Secure Wireless Connectivity of Electronic Gaming Machines to Systems

An International Gaming Standards Association Whitepaper

September, 2020

Table of Contents

Secure Wireless Connectivity of Electronic Gaming Machines to Systems

Being able to connect Electronic Gaming Machines (EGMs)[1] and computer systems over a network provides significant benefits to both land-based gaming operators and regulatory authorities. However, in some gaming jurisdictions, land-based gaming locations still do not have a wired Ethernet TCP/IP based network installed. For these locations, the benefits derived from having a high-speed network may not justify the cost of installing the required Ethernet cable. Wireless technology is an alternative that may significantly reduce the cost of implementing casino floor networking while providing all the benefits.

In the past, the use of wireless communication was seen as less than secure by most regulatory authorities. In some cases, that thinking lingers, even though those very same jurisdictions already allow online gaming, or are contemplating allowing online gaming. In fact, any form of online gaming, by its very nature, uses wireless devices and networks most commonly cellular wireless technology. The devices that players use communicate with the servers located in data centers combining wireless and wired networking technologies. Therefore, the use of wireless communication for regulated gaming purposes has been and continues to be used worldwide.

This whitepaper will:

- Compare wireless and wired networks from a security perspective and
- Use Game Authentication Terminal (GAT) and Regulatory Monitoring as use-case examples and describe how they can safely and securely be implemented over a wireless network.

[1] The term Electronic Gaming Machines (EGMs) in this document is intended to include Electronic Gaming Devices, Video Lottery Terminals, Electronic Table Games, and Slot Machines.t

Executive Summary

Wired networking has been thought of as being more secure than wireless networking for a long time. While wired networking will always have a slight security edge over wireless due to the physicality of a wire, wireless networks today provide comparable levels of data security.

Given the level of parity in data security of both wired and wireless networks, the slight additional security of having a wire no longer justifies the significant costs associated with implementing a wired network. The incremental costs of implementing a wired network are even more significant in land-based casinos where running physical wire might require jack-hammering concrete floors.

Both wired and wireless network components, such as routers and switches, must be configured and maintained to provide the best levels of security. Encryption adds another layer of security with encryption capabilities available over both networks that currently require quantum computing to break.

Today, the use of wireless communication is ubiquitous in our lives. From mobile phones to wireless networks in offices, houses, hotels and even airplanes, modern life depends on secure wireless communications. Businesses cannot, and in truth, most people, would not be able to manage without wireless communication for doing everything from banking and shopping to keeping up with current events and being social.

Wireless networks can be implemented using WiFi or Cellular (GPRS) technology. WiFi networks require more care in the configuration and maintenance of its components as encryption is not inherent to that technology. GPRS technology comes with a set level of encryption which, depending on the application, may be sufficient, however, additional encryption is recommended.

From a land-based casino perspective, functionality such as Networked GAT (Game Authentication Terminal) and Monitoring and Control systems, are an excellent fit for the use of wireless technology. These solutions can add significant value to both Operators and Regulators and help prove out the security which wireless networks can provide.

Wireless Networking

For a long time, wired networks were considered not only faster than wireless ones, but also far more secure. The thinking was that in order to hack into a wired network, a hacker had to gain physical access to the network either by tapping into a network cable or by plugging into a network jack. It was argued that the requirement to physically access the network made it more difficult and therefore more secure. The reasons often cited for this additional security were that other security features such as surveillance cameras, security personnel, and access-controls had to be circumvented first, to gain access to the network. While this may have been true in the past, the security differences between wired and wireless networks today have been eroded significantly.

Due to its very nature, wireless networking is always going to be somewhat less secure than wired networking. The physical nature of wired networks versus the over-the-air nature of wireless ones will continue to tilt the security scales towards the wire. Wireless data is more exposed, in that anyone with the right technology, the right know-how, the time and the means, can 'sniff' the data traveling over the air. They don't even have to be in the building, just close enough where they can 'see' the data being transmitted between routers and devices. This does not mean wireless networks are not secure. In fact, as we will discuss, numerous security features have been developed that elevate wireless network security to close parity with wired networks.

However, not all wireless networking technologies are created equal and appropriate security measures, both hardware and software, have to be implemented and configured correctly in order to achieve that level of close parity with wired network security.

