Data Security and Fraud Prevention in Casino Gaming

Data security, as applied to the casino gaming industry, requires advanced technology with the capability to stay one step ahead of sophisticated attackers. Modern casinos must secure patrons' personally identifiable information; ensure the validity of game-winning jackpots; secure Game to System (G2S) transfers of files, games, and configuration parameters; and guard against payment fraud.

Threats Casinos Encounter

Through means such as cameras and facial recognition technology, casinos combat physical security threats and cheating every day. In addition to safeguarding against those violating game rules, casinos also need to address the invisible threats. Hackers threaten the two most vital resources a casino has: its patrons and its gaming investments.

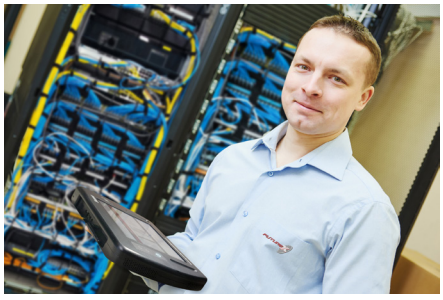
Casinos collect copious amounts of personal player data, including credit and debit card numbers, names, addresses, and other associated information. This information, often stored in a large, centralized database, presents a tempting target to thieves. Criminals threaten not only patron information, but also pose a risk to in-game currency, distribution of player credit, player rewards point systems, and the games themselves. Any information stored on a computer in software is suscepticle to a business-crippling attack.

Internal breaches, whether by intentional attack or through accidental misuse of privlege is also a possibility. With the amount of activity and traffic that casinos

About Futurex

For over 40 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions.

More than 15,000 customers worldwide have trusted Futurex's Hardened Enterprise Security Platform to provide innovative, first-to-market solutions for the secure encryption, storage, and transmission of sensitive data.



Futurex maintains an unyielding commitment to offering advanced, standards-compliant hardware security modules, key management servers, and general-purpose data encryption technology alongside world class customer service.

ENGINEERING CAMPUS 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF: 800.251.5112 - P: +1 830.980.9782 - info@futurex.com

see, maintaining large staffs and an even larger client bases, it is hard for casino operators to keep track of all of the activity that takes place within their walls. In addition to these threats, casinos must defend the integrity of the games they offer. A skilled hacker, accessing source code or protected information, need not be physically present to effect game functionality or payout percentage. Hardened cryptographic solutions protect the functionality and integrity of one of the most popular games: slot machines. Cryptographic devices with multiple functionalities, such as key management, encryption, storage, and centralized management can be applied to safeguard casinos from the possibility of a data breach. However casinos choose to protect their data, it must be secure against internal and external intrusion.

Securing the Patrons

Through player clubs and loyalty programs, casinos collect Personally Identifiable Information (PII) in many forms. This information provides marketing teams with highly valuable information. However, the high value and large volume of this data makes theft a lucrative business. Object signing provides the root of trust necessary to secure the operation of casino games and capture of data, while Point-to-Point Encryption (P2PE), database encryption, and tokenization protect data that has been submitted.

Futurex hardware security modules (HSMs) encrypt PII in a FIPS 140-2 Level 3 validated cryptographic module. If stolen, the data would be need to be decrypted using an inaccessible cryptographic key. To prevent the decryption of stolen data, keys are stored within the HSM and are subject to both physical and logical protections. In the unlikely case that encrypted data were to be stolen, it would be useless to those seeking to profit from it.

For data in motion, HSMs enable private key storage for TLS encryption, a type of encryption commonly used to secure web traffic between a browser and a server. Storing TLS private keys inside an HSM provides greater security for the exchange of PII over the Internet. Additionally, processing TLS handshakes within a dedicated cryptographic module frees up processing power within the web server itself while also providing tamper responsiveness, scalability, and secure storage for cryptographic keys.

Compliance Requirements

PCI Security Standards Council®

PCI HSM - Payment Card Industry Hardware Security Module dictates the secure design and deployment of HSMs to ensure their integrity. These cryptographic devices must meet a strict set of criteria satisfying physical and logical security requirements, including requirements for tamper detection and response, dual login, and separation of user roles.

NIST National Institute of Standards and Technology

FIPS 140-2 Level 3 - The Federal Information Processing Standards is a U.S. government security standard used to accredit cryptographic modules that are used to protect sensitive, but unclassified information. The Level 3 aspect adds requirements for physical tamper resistance, tamper responsiveness, and identity-based authentication.

