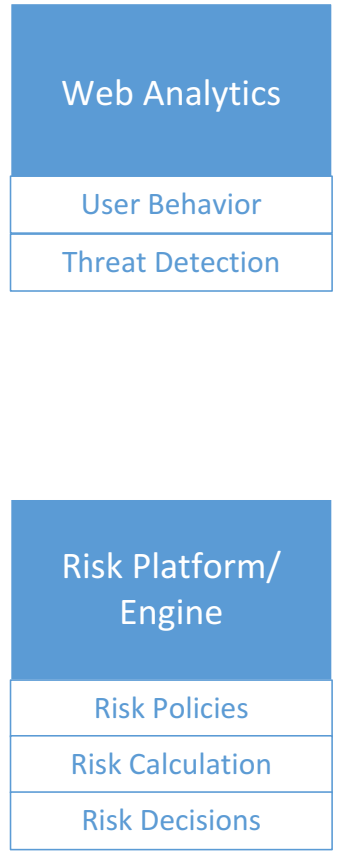
How Indicators of Fraud Can be Determined

- Patterns of fraud can be developed over time
  - Data from multiple customer interactions can be examined
- Behavior modeling and peer group analytics can assist retailers in finding threats
  - When threats are detected, this can trigger requests for customers to provide an additional authentication factor to complete a transaction



The Risk Engine provides risk management of the consumer's online shopping activities

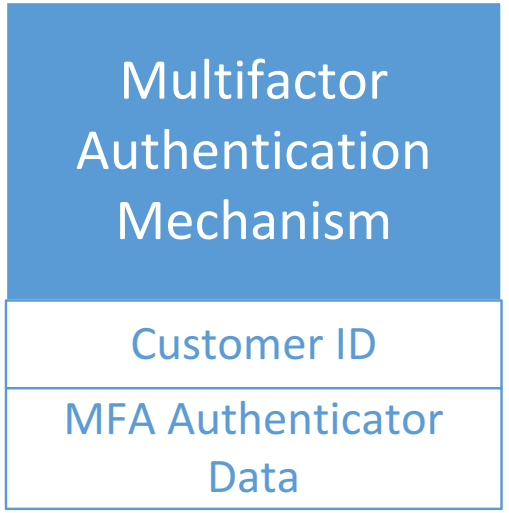
- The Risk Engine detects, analyzes, scores, and manages a consumer's online shopping activity
- Takes into account factors such as user behavior and device information to perform threat detection
- May include statistical models that can be used alongside a policy manager to calculate expected risk and make a risk-based authentication decision
- This will address fraud in a manner that supports a retailer's online e-Commerce risk tolerance
- Many consumer online purchases pass unhindered
- Only the transactions outside the retailer's risk tolerance level are asked for additional authentication



Multifactor Authentication Examples

After the risk engine identifies the existing customer's purchase as exceeding the retailer's risk policy, authentication factors such as the following may be employed:

- Look-up Secret
- Single-factor One-Time Password (OTP) Device
- Single-factor Cryptographic Software
- Single-factor Cryptographic Device



Standards and Best Practices

- EMVCo 3-D Secure 2.0
  - App and Browser-based Authentication Capability
    - Uses Frictionless Flow if a low risk transaction
    - Uses Challenge Flow if a high risk transaction
  - Includes analysis of Transaction Details

- FIDO U2F
  - Fast IDentity Online
    - Universal 2nd Factor
  - Standard for allowing devices to act as a 2nd Factor

