PROJECT DESCRIPTION

SECURING PROPERTY MANAGEMENT SYSTEMS

Cybersecurity for the Hospitality Sector

William Newhouse
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Sarah Weeks
The MITRE Corporation

DRAFT
April 28, 2017
consumer-nccoe@nist.gov

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries or broad, cross-sector technology challenges. Working with technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

This document describes a particular problem that is relevant across the hospitality sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the hospitality sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by hotels and other hospitality organizations.

ABSTRACT

Hospitality organizations rely on Property Management Systems (PMS) for daily tasks, planning, and record keeping. As the operations hub, the PMS interfaces with several services and components within a hotel's IT system, such as Point-of-Sale (POS) systems, door locks, Wi-Fi networks, and other guest service applications. Adding to the complexity of connections, external business partners' components and services are also typically connected to the PMS, such as on-premise spas or restaurants, online travel agents, and customer relationship management partners or applications (on-premise or cloud-based). [1] The numerous connections to and users of the PMS could provide a broader surface for attack by malicious actors. [2] Demonstrating methods to improve the security of the PMS can help protect the business from network intrusions that might lead to data breaches and fraud. [3]

Based on industry research and in collaboration with hospitality industry stakeholders, the NCCoE is starting a project that aims to help hospitality organizations implement stronger security measures within and around the PMS, with a focus on the POS system through network segmentation, point-to-point encryption, data tokenization, multifactor authentication for remote and partner access, network and user behavior analytics, and business-only usage restrictions.

In collaboration with the hospitality business community and technology vendors who implement standards that improve cybersecurity, the NCCoE will explore methods to strengthen the security of the PMS and its connections and will develop an example implementation composed of open-source and commercially available components. This

project will produce a NIST Cybersecurity Practice Guide—a freely available description of the solution and practical steps needed to effectively secure the PMS and its many connections within the hotel IT system.

KEYWORDS

Behavior analytics; hospitality cybersecurity; multifactor authentication; network analytics; point of sale; point-to-point encryption; property management system; tokenization

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/library.

Comments on this publication may be submitted to: consumer-nccoe@nist.gov

Public comment period: April 28, 2017 to May 31, 2017

Table of Contents

1. Executive Summary

Purpose

The purpose of this project is to help hoteliers implement stronger security measures within and around their Property Management Systems (PMS), with a focus on the connection to a point-of-sale (POS) system. The project will identify typical hotel IT infrastructures and PMS-POS configurations, systems, and components that typically integrate or interface with both applications, and interactions between hoteliers and third-party service provider (SP) systems (e.g., online booking or customer relationship marketing partners). The project will identify security-mitigation technologies and provide an example implementation.

The publication of this Project Description is the beginning of a process that will identify project participants, as well as standards-based, commercially available, and/or open- source hardware and software components. These products will be integrated and implemented in a laboratory environment to build open, standards-based, modular, end-to-end reference designs that will address the security challenges introduced by networking the PMS and POS. The approach may include architectural definition, logical design, build development, security character analysis, test and evaluation, security control mapping, and future build considerations. The output of the process will be the publication of a multi-volume NIST Cybersecurity Practice Guide that will help hoteliers implement stronger PMS-POS security.

Scope

The scope of this example solution includes the implementation of point-to-point encryption (P2PE), data tokenization, multifactor authentication for remote and partner access, access control, network and user behavior analytics, and business-only usage restrictions on the PMS and POS. For this project, the security controls implemented within third-party SP applications are out of scope; however, their interface and connection to the PMS-POS systems are in the project's scope.

Assumptions

A reference design for securing PMS can provide numerous security benefits, including reduced risk of network intrusion and data breach, and associated financial and reputational costs. The NCCoE understands that a hospitality business would weigh the cost of investment in a PMS-POS security solution with its potential benefits.

Background

The NCCoE, working with hospitality organizations such as the American Hotel & Lodging Association and Hotel Technology Next Generation (HTNG), identified the need for an example implementation to improve connections to and from the POS and PMS, and other integrated services and components. The NCCoE participated in HTNG's North American Insight Summit in August 2016 to discuss this project and solicit input from stakeholders that were incorporated into shaping this effort.