In addition to the use of TLS encryption, organizations often rely on tokenization for securing cardholder data (CHD) while also reducing the scope and cost of fulfilling compliance mandates. Storing CHD as clear data poses a security risk and is subject to heavier PCI DSS regulations. Tokenization allows sensitive data to be replaced with an identifying string, or "token," for storage after the transaction has taken place. A hardware security module executes this so that the data is never stored as clear text.

Securing Game to System Protocols with Futurex

As hardware-based slot machines transition to the new standard of electronic game machines (EGMs), system upgrades provide opportunities for huge increases in profitability and customization. For the purpose of this document, electronic game machines (EGMs) refer to any electronic betting game, such as video slot machines. Factoring into this profitability is the Game to System (G2S) communication protocols, developed by the Gaming Standards Association (GSA). To maintain a given casino's infrastructure and to keep payout percentages from being manipulated by users, it is vital that Game to System protocols are protected.

G2S protocols provide casinos the flexibility to cater environments to individual patrons, increasing both interactivity and overall profitability. In the United States, the Nevada Gaming Commission stipulates that a machine must be idle for four minutes before any change can be made to the game regarding the game itself, denominations, or payout percentages. These factors can be controlled securely, in real time, with relatively zero downtime through object signing and mutual authentication. Futurex offers this technology in a cryptographic environment, ensuring the validity of casino winnings and compliance with regulatory requirements. This protects both the slot machine manufacturer and the casino from outside threats.

Object Signing

Object signing using a certificate authority ensures both sending and receiving devices are authorized and have permission to share the files and configuration parameters which define electronic game machines.

It ensures the authorized transmission of data between two endpoints, in this case, the central server (where game files are stored) and the physical EGM on the casino floor. Information would only be shared only when the devices are mutually authenticated under a common certificate tree. An outside source, attempting to import and load games or configuration parameters into an EGM would be denied.

Closed-Loop Cards

Object signing can also be applied to prepaid payment cards. Many casinos deploy cards to identify users and accept payments. Using object signing, each card requires a unique cryptographic signature to be loaded on it to prevent clear data from being divulged. With a signature on a closed-loop card, cashiers are able to authenticate the integrity of game payouts.

Authenticating Payouts

Object signing allows payment slips to be validated as authentic. By including a cryptographic signature onto the payment slip from the moment it is generated by a EGM, an employee of the casino can decrypt the signature using an HSM and verify if the checksum matches that of the EGM. If not, the casino has evidence that the payment slip was fabricated or otherwise tampered with.

Collecting, Storing, and Protecting Sensitive Cardholder Data

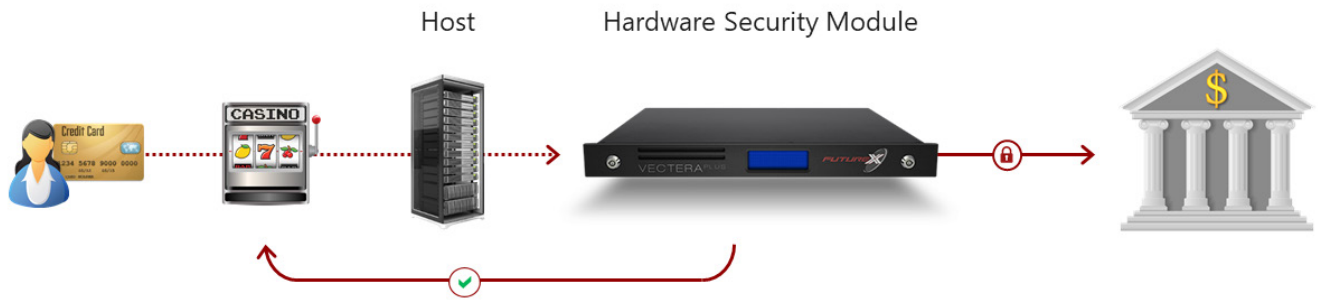
At many casinos, there is no downtime. A 24x7x365 environment needs security that operates efficiently around the clock. The uninterrupted flow of money between casinos and patrons stems large in part because of the overall convenience of modern payment methods. Digital credits, along with the ability to use debit or credit cards at individual slot machines, naturally promotes increased spending.

As the line between casino games and Internet of Things (IoT) devices has become irreverisbly blurred, many casino games now possess the capability to interpret a particular user's behavior and game preferences. Games can perceive when users are about to switch machines, which games appeal most to particular users, and more. Designed to maximize on profit, these machines can adjust on-the-fly to meet the needs of customers.