There are a variety of wireless networking technologies. These include short-range connectivity using technologies such as BlueTooth (BLE) or Near Field Communication (NFC). Mid-range connectivity can be achieved using WiFi, and wide-range connectivity can be achieved using Cellular technologies such as GPRS, 3G, LTE and the much hyped 5G.

For this whitepaper we will focus on 0WiFi, GPRS, and GSM wireless technologies and compare them to wired networks in terms of security.

WiFi

The WiFi IEEE 802.11 standard was first released in 1997. Over the years since then, there has been a steady stream of 802.11 standard enhancements, each denoted by a letter or letters and each improving the throughput, functionality and security capabilities of this most widely used wireless networking technology. While the latest version is 802.11ax, also known as WiFi-6, the most commonly used version of WiFi is 802.11n, which is what you find in laptops, routers, and wireless printers manufactured over the past few years.

WiFi networks are secured through the configuration of security protocols and encryption algorithms within wireless routers. Just as WiFi has evolved over the years, so too have the security protocols. The latest protocol version is WiFi Protected Access III, also known as WPA3, although its predecessor, WPA2 is also still widely used. WPA2 comes in Personal and Enterprise versions. As the name implies the Personal version provides suitable protection for home use, while the Enterprise version is recommended for business purposes where sensitive data is communicated.

Encryption protects the data being sent over both wired and wireless networks. It does this by taking the data being transmitted to and from a device and scrambling it using a mathematical algorithm, process or standard, making that data unreadable. The sending device scrambles the data using an encryption key and the receiving device unscrambles the data using the corresponding decryption key. The latest version of encryption supported by 802.11n and WPA3 is the Advanced Encryption Standard (AES).

In terms of encryption, AES continues to be the algorithm recommended by the National Institute of Standards and Technology (NIST). The reason for this is that AES supports encryption keys up to 256 bits. This makes breaking this encryption without the use of quantum computing practically impossible.

WiFi Summary – WiFi data transmission security can match that of wired networks if the routers used support the combination of WPA2 Enterprise or WPA3 with AES-256 encryption. This is currently considered the most secure method for provisioning WiFi networks for use in a variety of industries including medical and banking.

GPRS

The General Packet Radio Service (GPRS) is a mobile data standard for cellular communications that runs on 2G and 3G networks. GPRS was the technology that allowed Multimedia Messages (MMS) text and photo sharing to occur on mobile phones. While GPRS itself is not encrypted, the data transmitted via GPRS is typically encrypted by the Telecom companies that provide it.

2G communications utilizing Authentication and Key Agreement (AKA) protocol are only capable of providing 64-bit encryption, which is not considered secure. Therefore, an additional level of encryption is required beyond the 'basic' AKA level – which may or may not be provided as that differs by Telecom. While 2G is still available in many parts of the world, it is being phased out in the US and may no longer be available by the end of 2020.

3G communications, as the successor to 2G, was designed to build on the more robust security features and to fix the security holes, found in 2G. The 3G Universal Mobile Telecommunications Service (UMTS) architecture as defined by the International Telecommunication Union (ITC) was the result. 3G security enhanced the AKA protocol by introducing the use of AES encryption in the

UMTS-AKA. 3G networks were designed to deliver much more functionality than 2G networks, including web browsing and video telephony, and therefore had to provide for additional security.

GPRS Summary – GPRS running on 2G must utilize application layer encryption to provide adequate data security. GPRS running on 3G is more secure; however, the type of AES encryption used may differ from provider to provider. Therefore, to achieve wired network level data security, a robust application layer encryption methodology must be implemented.

GSM

The Global System for Mobile Communications (GSM) was developed by the European Telecommunications Standards Institute (ETSI) and was the precursor to GPRS. GSM was developed specifically for the 2G digital cellular networks. For that reason, data transmission via GSM can only be accomplished via Short Message Service (SMS).

GSM Summary - Since GSM only supports 2G, the security issues identified with 2G on GPRS apply. In order to provide adequate data transmission security, additional software-layer encryption will be required. Without this, the 2G cellular network is susceptible to hacking.

Additional Cellular Wireless Network Security

As described above, the communication protocol and AES data encryption provides significant security for a cellular-based wireless network. The use of APN (Access Point Name) as a point of entry into an IP based network further bolsters that security.

