

Case study: Working together to protect guest data

Delaware North and PAR Springer-Miller are collaborating to implement an HTNG workgroup standard for encrypting and transmitting guests' personal financial data.

Announcements from Fortune 500 companies regarding a breach of their data communication systems have become so regular that today's consumers are no longer shocked. What was once an alarming notification that triggered financial panic has become almost commonplace. But just because data breaches are occurring more frequently does not belittle the effect of their consequences. Data breaches today are a real and present danger, and to this point it seems we've been unable to slow them down.

The fragmentation of the hotel industry—which collects guest credit card information on more than a billion transactions a year—has made hotels an easy and high-profile target. Personal information collected by one supplier's hardware may be sent through another supplier's system before being stored in a third supplier's database. Therefore, over the past few years, various system providers have come together to make guest privacy and data security top priorities.

One particular example is currently underway. Delaware North, which owns or operates 20 hotels and resorts, is working with several of its technology providers to identify a standard code by which personal guest data will be transmitted and stored. The following case study outlines the business problem and the end goal, with specifics on how the goal will be accomplished and details on the players involved in solving one of today's trickiest challenges.

Business problem: Erase gaps in data security

- Breaches cast hotels in negative light
- Why hotels are an easy target
- Various systems must interpret the same data

The hotel industry is a prime target for hackers looking to gain access to sensitive personal data. In the past five years, the industry has seen cyber criminals steal customer or employee personal information, including credit card account numbers, bank account codes, social security numbers, e-mail addresses and other items useful in carrying out identity theft.

Why are hotels targeted? A few reasons: Hotels transact a large amount of business through credit and debit card swipes, and payment card fraud is a common type of identity theft. Because hotels must transmit data across multiple systems—often times from the individual hotel to the credit-card processor to the management company to the hotel brand and back—the data needs to be read and understood by

each of those systems, and therefore encrypting the data provides communication challenges.

For example, when Joe Smith checks in to his hotel, his credit card is commonly swiped at a front desk kiosk so that Mr. Smith can be charged for any incidentals at the end of his stay. His card is authorized and the personal data from his card needs to be stored in the property management system so it can be charged later if need be. If the front desk kiosk and the PMS are not operating under the same standard, that information is not easily encrypted and can be open and available to outside parties, including hackers.

Solution in progress

- HTNG promotes collaboration
- Tokenization is the first step
- Future standards will be available to everyone

To best tackle the problem, Delaware North and its technology providers are working extensively with Hotel Technology Next Generation, a global trade association made up of hotel IT executives that fosters collaboration among hoteliers and technology providers. In 2010, HTNG developed a workgroup centered on creating a payment integration standard between a hotel's property management system and its payment gateway. Many PMS providers will be affected, but Delaware North is working predominantly with Stowe, Vermont-based PAR Springer-Miller Systems, supplier of the ATRIO® and ^{SMS}|Host property management software solutions, which is also well represented in HTNG's payment standard workgroup.

Both the hotel managers and software providers are working together to define what data needs to be exchanged and how to best communicate it. Developers are discussing the pertinent information needed to satisfy requests from one system to the next (credit card numbers, cardholder names, expiration dates, etc.).

One step of the solution that will be implemented is tokenization, which is the process of converting credit card numbers to a data proxy. This token is stored in business systems and thus removes the liability of storing cardholder data in the property management or point-of-sale systems. Tokenization in the hotel space is a relatively new concept (the first major hotel chain implemented tokenization in 2007), and one that HTNG has adopted and endorsed and the basis of the industry's card data protection solution.

As the industry takes action to keep its customers' information safe and secure, the HTNG standard message set adapted by PMS and POS systems, in conjunction with a token vault, would allow a company to reduce their risk by utilizing tokens and reducing Payment Card Industry Data Security Standard requirements. If the token is the same across systems, robust reporting from the PMS or POS where the token

resides would allow a company to correlate sales information and customer profiles in a safe and PCI compliant manner.

End result

- Adoption is a long process
- PSMS expects 2016 API rollout
- Standards benefit the end user

Although the payment security standard has been established, hurdles remain in getting it adopted and built by various vendors throughout the industry. PAR Springer-Miller, for example, is in the process of building to the HTNG payment specs and hopes to roll it out in 2016. Other vendors will surely follow suit.

For hotels, having a standard for integration allows them to shop for best-in-breed services. If two software solutions are using a standard protocol to communicate hotels can switch from one provider to another without risking loss of functionality or gaps in data security.

Once the HTNG spec is adopted by a large number of providers, hotels will be that much closer to ensuring their guest data is protected to the fullest extent.

Sidebar: Additional benefits to integration

Before HTNG, property management providers often wrote interfaces to every point-of-sale system on the market. Each vendor had their own way of communicating and code was written to accommodate all of the various players. Now, HTNG develops the API and vendors such as PAR Springer-Miller write to it. Instead of a development effort, it becomes a certification project, and if new players want to integrate they must pass the certification process.

Building a standard specification is no small feat for hotel technology providers. It takes away from developers' main duties and therefore must come with some tangible ROI. Part of the value to building standards is that vendors can write once and then use the API in many different places. Once the interface is built, its standard practice for vendors to ask other technology providers that wish to integrate to build and adopt the same standard. This opens up the number of partners a technology provider can have throughout the industry.

Whether or not a technology provider is an HTNG member or involved in a workgroup, all companies could benefit from the creation of the standard. Once a standard is derived, various technology system providers can retrieve the technical specifications from HTNG's website free of charge and adopt them so that they can communicate across a common platform and integrate seamlessly with other technologies. For example, restaurants, spas and golf operations within the hotel will be able to deploy systems that adopt the standards, such as payment processing

or guest self-service, single guest itinerary, point of sale, guestroom status and many others. Business intelligence, revenue management, channel management and distribution systems are all able to adopt standards that will ensure their integration will be secure, feature-rich and seamless.

Pull Quotes

“When you look at it historically, integration has evolved incredibly. Before HTNG, two companies would sit down and spend months developing an API and then many more months building it. Now that we’ve got standards, you grab the specifications and you’re in building mode rather quickly.”

-- *Chris Donahue, senior product manager, PAR Springer-Miller Systems*

“Some of the workgroups have created a solution for something that isn’t even a problem yet.”

-- *Joe Rembold, solutions architect, Delaware North*