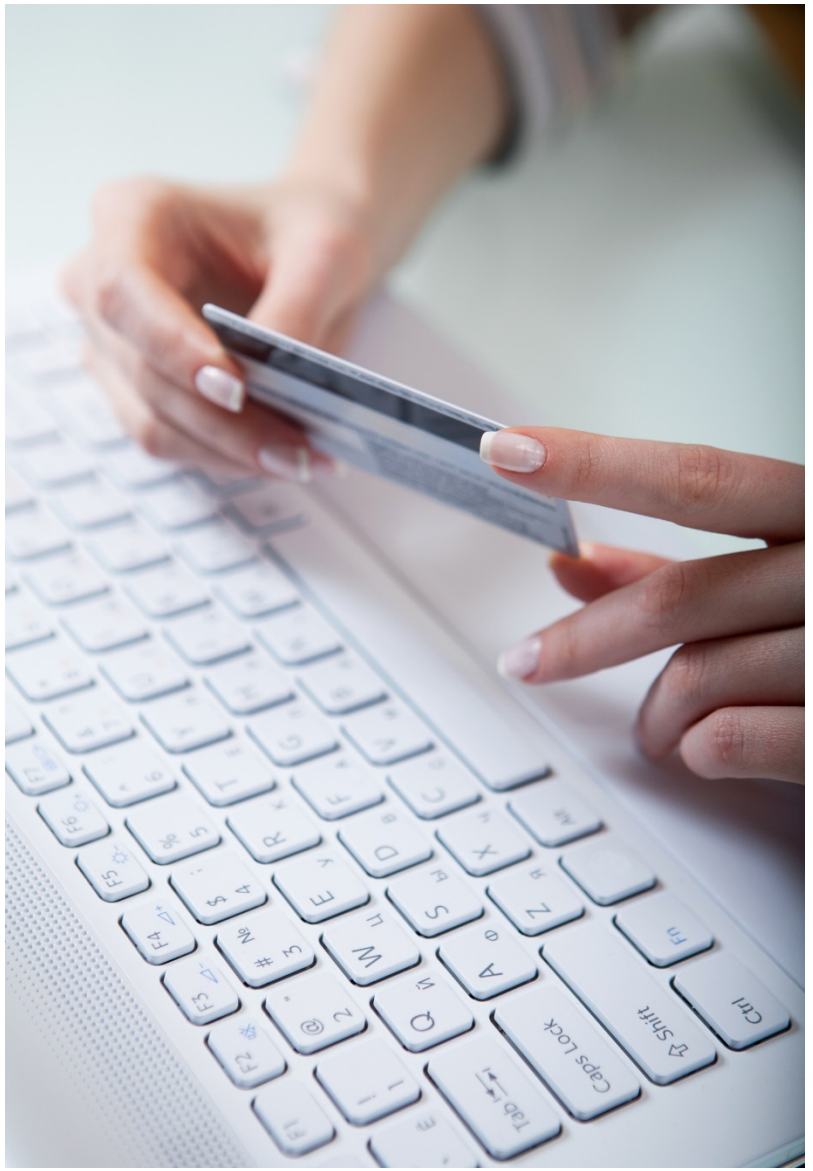
- NIST Special Publication 800-63-3 DRAFT
  - Digital Identity Guidelines

Primary Business Benefit

- Reduced risk of fraudulent CNP e-commerce transactions

Potential Other Business Benefits

- Increased level of security and assurance for CNP e-commerce transactions; increased consumer confidence
- Security alerts from web analytics and risk engine
- Ability to automate risk decisions to mitigate risks in real-time
- Ability to implement risk based multifactor authentication

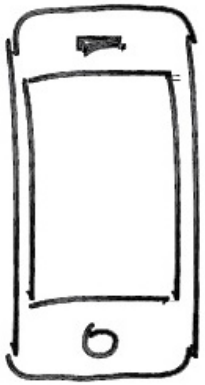


MULTIFACTOR AUTHENTICATION FOR E-COMMERCE: CURRENT STATUS

DEFINE + ARTICULATE	ORGANIZE + ENGAGE	IMPLEMENT + TEST	TRANSFER + LEARN
Describe the business problem	Partner with innovators	Build a reference design	Guide stronger practices
ACTION	**ACTION**	**ACTION**	**ACTION**
Identify and describe business problem	Publish project use cases and solicit responses	Build reference design	Collect documents
Conduct market research	Select partners and collaborators	Test reference design	Tech transfer
Vet project and use case descriptions	Sign CRADA	Identify gaps	Document lessons learned
OUTCOME	**OUTCOME**	**OUTCOME**	**OUTCOME**
Define business problems and project descriptions, refine into specific use case	Collaborate with partners from industry, government, academia and the IT community on reference design	Practical, usable, repeatable reference design that addresses the business problem	Set of all material necessary to implement and easily adopt the reference design

Join the Retail Community of Interest

Help the NCCoE retail team refine and produce the Multifactor for Authentication project with your feedback. New project ideas always welcome. Email consumer-nccoe@nist.gov to join.

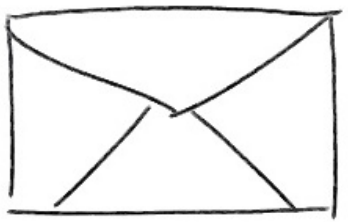


301-975-0200

consumer-nccoe@nist.gov

Participate

http://nccoe.nist.gov



100 Bureau Dr, M/S 2002
Gaithersburg, MD 20899