A cellular device wishing to connect to a cellular network has to provide its APN to the cellular network provider. That provider will then evaluate the APN to determine with IP address(es) the device should be provided it, what type of security should be applied, and if it should be connected to a private network. It is this last feature that is of particular importance to help bolster the security of the 2G or 3G wireless cellular network.

APN bolsters security by providing a direct pathway from the cellular device such as a mobile phone or IoT (Internet of Things) device directly to the private organization's network. This is done at the SIM card level and avoids data travelling over the 'public' data pathways. Using a Static Fixed IP further increases security as the device does not have to search for an IP address that changes, but rather knows exactly which one to use. Through the use of APN and a Static Fixed IP makes it much harder for hackers to 'see' the data as well as to hack it.

Wireless Security Summary

Wireless network data security can achieve parity with that provided through wired networks. Using WiFi, this security parity can only be achieved through diligent selection and configuration of hardware, communication protocols and encryption algorithms. Using low-cost, low-power usage,

cellular technologies, the security parity can only be achieved by adding application layer encryption to the minimal data link layer protection that may exist.

Wireless networks, by their very nature, will never match the physical security of a wired network. However, the minimal amount of security provided via a wire or a network jack come at a significant expense that may overshadow their benefits.

Bottom line: using readily available technologies wireless networks continue to be used within industries such as FinTech, Medicine, and Manufacturing, due to its lower implementation cost, greater flexibility and wired-network level security.

Wired Networking

The world of wired networking today is almost universally reliant on Ethernet computing technologies. Ethernet networking has been commercially available since 1980, when it was introduced as the IEEE 802.3 standard, and has evolved to support faster data transmission speeds, greater distances, and a variety of wire types. It works well with wireless networks, supporting the Internet Protocol (IP) and is used as one of the key technologies that support the internet.

Ethernet Network Security

The Ethernet network technology works at the OSI Physical and Data Link layers. In other words, it handles the type of wire being used and how data is transmitted and travels over that wire. You may hear of terms such as 10BaseT for standard Ethernet or 100BaseTX for fast Ethernet. They refer to the transmission speed in millions of bits per second.

Just like with wireless networks, the security applied to Ethernet wired networks is achieved through a combination of hardware and software. In some cases, a security solution may be available in both a hardware and software version.

The most commonly used communication protocol over Ethernet is the Transmission Control Protocol / Internet Protocol or TCP/IP. This protocol is broken down into five layers, which are, from the bottom up, are the Physical, Data Link, Network, Transport and Application layers. We will skip discussing Application Layer security since applications are common to both wireless and wired networks. While applicable to both wired and wireless networks, we'll discuss the Network Layer Security and Transport Layer security in this section.

Layer 1 - Physical Security

While this may be just plain common sense, it goes without saying that sensitive and critical network hardware has to be secured. Routers, Switches, Repeaters, etc. must be in access-controlled locations. As previously described, this physical security is an edge that wired networks will always have over their wireless kin.

Layer 2 – Data Link Security

The use of smart Ethernet switches can prevent a number of common attacks that the Data Link layer is susceptible to. These attacks include Address Range Protocol (ARP) Spoofing, Media Access Control (MAC) address flooding, Port stealing and general attacks such Distributed Denial of Service (DDOS).

These types of attacks can be thwarted by correctly configuring smart Ethernet switches that can limit MAC address access, identify and allow traffic from only trusted DHCP ports, and only reply to ARP on trusted ports. This is neither a comprehensive list of attacks nor of counter-measures, but rather a sample of issues and solutions to point out that smart Ethernet switches must be utilized and configured correctly to prevent these attacks.

Layer 3 – Network Layer Security

The Internet Protocol Security (IPsec) protocol is a very popular tool for securing the Network layer. IPsec works with both TCP and User Datagram Protocol (UDP) and provides for a secure means of connecting two different network entities. Data packets being transmitted over the network are fully protected by IPsec which makes it ideal for cross-network communication. It is for this reason that one of the most common uses of IPsec is facilitate the creation of Virtual Private Networks (VPNs) between two hosts or between a user and a host.

