PROJECT DESCRIPTION

SECURING PROPERTY MANAGEMENT SYSTEMS

Cybersecurity for the Hospitality Sector

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

Michael Ekstrom
Jeff Finke
Sarah Weeks
The MITRE Corporation

September 13, 2017
hospitality-nccoe@nist.gov

This revision incorporates comments from the public.

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. 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 (MFA) 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; MFA; network analytics; network segmentation; point of sale; point-to-point encryption; property management system; tokenization

Disclaimer

Certain commercial entities, equipment, products, 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, equipment, products, or materials are necessarily the best available for the purpose.

CONTENTS

1 EXECUTIVE SUMMARY

Purpose

The purpose of this project is to help hoteliers implement stronger security measures and reduce vulnerabilities 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 integrate or interface with both applications. The project will also identify interactions between hoteliers and authorized third-party service provider (SP) systems (e.g., online booking or customer relationship marketing partners).

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, 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, MFA for remote and partner access, risk calculation, access control (it is assumed that, at a minimum, users will be authenticated with login and password), network and user behavior analytics, and business-only usage restrictions on the PMS and POS. Strong cybersecurity measures such as irreversible tokens (both authenticatable and non-authenticatable), cryptographic tokens, etc., will be analyzed and trade-offs considered. Further protection of the confidentiality and integrity of the data via strong measure such as network segmentation, zero-trust, etc., will be analyzed in the lab builds and trade-offs examined. Other hotel features such as check-in kiosks, business centers, guest telephone systems that interface with the PMS will also be considered in the lab builds.

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, accrues incidentals – 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 they are 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 only takes a few minutes, after which the guest leaves for their 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 when the guest accrues incidental(s) e.g. mini-bar usage, phone usage, room service, etc., 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 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.

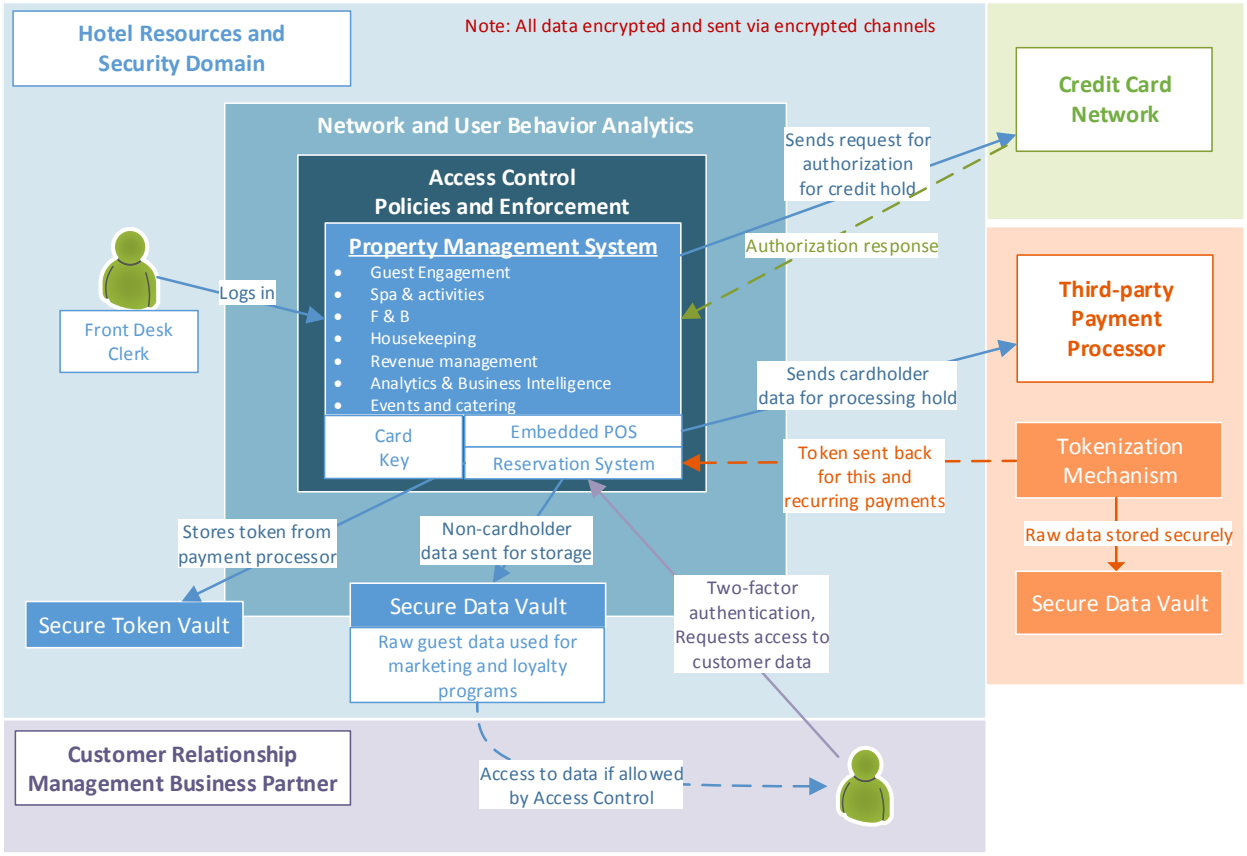
Scenario 2: Third-party service provider remotely accesses hotel system – Multifactor Authentication, Access Control, Network and User Analytics