Rather than having to carry physical currency, patrons regularly opt to exchange digital currency. This flow of money, one that casinos rely on, endures because casino patrons have confidence that their money and data is secure. If thieves steal cardholder data, modify player rewards databases, or even threaten the integrity of casino gaming systems, patrons will lose no longer feel comfortable trusting casinos with their data and their money. In many cases, customer distrust could signal the downfall of a business. To prevent this, patron data requires diligent safeguarding.

P2PE, database encryption, and tokenization are three distinct solutions that work together to create a secure infrastructure, protecting sensitive data at the point of capture, in transit, and at rest.

Point-to-Point Encryption



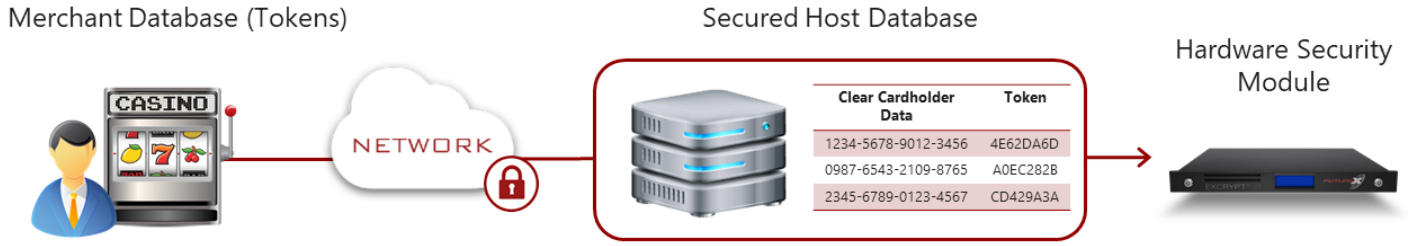
In a compliant P2PE environment, sensitive cardholder data is encrypted from the point of interaction with the EGM and decrypted only within the secure boundary of a FIPS 140-2 Level 3 and PCI HSM-validated hardware security module. In the casino gaming industry, the point of interaction is most frequently provided by the mobile terminals carried by the wait staff. Terminals can also be located within the game itself, or at a POS terminal located at the front desk. From any of these entry points, card data becomes encrypted until it reaches the HSM and can be validated for payment. By implementing P2PE, organizations can enhance their data security infrastructure while simultaneously reducing PCI compliance scope.

Database Encryption

To protect cardholder data and PII, it is a necessity for casinos to configure database encryption, whether at a column or transparent data encryption (TDE) level. Not only does this make data inaccessible to unauthorized parties, it ensures the integrity of the contents of a database, and it allows multiple users to access the database securely. Futurex devices allow for the encrypting of databases and the logging of all access attempts. It is up to the organization as to whether to deploy granular protection on a field-by-field basis (column level) or to encrypt the database in its entirety, in a manner that does not affect users (transparent data encryption).

Tokenization

The payment card data casinos collect is stored in a centralized database, presenting a tempting target for thieves. Tokenization offers a way to protect this information. To validate cardholder data, the EGM or Point of Sale terminal device first captures the clear cardholder data. This can occur at the electronic game, or at any of the POS terminals located in the casino. Next, the relevant token is sent to the HSM through the secured host database, which returns the requested data in a secure manner. By implementing tokenization and eliminating in-the-clear storage of sensitive data, operators of these machines enjoy a considerable reduction of PCI scope and cost. In turn, organizations who practice tokenization do not need to devote significant resources to maintaining compliance, seeing as a security breach is substantially lessened.



Conclusion

Together, P2PE, database encryption, and tokenization ensure robust protection for an organization's data security infrastructure. These solutions are easily integrated into existing data infrastructures for optimum performance and can scale seamlessly to meet an organization's future needs.

Casino owners and operators can take preventative measures to ensure the data they are responsible for is protected. Hardware-based data encryption technology provides a secure, cost-effective solution that grows with an infrastructure rather than restricting growth. Hardware solutions ensure the rigorous protection of sensitive data for the comfort of casino owners and patrons. Continued compliance with regulated data security standards ensures that an organization's defenses will be one step ahead of internal and external threats.

Sources

Columbus, Louis. "Gartner's Top 10 Predictions For IT Organizations In 2017 And Beyond." Forbes. October 19, 2016.

Gaming Standards Association. "G2S: Game To System." GSA. March 3, 2016.

Gill, Chandeni K. "Patron Data Privacy and Security in the Casino Industry." Scholarly Commons at UNLV Law. June 6, 2012.

Mazzeo, Krista. "Cyber Extortion – A Troubling Trend." NJ Cybersecurity. August 27, 2015.

FUTUREX ENGINEERING CAMPUS

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112

864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163