PROJECT DESCRIPTION

SECURING NON-CREDIT CARD, SENSITIVE CONSUMER DATA

Consumer Data Security 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 a result of payment card industry standards and a strong understanding of the value of valid credit card information in the black market, the retail industry has already invested in security mechanisms to protect credit card data, also referred to as cardholder data. However, this cardholder data is not the only valuable consumer information that is transmitted and stored by retailers. Other data that can be personally identifiable and is transmitted and stored in this ecosystem includes but is not limited to: consumer purchasing habits (including geographical locations, preferences, search history), date of birth, home or business address, phone number, email address, user id, password, IP addresses, and Social Security Number. As seen following high-profile data breaches in the healthcare sector, personally identifiable information (PII) is valued at up to 20 times more than credit card data, with a single credit card number sold at $1 and the average individual's PII sold at $20.[1]

In collaboration with stakeholders in the retail and commercial payment ecosystem, the NCCoE has identified that implementing data masking and tokenization, coupled with fine grained access control such as Attribute Based Access Control[2], may significantly improve the security of PII transmitted and stored during commercial payment transactions, as well as PII shared internally within a retail organization and externally with business partners. Building on this collaboration with the business community and vendors of cybersecurity solutions, the NCCoE will explore methods of effectively masking and tokenizing PII during commercial payment transactions and develop an example solution composed of open-source and commercially available components to address these real-world business challenges. This project will produce a NIST

Cybersecurity Practice Guide—a publically available description of the solution and practical steps needed to implement practices that more effectively secure the handling of non-credit card, sensitive consumer data.

KEYWORDS

retail; e-commerce; data masking; tokenization; access control; ABAC; attribute based access control; PII; consumer data

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 secure non-credit card, sensitive consumer data by utilizing standards-based commercially available and open source products. The project process includes identifying stakeholders who interact with retail systems and non-credit card consumer data; defining the interactions between the stakeholders, system, and data; identifying mitigating security technologies; and ultimately providing an example implementation.

Retailers easily gather sensitive data during typical business activities, which can be used by various internal users and external partners to accelerate business operations, improve consumer shopping experience, and increase revenue opportunities. There has been an increase in the value of non-credit card, sensitive consumer data on the black market and relatively few regulations or standards specific to this topic in the consumer-facing/retail industry in the United States. Some regulations and standards have emerged or are emerging in Europe and other parts of the world around privacy and protecting personally identifiable information (PII), and those precedents can inform our work in this space. There remains a gap to be filled in terms of understanding the risks and implementing security controls to mitigate those risks concerning non-credit card, sensitive consumer data.

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. 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 the community consider practices that should improve the security environment surrounding protecting non-credit card, sensitive consumer data.

Scope

The scope of this example solution includes the implementation of data masking and tokenization mechanisms for non-credit card, sensitive consumer data during commercial payment transactions both via point-of-sale (POS) and e-commerce transactions, along with fine grained attribute based access control (ABAC) for users both inside and outside an organization. A layered approach to data security including point-to-point encryption (P2PE) is generally advisable.

Assumptions

This example solution of securing non-credit card, sensitive consumer data will provide security benefits including reduced risk of data breach and an increased confidence and trust between the consumer and retailer. The benefits of using a solution that protects

non-credit card, sensitive consumer data will outweigh any additional 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 the build or any of its components already have in place some degree of system and network security. Therefore, we focused on the effort of implementing fine-grained access control, tokenization, and data masking. The goal of this solution is to not introduce additional vulnerabilities into existing systems.

Background

The NCCoE, working with consumer-facing and retail organizations and 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 solution that protects non-credit card, sensitive consumer data. The need arises from the recognition that the value of this data is now significantly higher than credit card data on the black market, in addition to potential value for the purposes of extortion or reputational embarrassment depending on the details of the data, and thus is a higher value target for malicious actors. Also, with the general trend of widespread digital collaboration inside and outside an organization, various stakeholders need varying levels of access to the same and different resources. The NCCoE held a workshop to identify key issues that affect securing non-credit card, sensitive consumer data. The conversations held and insight derived from that workshop have informed the direction of this project and this Project Description.

2. Scenarios

The scenarios described here provide high-level context for this challenge and inform the high-level architecture. Continued work on this project will result in a NIST Cybersecurity Practice Guide, Special Publication Series 1800, which will detail how noted security mechanisms are implemented.