2. SCENARIOS

Scenario 1: Guest checks in, dines on-premise – Tokenization, P2PE, Network and User Analytics

A guest checks in at the front desk, and the hotel clerk logs in to the PMS. The clerk checks the guest's identification and finds that she is a member of the hotel's loyalty program. The clerk finds an available room in the PMS, reserves the room, and swipes the guest's credit card for incidentals. This process takes only a few minutes, after which the guest leaves for her room. The hotel clerk logs out of the PMS and/or locks the computer.

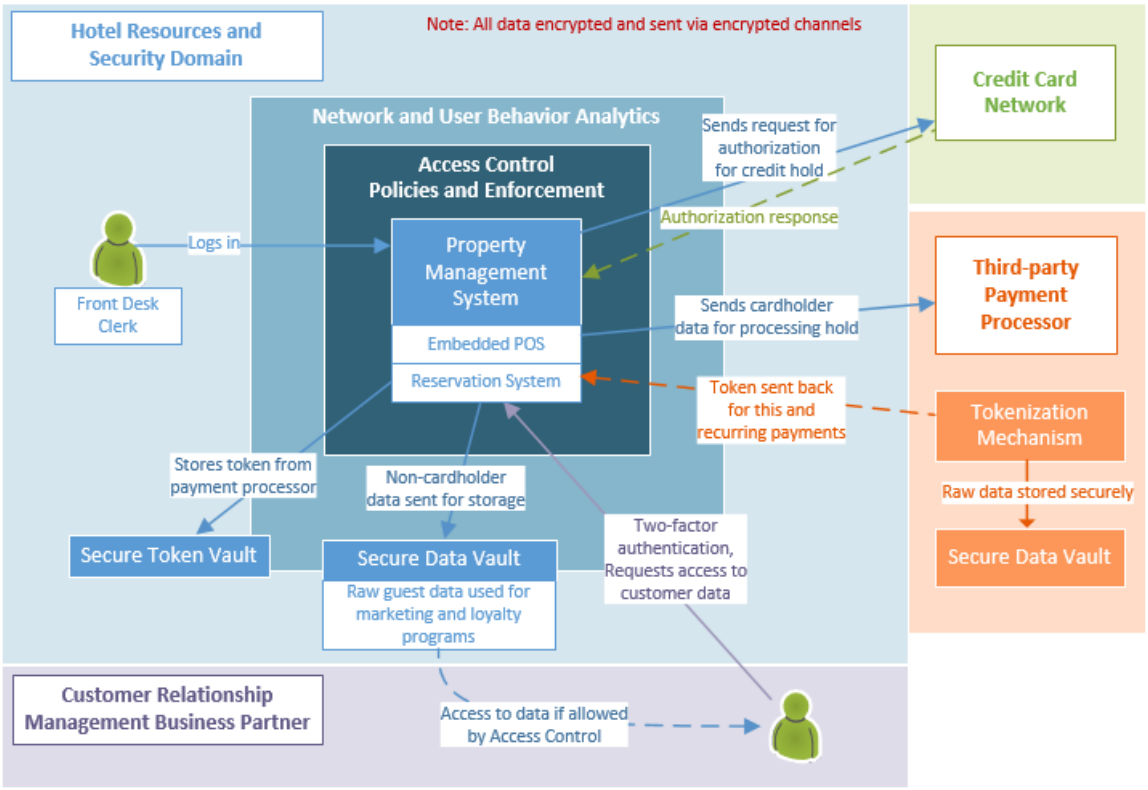
In the background, the guest's payment information is tokenized, such that after a transaction authorization is returned from the credit card network, a trusted third party stores all the actual cardholder data (defined by the Payment Card Industry Data Security Standard as cardholder name, primary account number, and expiration date) and issues tokens, which are stored in the hotel's system. The hotel's system can then use that token for recurring charges, as well as for the loyalty program. Any other non-payment data pertaining to the guest is encrypted and sent through encrypted channels to be stored in the hotel's own databases or at the hotel's third-party trusted SPs. Furthermore, the hotel's monitoring and analytics system produced no alerts or warnings because the hotel clerk's activity within the PMS is consistent with a baseline, following a typical check-in process with no deviation, and the computer hosting the PMS was used exclusively for business purposes.

