Gaming System Software Verification & Assurance:

An Overview of Current Industry Best Practices

November 4, 2011

Prepared by Todd Elsasser
Independent Gaming Consultant

Executive Summary

Gaming System Software Verification and Assurance: An Overview of Current Industry Best Practices.

It is no secret that the Gaming industry is one of the most tightly regulated and reviewed enterprises in the world today. For decades now regulators and gaming operators have demanded the most secure operating environment possible and the gaming industry manufacturers and providers have complied with those demands. Recently centralized, server supported or server based gaming and lottery systems have manifested a slight erosion in these critical security standards. Newer systems are beginning to rely on commercial off-the-shelf software to automate processes with information technology that was originally designed for intranet communications and office operations. Even communications protocol software specifically designed for gaming applications leaves data security and integrity checking almost wholly "at the whim" of the system manufacturer.

Customized and semi-customized gaming software underpins the information infrastructure that governments, independent gaming operators and gaming providers worldwide depend upon for daily operations and business processes. These organizations depend on the security and integrity of their software in order to provide the players with a fair, honest playing environment. At the same time, cyber attacks are becoming more stealthy and sophisticated, creating a complex and dynamic risk environment for IT-based operations that users are working to better understand and manage. As such, users have become increasingly concerned about the integrity, security and reliability of commercial software.

To address these concerns and meet both regulator and customer requirements, vendors have undertaken significant efforts to reduce vulnerabilities, improve resistance to attack and protect the integrity of the products they sell. These efforts are often referred to as "software assurance." Software assurance is especially important for casino regulators who are often not always present at the gaming locations and lottery organizations where they are often both regulator and operator of the system. These users both require a high level of confidence that both customized and commercial software is as secure as possible, something only achieved when software is verified using best practices for secure software integrity inspection.

This white paper provides an overview of how Kobetron recommends regulators approach software assurance, and how the use of best practices for software integrity checking helps to provide stronger controls and integrity for gaming applications.

The Challenge of Software Assurance and Security

Software assurance encompasses the development and implementation of methods and processes for ensuring that software installed in the field is identical to that which was originally coded and certified during the testing and acceptance process. It also is essential to verify that archived or saved data remains unaltered and that all financial and integrity data files can be independently verified at any time using safe, secure means. Uncontrolled and unregulated software modifications could easily lead to malicious code or defects that could bring harm to the end user. Software assurance is vital to ensuring the security of critical information technology resources. Information and communications technology vendors have a responsibility to address assurance through every stage of application development.

This paper will focus on the software assurance responsibilities of regulators and operators. However, developers and integrators also share some responsibility for ensuring the security of critical information data. Because of the rapidly changing nature of the threat environment, even an application with a high level of quality assurance will not be impervious from attack if improperly configured and maintained. Managing the threats we face today in cyberspace requires a layered system of security, with vendors building more secure software, integrators ensuring that the software is installed correctly, operators maintaining the system properly, and end users using the products in a safe and secure manner all done under the regulatory umbrella provided by the gaming regulators who have a need for 3rd party tools to ensure the integrity of their systems from end to end.

New Risks and Countermeasures

For over 25 years the gaming industry has relied on independent testing and regulator controlled on-site verification of all critical gaming software. Control was centered on the actual gaming floor and each and every gaming machine was inspected, had the EPROM containing the critical gaming software verified and sealed, and access to the gaming devices was strictly controlled. The 3rd party tool used for this EPROM based software verification was the Kobetron device. So widespread was the use of the Kobetron test device that the very name; Kobetron became both a noun describing the physical testing device as well as a verb describing the act of verification of gaming device software. In all the years of use the Kobetron device security algorithm was never defeated and no modified, unauthorized software has ever 'passed' a Kobetron signature test.

New enhancements in gaming software reduce or eliminate the use of EPROM technology. Flash drive units as well as conventional computer hard drives are beginning to supplement EPROMs. Downloadable or server based gaming is coming into play. New systems where the key gaming functions and random outcomes are server determined and downloaded to the player's device are in operation. Mobile and other remote gaming devices are becoming more prevalent and finally, internet based gaming is rapidly looking to become the next platform for gaming development. Use of all of these varied technologies expand the threat from the actual gaming floor to virtually anywhere access to the computer network might be obtained. This greatly expands the area regulators need to concern themselves with and creates multitude of regulatory and control problems for the operators. The threat environment is also increased and creates new challenges for all software-related operations. Vectors for attacks that could interrupt or stop critical software functions must be considered in design and development. The software assurance risks faced by regulators today can be categorized in three areas:

Accidental installation of incorrect or obsolete software that lead to exploitable code vulnerabilities or improper gaming operations

The changing technological environment, which exposes new vulnerabilities and provides adversaries with new tools to exploit them

Malicious insiders who seek to do harm to users or vendors or to exploit vulnerabilities for personal financial gain

Accidental installation of incorrect or obsolete software

A gaming device today contains thousands of individual files, programs, tables and operational command functions that must be tested and certified by a gaming lab prior to installation. It is virtually impossible to track each of these files individually so a means is needed to 'bundle' all code needed for a single operable product into one signature that the regulator can use to verify the field installed versions against. Any change or update to this bundle of programs must result in a new, unique signature so that obsolete or replaced software can easily be spotted and removed from play. Regulators need a means to verify only certified software is installed and in use and that all obsolete code is removed in a timely fashion.