The use of a Firewall at the Network layer can provide an additional level of security. At the Network layer, a firewall works by packet-filtering, which is identifying what to let through it and what to keep out. It does this by evaluating the source address and the destination address. However, this has some inherent flaws, as ports are either open or closed and all the Firewall does is inspect the addresses. Firewalls have evolved over time and are no longer just relegated to Layer 3. In fact, Firewalls today can be used up to the Application Layer 5. Firewall manufacturers have also combined functionality depending on how they will be used on the network, making them a very useful component of network security.

As mentioned above, please note that Network layer security applies to wireless networks as well.

Layer 4 – Transport Layer Security

Transport layer security starts with the TCP portion of TCP/IP. TCP is responsible for handling the data packets transmitted over the network and the error checking to ensure that all the packets have been received, and if not, to ask for them to be sent. While TCP maintains data packet order over the network, it does not really do much in the way of ensuring data privacy.

Here's where we find one of the most widely adopted security protocols, which was designed specifically for the Transport Layer. The Transport Layer Security (TLS) protocol is the newer version of the data encryption protocol called Secure Socket Layer (SSL). TLS is designed to work on top of TCP to provide data confidentiality through encryption, authentication of the data sender and data receiver via certificates, and data transmission reliability by maintaining message integrity checking. Both TLS and its predecessor SSL were designed primarily for web-based applications and for eCommerce in particular.

Secure Shell (SSH) protocol enables secure administration and data transmission over networks and is used in almost every data center in the world. SSH uses encryption to secure the network connection between the data sender and the data receiver. All of the traffic between those two end-points is encrypted.

As mentioned above, please not that Transport Layer security applies to wireless networks as well.

Wired Security Summary

Wired networks are as susceptible to attacks as wireless ones. It is true that gaining access to the physical wired network is more difficult, but an unsecured switch, router, or network jack is all that is required for a hacker to gain access to the network. To provide a secure network, the right hardware has to be selected and correctly configured. Additional layers of protection must be employed to prevent threats across the various TCP/IP layers.

It is also important to note that more and more wired networks are incorporating wireless components or segments. Therefore, while wired networks are not obsolete, perhaps the idea of a purely wired network is becoming a thing of the past.

Bottom line, wired networks will most likely always have a security edge over wireless ones, but the cost, overhead, and complexity of those networks may make the wireless alternative more attractive with minimal security degradation.

Wireless Network Use in Land-based Gaming Sites

Communication Protocols

In most regulated gaming jurisdictions, EGMs must be connected to a central Casino Management System (CMS) which is used to monitor the EGMs, collect data, and generate reports which are used for numerous functions both by operators and regulators.

There are two widely adopted communications protocols used to connect EGMs to a CMS: the legacy Slot Accounting System (SAS) and the newer Game-to-System (G2S) protocols. SAS is a serial-based protocol that does not require a TCP/IP network, whereas G2S was designed specifically to run over a TCP/IP high-speed network. Therefore, land-based gaming sites such as casinos, betting shops, and parlours that are using the SAS protocol are the ones that typically do not have a high-speed network on the casino floor.

In a SAS-based implementation, each EGM must use a Slot Machine Interface Board (SMIB) which is installed into the EGM. SMIBs are manufactured and sold by the same company that publishes and sells the CMS and is considered part of the system. The SMIB is what actually 'speaks' SAS to the EGM, whereas the SMIB may 'speak' a completely different protocol upstream to the CMS. The SMIB connects to the EGM using a serial communications port known as a COM Port. An EGM may have multiple COM ports, usually numbered from 1 on up.

In a G2S-based implementation, each EGM is connected directly to the Ethernet network via an RJ45 connector that EGM manufactures include. EGM manufactured over the past decade generally have this type of connector along with the serial COM ports. G2S eliminates the need for the SMIB.

Communication Protocols and Connectivity

As described above, the SAS based protocol is serial based and requires connectivity to the EGM via a serial COM port. However, networking technology has evolved from the 80's which was when SAS was developed.

Today it is possible for SAS-based EGMs to actually be connected to a TCP/IP network. Since the SMIBs are connected to the EGM and the CMS then those connections could occur using different protocols and different communications methods. Therefore, it is possible that the SMIB to CMS connection could occur over a TCP/IP network while the SMIB to EGM connection could still be occurring using a serial connection and SAS.

