INFORMATION, INSIGHT AND ANALYSIS FOR THE BUSINESS OF INTERACTIVE GAMING IN NORTH AMERICA

iGAMING BUSINESS NORTH AMERICA

ISSUE 27 OCTOBER/NOVEMBER 2016

THE LONG GAME

GAN'S DERMOT SMURFIT ON B2B SOCIAL AND THE "EXTRAORDINARY OPPORTUNITY" OF US IGAMING

PLUS:

What's the next big thing in social slots?

The DGE-KGC agreement

eSports bootcamp

The Valve effect

SECURING THE FUTURE OF ESPORTS

The integration of eSports with gaming brings huge opportunities but also a technology gap when it comes to verifying the age and identity of participants, often intentionally obscured via an online identity or avatar. **Sam McMullen** of FiveGen looks at the issues facing the integration of eSports into a wagering or gambling environment, and how this gap is being closed.

The meteoric rise of eSports has far outstripped expectations or projections from the publishers, vendors, and fans. With this great rise in popularity comes a huge influx of capital. But where there's a lot of money there's usually a lot of risk. And for an industry that is largely driven by technology there is an abnormal gap between the rise of the popularity of eSports and the adoption of more advanced technologies to secure its stability and integrity. This is especially true when we examine how best this industry will integrate with iGaming.

Though many opportunities exist, there are even more pitfalls if certain technological security and integrity measures aren't taken, and very soon. Here I hope to showcase a few of the issues that face the integration of eSports into a wagering or other type of gambling environment.

Who are the participants?

Different factors affect and influence professionals and amateurs alike, and there are certainly problems and questions that arise when a person's active player on the field is not their persona but a virtual player or avatar that represents them in the virtual competition.

Spectators and fans expect a certain type of experience, ranging between professional arena events and venue-specific eContests, or social gaming spaces, either online or land-based. But underlying all of this are important questions for gambling regulators and vendors - who are the people behind the avatars and are they of the required age to play or to be wagering on that play? It becomes more difficult for them to spot or identify a cheater or illegal wager if both the player and spectator are intentionally obscured via an online identity or avatar.

> *"Next-generation authentication systems won't necessarily ever have more than one field for users to enter information"*

The rise of skins betting certainly proved that these players and spectators are everywhere, and some are illegally young and underage for most, if not all, jurisdictions. So how do we solve the problem of underage gambling via skins betting or laundering money via the DLC (or data life cycle)? And when you can't directly verify the age of participants, should you shut down operations? Many believe this is the best option, but I disagree.

The problem will continue to exist, regardless of official sanction. So it's best to get ahead of the black market spaces and integrate smart systems that verify a person's age and overall identity quickly and smoothly while also defining their jurisdiction to gauge the types of currency or prizes allowed. This can be done by integrating biometrically secured multifactor authentication that also maps a person's location via global positioning and local reflection (iBeacon or WiFi) technologies, and checks to see if the user has modified their device to circumvent the security or to place themselves in another locale.

Limitations to operations

Whether you're a land-based casino, an online wagering site, a mobile, desktop, console, web or social game, or providing any other kind of interactive and online content, in order for a user or player to interact and share data with the system, initiate payment or retrieve funds from their account, they require one fundamental interaction - the login request. Usually this takes the form of an identifier such as an email or username and password pairing. But coming up with unique pairs for each of our accounts has become a very difficult and cumbersome process many of us would like to avoid entirely. Most recently, it's become nearly impossible to create something that's secure and stands the test of time, as most systems require a password change every 90 days at the very least, in order to maintain a rotating level of obscurity and security for each online account. And on top of rotating passwords, many systems require that users adopt two-factor authentication to provide additional security, performed by pushing a unique code via text message or special code-generating device or application in a user's possession or on their phone. But is that really the most secure, effective and engaging way to authenticate users to gaming systems premised on providing fun experiences to players?

Many in the industry believe that two-factor authentication is sufficient; there are others that argue that it's woefully inadequate, and as many of you know, the least favorite part of accessing any of your accounts is having to remember your password or figure out how to read the sometimes obscure CAPTCHA messages or enter the time-based codes generated by your mobile before they expire. This isn't the kind of entry-point difficulty many operators want their customers to endure when trying to get them to spend money in a gaming environment.

But there's hope for the future. Next-generation authentication systems won't necessarily ever have more than one field for users to enter information. In fact, there are systems right now using what's called multifactor authentication, which incorporates everything the two-factor has as well as location, biometric, knowledge, action, facial, auditory, and even other factors into one seamless process to enable a person to gain entry into a system.

But how simple?

When trying to play online games in the very near future, or subsequently games on a casino floor, you would visit the portal or step up to the machine and merely type in your first name, then the system would recognize the device in your possession and would push a biometric request for your fingerprint to your smartphone or your identification device that could come in the form of a biometric rewards card.