Scenario 1: Access to sensitive data inside an organization

A new customer is signing up for the loyalty program of a brick-and-mortar retailer that also has an e-commerce website. At the Customer Service desk, the user is asked to enter the following data in order to register: name, address, email address, phone number, and date of birth. After the user enters his information, he receives a physical loyalty card that provides benefits including discounts both in-store and online. The user shops in the store during the day, and then logs into the website in the evening to purchase a few more items.

In the background, at the point of capture in-store, the retailer has tokenized the cardholder data as required by PCI DSS standards during the payment transaction, but has also tokenized and data masked the non-credit card sensitive PII gathered during account registration and during the shopping trip online. The tokens are secured but accessible to parties with need-to-know access rights, while the actual raw data is

stored in a highly secure data store. Subsequent access requests from within the retailer's organization for the tokens or actual data are evaluated according to access control policies that correlate to the organization's business rules and relevant standards and regulations. In some cases, access to the non-credit card, sensitive data may be granted, but in many cases the token itself can be used in place of the actual data, such as internal business functions including returns, sales reports, marketing analysis, and recurring payments. Employees in sales, marketing, and order management and fulfillment departments are all granted access to the tokens when there is a verified need-to-know access request, but not the actual data. Customer service employees are granted access to the actual data when there is a verified need-to-know request, but with other sensitive data masked.

Scenario 2: Access to sensitive data outside an organization

The retailer has decided to outsource its marketing analysis to a consulting company and its order fulfillment to a fulfillment house, both of whom frequently need access to some consumer data. Similar to the above scenario, all cardholder and non-cardholder, sensitive PII data are tokenized and the actual data is stored in a highly secure data store.

A marketing analyst outside the organization has been assigned a project related to long-standing customers and shopping patterns over time. The analyst requests access to the purchasing habits data of the retailer's long-standing customers. Instead of access to actual or masked data, the analyst is granted access to the tokens, which can still be used for the project at hand.

Similarly, when a retailer receives an online order, a fulfillment request is sent over as a token to the fulfillment house. The fulfillment house must use the token to access the real data in order to access the customer's shipping address and ship the order.

