NIST SPECIAL PUBLICATION 1800-27A

Securing Property Management Systems

Volume A:
Executive Summary

William Newhouse
Information Technology Laboratory
National Institute of Standards and Technology

Michael Ekstrom
Jeff Finke
Marisa Harriston
The MITRE Corporation
McLean, Virginia

March 2021

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-27

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

In recent years criminals and other attackers have compromised the networks of several major hotel chains, exposing the information of hundreds of millions of guests. Breaches like these can result in huge financial loss, operational disruption, and reputational harm, along with lengthy regulatory investigations and litigation. Hospitality organizations can reduce the likelihood of a hotel data breach by strengthening the cybersecurity of their property management system (PMS). The PMS is an attractive target for attackers because it serves as the information technology (IT) operations and data management hub of a hotel. This cybersecurity practice guide shows an approach to securing a PMS and the system of guest services it supports. It offers how-to guidance for building a reference design using commercially available products within a zero trust architecture to mitigate cybersecurity risk that includes role-based access control, privileged access management, network segmentation, moving target defense, and data protection.

CHALLENGE

Hospitality organizations rely on a 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 systems, such as point-of-sale (POS) systems, physical access control systems, Wi-Fi networks, and other guest service applications. A PMS and its extended systems store, process, and transmit a variety of sensitive guest information, including payment card information and personally identifiable information. An unsecured or poorly secured PMS could expose a hotel–and the larger hospitality organization of which the hotel is a part–to a significant and costly data breach, which may result in financial penalties for violating state, federal, and international privacy and other regulatory regimes.

> ***An unsecured or poorly secured PMS*** *could expose a hotel—and the larger hospitality organization of which the hotel is a part—to a significant and costly data breach…*

This practice guide can help your organization:

- **increase overall PMS security** situational awareness and limit exposure of the PMS to incidents in systems that interface with it
- **control and limit access** to your PMS to those with a business need
- **instill consumer confidence and brand loyalty** by protecting guest privacy and payment card information
- **decrease breach potential and data exfiltration** by limiting lateral movement, thus decreasing organizational risk
- **build the business case,** functional requirements, and test plan for a similar solution within your own environment
- **support privacy/regulatory compliance** by using data tokenization and limiting the spread of data beyond need-to-know

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

SOLUTION

The National Cybersecurity Center of Excellence (NCCoE) collaborated with the hospitality business community and cybersecurity technology providers to build a PMS reference design that simulates a hotel's IT infrastructure, including guest Wi-Fi and a PMS integrated with a POS module and an electronic door lock system. Using commercially available products, the reference design shows how to protect data moving within this environment and how to limit or prevent user access to the various systems and services.

The reference design uses technologies and security capabilities (shown below) from our project collaborators. All technologies used in the solution support security standards and guidelines of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Hospitality Technology Next Generation, and the Payment Card Industry (PCI) Security Standards Council, among others. The reference design aligns with the privacy protection activities and desired outcomes of the *NIST Privacy Framework*.

Collaborator	Security Capability or Component
CRYPTONITE NXT™	Network protection appliance that provides an additional layer of protection against cyber attacks
<) FORESCOUT.	Visualizes the diverse types of devices connected to the network; enforces policy-based controls
HÄFELE	Physical access control system, including door locks, room key encoding, and management
Remediant	Real-time incident monitoring and detection, privilege escalation management, and reporting functions
STRONGKEY	Payment solution appliance that secures credit card transactions and shrinks the PCI compliance enclave
tdi technologies	Access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers, can use this part of the guide, NIST SP 1800-27A: *Executive Summary,* to understand the impetus for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use NIST SP 1800-27B: *Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of NIST SP 1800-27C: *How-To Guides*, which provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hospitality-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.