An authorized third-party SP needs remote access to one of the hotel system's components. The SP user remotely connects and begins authentication via MFA. The hotel authenticates the identity of the SP user and allows the authenticated user to access certain resources. The hotel's analytics component should log this access, as 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

Figure 1 identifies a high-level architecture of the PMS and associated systems that are in use for most hotels. During the development of the laboratory environment implementing the use case, the figure will be refined to describe detailed components and mapped to the physical architecture in the lab environment for the specific scenario being implemented. A goal of this figure is to help spur identification of project participants and hardware and software components for collaborative use in a laboratory environment to build open, standards-based, modular, end-to-end reference designs.

Figure 1: High-level Architecture



Authentication is defined as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources" by NIST SP 800-63-3 "Digital Identity Guidelines." [4] Authenticating an identity establishes a subject as who they claim to be. Successful authentication requires that the claimant prove possession and control of the authenticator via an authentication process. Authentication establishes confidence that the claimant has possession of an authenticator(s) bound to the credential, and in some cases in the attribute values of the subscriber. Successful authentication provides reasonable risk-based assurances that the subject accessing the system today is the same as that which previously accessed the service.

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)
- Point-to-Point Encryption (P2PE)
- Data tokenization
- Multifactor authentication mechanism
- Access control platform
- Network and user behavior analytics
- Data logging
- Data storage
- Virtualization

Desired Characteristics

Auditing and Analytics capabilities such as:

- Complete, real-time auditing and reporting of user activity, including:
    - User behavior analytics
    - Unauthorized access
    - Unauthorized user behavior
    - Access requests and decisions
- Automated detection and/or response to incidents
- Continuous monitoring and retention of network events
- Continuous monitoring and retention of information on component Interactions

System Protection and Authentication capabilities with enforcement. These capabilities will help prevent damage to PMS functionality and security, and include:

- Multifactor Authentication for remote and third-party access
- Access control for internal and third-party users, including:
    - Access control policy creation
    - Determination of access control decisions based on policies
    - Access control policy enforcement
- Adherence to principles of segmentation and zero-trust, including:
    - Multiple trust zones and logical trust boundaries
    - Network segmentation gateways
    - Network virtualization platform and micro-segmentation

Data Protection and Encryption capabilities to prevent damage to PCI/PII confidentiality, as well as the confidentiality and integrity of system data. These capabilities will meet or exceed hospitality industry best practices for privacy, and include:

- Point-to-point encryption (P2PE)
- Limited/no storing/processing/transmission of payment card data
- Secure data tokenization and token management capabilities, including:

    - Token generation
    - Token mapping
    - Cryptographic key management
- Utilization of a non-PCI, sensitive consumer secure data vault
- Prevention of damage to PCI/PII confidentiality
- Prevention of damage to PMS functionality and security, and improved mitigation of cybersecurity risks
- Secure Payment Terminal
- Payment Information Proxy service

4 Relevant Standards

- 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
- Hotel Technology Next Generation, Secure Payments Framework for Hospitality, 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
- ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems https://www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27018, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors https://www.iso.org/standard/61498.html

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
- ISO/IEC 29146, Information Technology – Security techniques – A framework for access management, https://www.iso.org/obp/ui/#iso:std:iso-iec:29146:ed-1:v1:en
- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure https://www.nist.gov/cyberframework
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
- NIST SP 800-63-3, Digital Identity Guidelines http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2, April 2016, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

5 Security Control Map

Table 1 maps the characteristics of the applicable standards and best practices described in the NIST Cybersecurity Framework for Critical Infrastructure (NIST 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 **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 [accessed 4/11/17]

[4] *NIST 800-63-3 Digital Identity Guidelines*, National Institute of Standards and Technology, June 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf [accessed 8/25/17]