PokerGFX Security Whitepaper

PokerGFX
support@pokergfx.io

Introduction

PokerGFX is the de-facto standard for cards-up live poker production graphics across more than 40 countries. It is used in the majority of live streamed games measured by both number of streams and total hours streamed monthly.

A typical PokerGFX system consists of RFID electronics embedded in a poker table communicating with the PokerGFX Server software running on a Windows computer, along with playing cards that contain RFID chips. Movement of the playing cards is tracked in real time and combined with player actions manually entered by an operator (call, bet raise, fold etc) to generate the graphics that are seen by the audience.

Game integrity relies on a layered security model, ensuring vulnerabilities are eliminated or minimized at each potential attack surface.

Playing Cards

Each playing card contains an RFID chip that has been encoded at time of manufacture with a Unique ID (UID). There is no data stored on the RFID chip that can be used to directly identify the rank or suit of the card. The database that maps this information is stored on the PokerGFX server and protected with an AES-256 encryption key that is unique to each software installation.

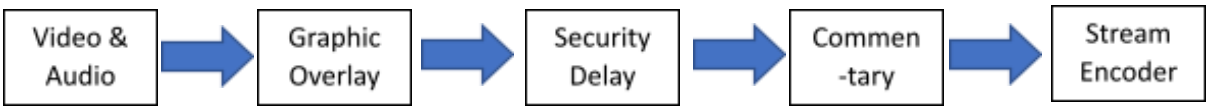
RFID Equipment

Each table typically contains multiple RFID antennas / sensors at the player positions, connected to a central Reader Module. The Reader Module periodically polls the antennas to detect the presence of playing cards and sends this information to the PokerGFX Server application via a hard wired USB connection. All data transiting this connection is protected by an encrypted TLS 1.2 session. Background reading on TLS can be found here:

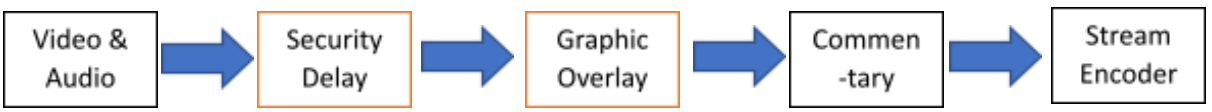
https://www.internetsociety.org/deploy360/tls/basics/

Secure Delay & Trustless Security

Live poker streams utilize a security delay to protect game integrity by ensuring real time hole card information is not available to the audience. Legacy systems implement this delay using the following workflow (this is somewhat simplified but it captures the key processes): Real time graphics are added to the live video and audio, which is then fed into the security delay. At the other end of the delay, commentary is added and then the final program is sent to the stream encoder for distribution to the streaming platform (YouTube, Twitch, Facebook etc).



PokerGFX implements this workflow in a much more secure way using an optional 'Secure Delay' feature:



Note that the Security Delay and Graphic Overlay processes have been swapped. Instead of converting the RFID data into graphics in real time, the conversion doesn't take place until after the security delay has been added, just before the audience sees it. There are two significant advantages to this model:

1. Real time hole cards are not available to the production crew or a malicious actor because those graphics don't exist until after the security delay has passed. Real time graphics are 'cards down' – the operator can see the flow of the game and whether or not a player's cards have been scanned, but not what they are.

2. Because the graphics are generated retrospectively, players do not need to scan their cards on the RFID sensor until the end of each hand, yet the cards will still appear in the graphics from the start of the hand. Players can therefore be 100% confident a security breach is effectively impossible, as the system doesn't know what the cards are until after the hand has finished.

   This has been termed 'Trustless Security' because a player doesn't need to rely on the representations of the venue or production that their hole cards are secure. Keeping their cards clear of the designated sensor position until folding or the hand has ended enables the player to control when the information becomes known to the system, without affecting the quality of the production.

The Secure Delay feature is optional but once enabled cannot be disabled until the stream has ended.