Gaming entities that have a TCP/IP network can leverage that network to implement both Networked GAT and Regulatory Monitoring using the existing SAS-based EGMs and with no impact to the CMS. Information on how will not be included in this whitepaper since it is addressing the use of wireless networking as an alternative solution for gaming sites that do not have a wired network.

G2S was designed specifically to run over a TCP/IP network and therefore takes full advantage of that network's capabilities. For this reason, the whitepaper will not discuss G2S based solutions.

Functionality Suitable for Wireless Networks

As identified in the comparison of Wireless and Wired networks, if both types of networks are deployed using properly selected components, those components configured correctly and the appropriate security features utilized, then the security difference between the two types of networks is minimal. As almost every regulated jurisdiction requires EGMs to be connected to some type of CMS and since that required system is already in place, this whitepaper will not focus on how the existing wired connection can be replaced with wireless. Rather, this whitepaper will suggest two other solutions that are well suited to being implemented over a wireless network.

Networked GAT

The first solution is Networked GAT. Networked GAT works essentially just like Serial GAT and allows regulators to request an EGM to calculate, and send back, a hash value for one or more pieces of software running within it. Using the Networked GAT Interface (NGI), Networked GAT allows the request to occur from a remote computer connected to the network and for the calculated hash value to be sent back over the network to that same computer. This is in sharp contrast to serial GAT which requires operator staff along with a regulatory agent to open the EGM and plug a device, usually a laptop computer, into the EGM's GAT port. The hash calculation request is then done, EGM by EGM. Both versions of GAT allow the EGM to be playable while it is calculating the hash value. However, with serial GAT, the EGM has to be re-opened, and the laptop re-connected to get the hash value one EGM at a time. With Network GAT, the value is simply sent over the network when it is done.

The GAT calculated hash value allows regulators to ensure the authenticity of the software running within EGMs. It also allows regulators to verify that only the approved version of the Operating System and Game Theme Software is being used. This is done by comparing the hash value results with those of the originally tested and approved software version.

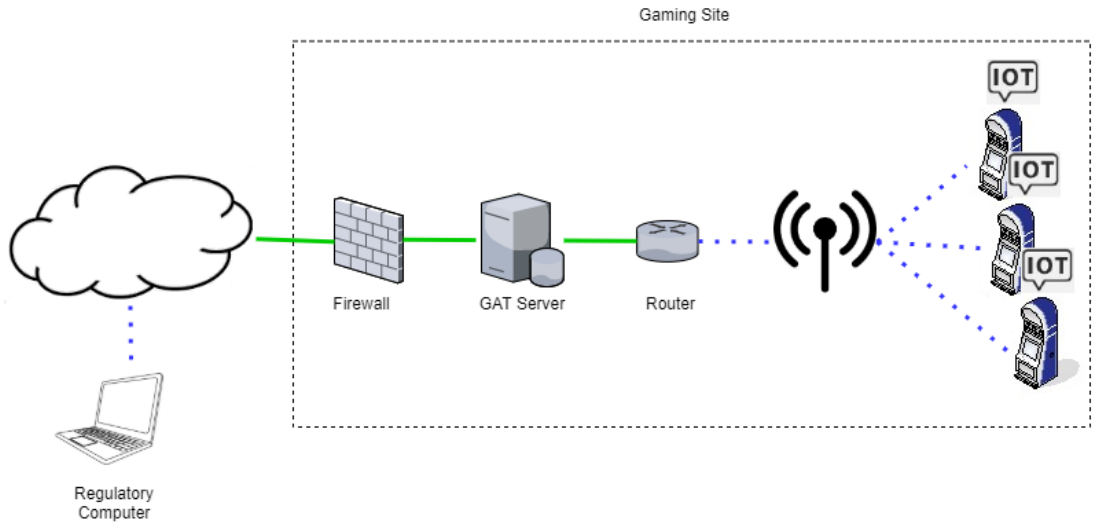
Serial GAT is much less efficient than Networked GAT, however it is far more widely implemented. Therefore, it may be impractical to expect that EGM manufacturers will update their EGM Operating Systems to implement the NGI protocol required to support Networked GAT. A far more practical solution is to use a small, inexpensive, Internet of Things (IoT) device that supports both the NGI protocol as well as the Serial GAT protocol. The IoT device would be installed in every EGM and physically connected to the EGM's GAT port.