> ***"Beyond next-gen systems that go further than even multifactor does will include a user's cognitive and emotional state upon requesting access, effectively showing if someone is requesting access under duress or another stress indicator"***

Upon placing your finger on the reader, the system would simultaneously identify that your fingerprint is yours, that you have a pulse and aren't a dead finger and that you're applying pressure so it's not a facsimile; and also your location using GPS and WiFi or Bluetooth triangulation to verify you're standing inside the right building and facing the machine requesting access. Also that your actions happened in the correct order and this is the only request occurring right now and you should be granted access to the game you'd like to play. All of this happens in about as much time as it takes for you to pay for a soda and a pack of gum using Apple Pay or Android Payments when at the convenience store. But without all the cashier's time spent ringing up your purchases. That is to say it takes about 30 or so seconds from start to finish and there's only the effort of having to enter your name and put your finger on a reader. Pretty simple indeed.

But can technology like this actually solve the problems facing regulators and gaming providers? I believe it can. There are only a handful of companies globally which are currently tackling this problem, less if we are specifically looking at iGaming, eGaming, video games and eSports-focused solutions, with just two companies based in Nevada and California so far having developed next-generation multifactor solutions to deal with these problems.

Do multiple factors lead to multiple headaches?

Multiple factors actually don't mean multiple headaches. In fact, it actually means the opposite. Typically a multifactor system is decentralized, which allows for less maintenance or IT headaches than may arise from having to manage a centralized authentication system like those we have everywhere today.

What the latter means is that typical central authentication implementations are built directly on top of the system which they are meant to protect. This causes security problems, because if one of these is breached, the attacker not only has total access to the system, but also to the private user data of everyone who has an account in the system. When systems are compromised in this way, there usually are apologies to the users that have to be made, lawsuits and firings usually follow and the whole system has to be taken offline and out of service in order to fix the problem. And when it gets back up and operating again, the users may not be there as customers any longer. Therefore, changing our methods of authentication is an urgent and serious business.

The fact is that in a decentralized system, the individual users are the ones who are handling the authentication requests through their devices. If one user's device is somehow compromised or doesn't authenticate properly to the system because of a virus or modification to the hardware, only that device is denied access. And it in no way affects the central system integrity or infects any other user's account or device. The faulty account or device can then be individually flagged for security check-up and the user can be notified to make the changes necessary.

Just as random number generators (RNGs) have been adopted to try to give players a sense of fairness when playing an electronic facsimile of a reel slot, card or dice game, security like this is truly random access oriented and also out-of-band (OoB). MFA and OoB systems like this can also handle identity and age verification, assuming that an initial identity verification or age check has been initiated by the system manned by a human being. Human beings are still the best way to verify existing documents of a person's identity and age. Once this has been done, MFA-OoB systems are very reliable to continually authenticate people based on the single context of the system in which they are trying to gain access.

Persistent access can be maintained as well, although it is not recommended unless using a continuous biometric identification factor in the form of a wrist or head-mounted wearable. This could be as simple as a smartwatch that is checking a user's pulse while maintaining the location presence on the wrist of the user without alteration. Or it could come in the form of the soon-to-hit-the-market augmented reality glasses which will incorporate iris or retina print tracking that will allow for a 10ms to three-minute delay between checks. These forms of identifying factors will only add to the robust nature of MFA systems by increasing the inability to compromise their integrity, simply because there are too many inherently impossible factors to impersonate or to hack simultaneously in order to gain access to the critical portion of a user's account, let alone the backend of any protected systems.

Multifactor authentication uses public key exchange to identify the authenticator to the system requesting access. But the public key cannot be exchanged unless the verification of identity, i.e. in the form of a fingerprint, iris, retina, knowledge, action or other factors, are provided which are unique to the user and that will readily identify the requesting party.

Beyond advanced authenticators into the future

Beyond next-gen systems that go further than even multifactor will include facial detection, ocular and neurological or cognitive-imprinted factors that may also serve to identify a person's demographics by way of their approximate age, race, gender and even their cognitive and emotional state upon requesting access. The latter will effectively show if someone is requesting access under duress or another stress indicator. Ocular or eye-tracking systems with or without ARDs (augmented reality displays), as well as active or passive dry EEG neurological trackers and advanced facial and body tracking systems, are in some cases being used remotely in venues already, but will become more widely available to the public in the next 18-24 months.

Regardless of time frame there are already systems like the ones described above being tested in gaming labs in Las Vegas and these will soon be available for wider use and licensing. In a future where eSports and new modes and methods are being used to gain loyalty and attract players and guests, we need to look first at the foundational systems that allow our patrons to feel secure and protected. The integrity of the industry not only relies on this perception, but demands our closest attention and determination to make the changes necessary to create a safe and fun environment for everyone, while removing the headaches for our employees and maintenance staff, suppliers, vendors and providers.

Sam McMullen is co-founder and CEO of FiveGen, a technology solutions and business consulting firm. FiveGen specializes in evolving the ways of play and curating new options for land-based and online gaming operators built on a strong foundation and allowing for growth at scale. This includes game design, security, integrated resort and next-gen wagering, iGaming and eGaming technologies. A true futurist, Sam sees and is working to build upon a changing landscape of entertainment options designed to attract new and younger visitors to casinos, including eSports, video game play, and augmented, mixed and virtual reality experiences.