3. High-Level Architecture of Scenario 2

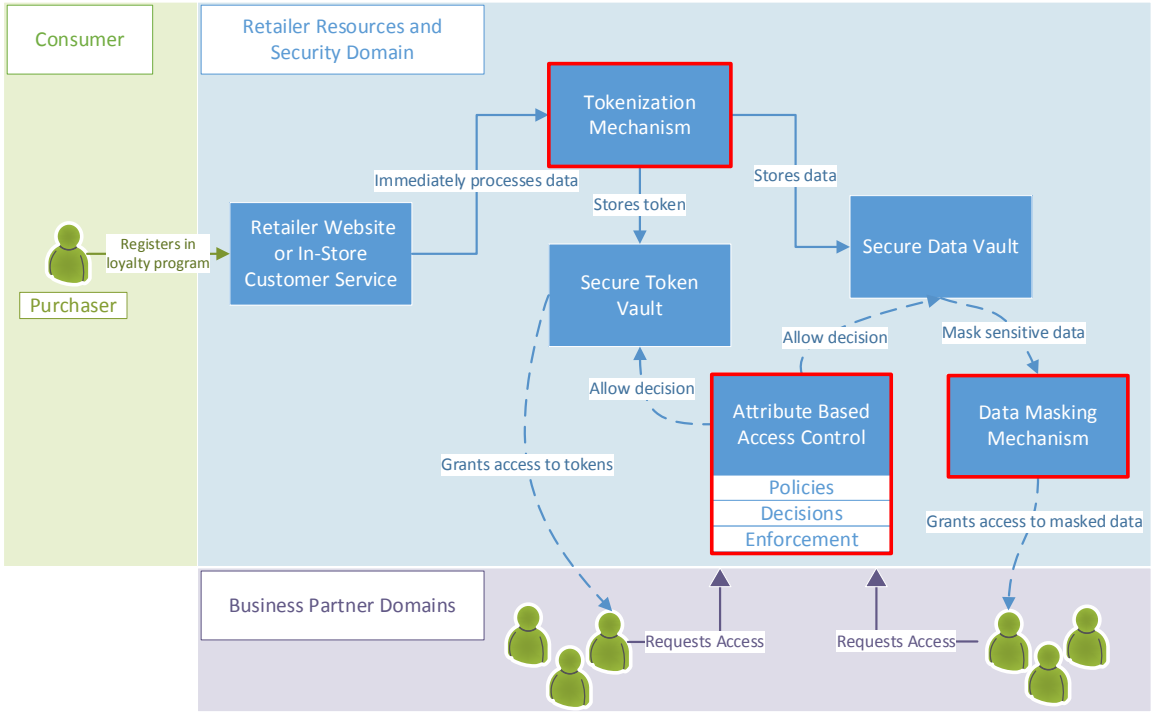

Diagram 1: High-level Architecture Illustrating Scenario 2

Component List

A solution for securing non-credit card, sensitive consumer data includes but is not limited to the following components:

- Online retail website or simulated customer service portal with loyalty program registration
- Tokenization mechanism
- Secure data store for tokens
- Secure data vault for actual data
- Data masking mechanism
- Attribute Based Access Control (ABAC) platform
    a. Policies
    b. Decision making
    c. Decision enforcement

Desired Requirements

- Data tokenization and token management
    - Token generation

- Token mapping
- Non-credit card, sensitive consumer data vault
- Cryptographic key management

- Data masking
- Fine-grained Attribute Based Access Control (ABAC) for internal and external users
  - Automated logging of access requests and decisions
  - Access control policy creation
  - Determining access control decisions based on policies
  - Access control policy enforcement

4. Relevant Standards and Guidance

- American Institute of CPAs, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)

  https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCGuidesandPublications.aspx
- European Parliament/Legislative Observatory, European Commission, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- 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 27018, Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
- 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 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.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
Data vaults	PR.DS-1 PR.DS-3	**NIST SP 800-53 Rev. 4** SC-28; CM-8, MP-6, PE-16 **ISO/IEC 27001:2013** 7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3
Cryptographic key management	PR.DS-1 PR.DS-2	**NIST SP 800-53 Rev. 4** SC-28, SC-8 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.1.2, A.13.2.3, A.14.1.2, A.14.1.3
Data masking	PR.DS-1	**NIST SP 800-53 Rev. 4** SC-28; CM-8, MP-6, PE-16 **ISO/IEC 27001:2013** 7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3
Automated logging	PR.PT-1	**NIST SP 800-53 Rev. 4** AU Family, IR-5, IR-6 **ISO/IEC 27001:2013** 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/IEC 27001:2013** 7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3
Access control	PR.PT-3	**NIST SP 800-53 Rev. 4** AC-3, CM-7 **ISO/IEC 27001:2013** A.9.1.2

Table 1: Security Control Map

Appendix A – References

[1] Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security Survey 2015, September 30, 2014, PricewaterhouseCoopers, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[2] NIST Cybersecurity Practice Guide, SP-1800-3: "Attribute Based Access Control," NIST, https://nccoe.nist.gov/library/nist-sp-1800-3-attribute-based-access-control-practice-guide

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

[4] EMV Payment Tokenisation Specification – Technical Framework, Version 1.0, March 2013, EMVCo, LLC, https://www.emvco.com/specifications.aspx?id=263

[5] EMV and Encryption + Tokenization: A Layered Approach to Security, A First Data White Paper, 2012, First Data, http://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF

[6] What Every Card Not Present Merchant Should Know, Navigating Today's Challenging Payments Ecosystem, 2014, Verifi Inc, http://www.verifi.com/wp-content/uploads/2014/05/Verifi_eBook_web_noCNP.pdf

[7] Visa Best Practices for Tokenization Version 1.0, July 14, 2010, Visa Inc, https://www.visa-asia.com/ap/sg/merchants/include/ais_bp_tokenization.pdf

[8] Information Supplement: PCI DSS Tokenization Guidelines Version 2.0, August 2011, Scoping SIG, Tokenization Taskforce, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

[9] Tokenization Product Security Guidelines – Irreversible and Reversible Tokens Version 1.0, April 2015, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

[10] Implement Data Masking to Protect Sensitive Data: Part 1, January 5, 2015, Biswajit Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-masking-protect-sensitive-data-part-1

[11] Implement Data Masking to Protect Sensitive Data: Part 2, January 9, 2015, Biswajit Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-masking-protect-sensitive-data-part-2

[12] Data Masking Best Practice, an Oracle White Paper, June 2013, Oracle Corporation, http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf

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

173