Scenario 2: Third-party service provider remotely accesses hotel system – Multifactor Authentication, Access Control, Network and User Analytics

A third-party SP needs remote access to one of the hotel system's components. The SP user remotely connects and begins authentication with a username and password. To complete the authentication process, the SP user must provide a second authenticator. The hotel system verifies the identity of the SP user with multifactor authentication and allows the authenticated user to access certain resources. The hotel's analytics component produces no alerts or warnings because the SP user's second authenticator was valid, his activity is consistent with a baseline, and no unusual network or user activity was detected.

3. High-Level Architecture

Diagram 1: High-level Architecture



Component List

To better secure the PMS, an example solution may include, but is not limited to, the following components:

- PMS and POS system(s)
- P2PE
- Data tokenization
- Multifactor authentication mechanism
- Access control platform
- Network and user behavior analytics
- Data logging
- Data storage

Desired Requirements

- Automated network and user behavior analytics
- P2PE
- Data tokenization and token management

158 - Token generation
159 - Token mapping
160 - Non-credit card, sensitive consumer data vault
161 - Cryptographic key management
162 • Multifactor authentication for remote and third-party access
163 • Access control for internal and third-party users
164 - Automated logging of access requests and decisions
165 - Access control policy creation
166 - Determining access control decisions based on policies
167 - Access control policy enforcement
168 • Automated logging of analytics and component interactions

169 ## 4. Relevant Standards

170 • American Institute of CPAs, Reporting on Controls at a Service Organization Relevant to
171 Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)
172 https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCGuides
173 andPublications.aspx
174 • Hotel Technology Next Generation, Secure Payments Framework for Hospitality, Version
175 1.0, February 2013, https://c.ymcdn.com/sites/htng.site-
176 ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-
177 27CFDD77E17B/HTNG_Secure_Payments_Framework_v1.0_FINAL.pdf
178 • ISO/IEC 27001, Information Technology – Security Techniques – Information Security
179 Management Systems https://www.iso.org/isoiec-27001-information-security.html
180 • ISO/IEC 27018, Information technology -- Security techniques -- Code of practice for
181 protection of personally identifiable information (PII) in public clouds acting as PII
182 processors https://www.iso.org/standard/61498.html
183 http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
184 • ISO/IEC 29146, Information Technology – Security techniques – A framework for access
185 management, https://www.iso.org/obp/ui/#iso:std:iso-iec:29146:ed-1:v1:en
186 • NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote
187 the protection of critical infrastructure
188 http://www.nist.gov/itl/cyberframework.cfm
189 • NIST SP 800-53, Recommended Security Controls for Federal Information Systems
190 http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
191 • NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable
192 Information (PII) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-
193 122.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.

Table 1: Security Control Map

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 user and network 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
Secure 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
Access control	PR.PT-3	**NIST SP 800-53 Rev. 4** AC-3, CM-7 **ISO/IEC 27001:2013** A.9.1.2
Point-to-point encryption	PR.DS-1, PR.DS-2, PR.DS-5, PR.PT-4	**NIST SP 800-53 Rev. 4** AC-20, AU-9, IA-6, IA-7, MP-6, SA-13, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12 **ISO/IEC 27001:2013** 6.2.1, 9.4.3, 9.4.4, 9.4.5, 10.1.2, 12.4.2, 12.4.3, 13.1.1, 13.2.1, 13.2.3, 14.1.3

APPENDIX A REFERENCES

[1] "Hotel Property Management System Interfaces," Atrio, Feb 16, 2016, http://www.atrio.com/hotel-property-management-system-interfaces/

[2] *2015 Data Breach Investigations Report: Hospitality*, Verizon http://www.verizonenterprise.com/resources/reports/rp_dbir-hospitality-2015_en_xg.pdf [accessed 4/11/17]

[3] *Secure Payments Framework for Hospitality*, Hotel Technology Next Generation, Version 1.0, February 2013, https://c.ymcdn.com/sites/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/HTNG_Secure_Payments_Framework_v1.0_FINAL.pdf