Recommended Implementation

Networked GAT requires a two-way conversation between the Requestor – the regulator's computer – and the Responder – the EGM. To introduce additional security, NGI supports the use of a GAT Server which acts as the Intermediary between the Requestor and the Responder. This Intermediary server is located at the operator's site and physically connected to the operator's network.

To secure the Intermediary Network GAT server, a firewall is placed before it on the network. Since the traffic that will be flowing from the Requestor to the Intermediary is known, and since the Requestor computer can also be known, the firewall can be configured to filter out any unexpected data flowing over the connection. This introduces security that prevents direct access to EGMs from outside networks.

The IoT device in this implementation is heavily restricted in functionality, capable only of executing GAT requests. It is also connected only to the EGM's GAT port, further restricting what it can do. An implementation using these components could look like this:



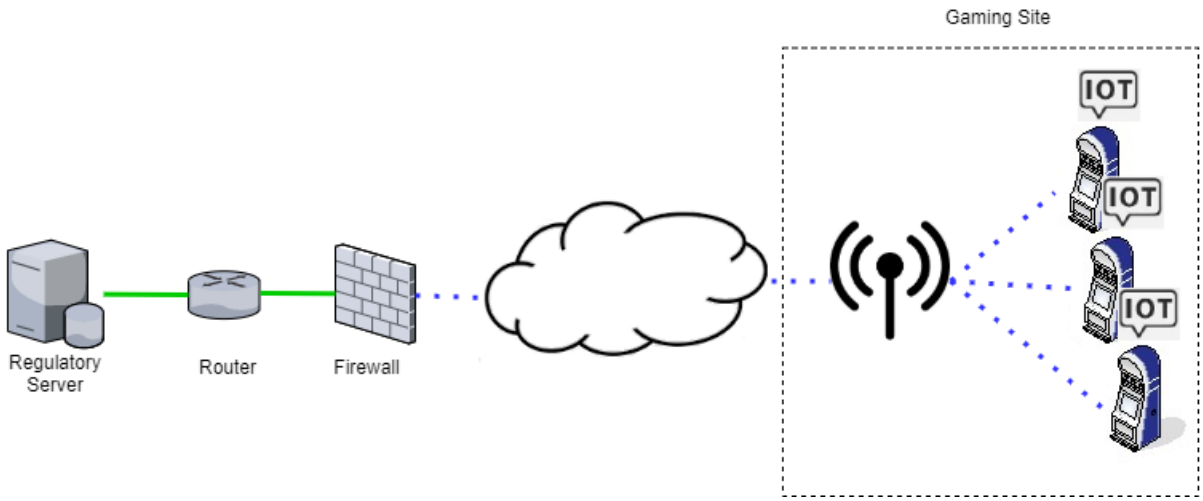
Regulatory Monitoring and Reporting Systems

In North America, there are a number of regulatory authorities that have mandated the use of a Monitoring and Reporting system that is separate from the CMS. In other parts of the world, more and more regulators are mandating the use of these systems. Regulators see having direct access to EGM data, such as meters and events, see that intentionally bypassing the operator-owned network and CMS, as beneficial.

The simplest and most practical way to implement such a system without utilizing the operator's network is to use a GPRS or GSM based network. A cellular wireless solution bypasses the operator's network completely regardless of the protocol the EGM supports. Therefore, this solution works equally well with EGMs that only support the SAS protocol, EGMs that support the G2S protocol, or EGMs that support both.

A low-cost IoT device with a GPRS or GSM modem installed in each EGM provides an ideal solution. In this case how the IoT devices connects to the EGM will depend on what protocol the EGM supports. If the EGM only supports the serial-based SAS network, then the IoT device will need to connect directly to one of the serial COM ports. If the EGM supports G2S, then it can be connected to a small smart switch which in turn is connected to the EGM's Ethernet port.

The IoT device using GPRS or GSM will communicate through the Cellular Service Provider (CSP) directly to the regulatory authorities Monitoring and Reporting server directly. All data is encrypted for security. This type of implementation may look like this:



The same IoT device can be used to provide both Networked GAT and Monitoring and Reporting functionality, if the regulatory authority is implementing both.