The Changing Technological Environment

Rapid change and innovation are two of the most enduring characteristics of the IT industry. Unfortunately innovation comes more slowly to the gaming industry than to other areas of IT. Innovation is also not unique to vendors, criminals can and do innovate. In the span of only a few years a complex and lucrative criminal economy capable of supporting specialized skill sets for identifying and attacking software has developed.

The development of this sophisticated criminal economy contributes to increasingly targeted and complex attacks. Vendors commit resources to understand emerging threats and use state-of-the-art technologies, tools and techniques to develop software, hardware and services that can resist attack. The process is one of on-going improvement as new vulnerabilities are exposed, new threats are created and new countermeasures developed and implemented. Due to the time lag between the gaming industry and the rest of the IT world, publically exposed software vulnerabilities are often commonly still in use in gaming systems making them all the more lucrative to potential thieves and criminal enterprises.

The regulator is often faced with both technical and security challenges as he struggles to understand the new technology while still mandated to provide a safe, secure gaming platform for the players. Unfortunately, voluntary strides by the manufacturers to provide better security often only come after someone has exploited the system and the operator has experienced financial loss.

Malicious Insiders

There is a growing concern that gaming software could be exploited by a rogue programmer or an organized group of operational insiders that would compromise software or services during the gaming process. Vendors are extremely protective of their "soft assets" such as their code base. The complex development process and the series of controls used to protect the development process provide powerful management, policy and technical controls that reduce these risks. Independent lab testing helps ensure that code is as free from bugs and other malicious code as possible but there is no single way to manage or control the entire development process. Rather there are proven best practices and 3rd party tools such as the Kobetron series of tools that companies and regulators can use to manage their unique developed game and systems software.

Managing Risk Through Use of 3rd Party Verification Tools

These risks can be managed through the adoption of best practices in software assurance. While a number of international standards and certification regimes for software assurance have been issued, their effectiveness in achieving real-world reduction in vulnerabilities is debatable. Certain regulators on their own have been taking the lead in developing and implementing practices to produce higher levels of software security that are better tuned to real-world processes and result in higher levels of both confidence and security. Kobetron's mission is to bring their decades of experience to this expanding technology and to give regulators the tools they need to provide the same level of assurance the gaming industry has always enjoyed.

Recommended Best Practices for Software Assurance and Security

Gaming devices today incorporate a wide variety of technology, and this use of mixed old and new technology has made verification procedures become increasingly convoluted. There is little standardization of media or platform architecture between the various suppliers. Testing lab approval letters contain multiple pages of approval information that must be sifted through to determine the exact location, media type, and verification methodology for each product. Increasingly regulators are encountering problems with verifying critical memory stored on media that they had not previously encountered. These problems cause delays and create difficulties in getting new products into the marketplace. Recently, for perhaps the first time in regulated gaming history, there was a situation where critical code cannot be verified by any currently-available method once it's been downloaded onto the media. A very difficult and cumbersome situation is now facing the regulators rejecting new innovations and declaring the entire verification process as unacceptable.

Kobetron has always stressed the importance of a requirement for Third Party Verification. 'Third party' in this case could be defined as "an entity that is not bound contractually or financially to either the manufacturer of any gaming device, or to any gaming testing lab." Current methodologies that enable hashing of gaming device code while the media remains installed in the device, even when they are successfully executed, technically involve the device "verifying itself" upon command and displaying the result rather than utilizing a true third party verification routine and are thus inherently suspect and unreliable.

An ideal solution would not require the purchase of expensive new equipment, but would utilize or build upon tools already in use and widely available. Kobetron believes that we have these tools and are committed to working with the industry to provide a continued record of 100% total software verification and integrity assurance.

A Word On The Use Of MD5 And SHA1 Algorithms For Software Verification

A recent review of gaming systems design and security processes reveals an almost universal reliance on either SHA1 or MD5 algorithms for providing communications as well as data security and integrity. Without going into intimate detail about either of these methods it should be noted that both have widespread use in current network and internet frameworks and that both are considered not to be secure by manufacturers such as Oracle, Intel, Microsoft and IBM. Both formulas have been 'cracked", that is, hackers and other criminals know how to use specialized programs to decrypt data encrypted by these methods and to modify the data without either SHA1 or MD5 dependant watchdog programs detecting the changes.

What does that mean to a regulator?

If a regulator uses a server communicating critical game information to a device, say a Random Number sequence used to determine a the outcome of a slot game program, and a hacker is able to alter this data. The player may be presented with a losing combination of symbols on screen instead of a winning combination that they were supposed to receive. An unscrupulous operator can then claim these winnings for himself instead of the player. Use of SHA1 or MD5 to verify software integrity could result in incorrect games being installed in the field. The State of Nevada had this situation occur when one of their State employees substituted valid code for modified software that enabled him to win on electronic Bingo. In another regulated jurisdiction, EZ Pay tickets were counterfeited when criminals got access to the ticket database and were able to reproduce copies of unclaimed winning tickets.

In September 2007, Research Concepts LLC asked 185 members of Networkworld's Technology Opinion Panel about the state of computer and data security in their organizations. The companies represented were some of the most trusted names in IT and computer applications. The results revealed that, although computer and data security are high priorities for corporations, they are nevertheless unprepared to prevent data breaches and computer theft. Common approaches to computer security aimed at minimizing the possibility of data breach were consistently undermined by employees. Indeed, those surveyed reported that only one in 100 employees consistently follows corporate data and security policies. If these are the most technologically advanced and secure companies in the world, how secure are the casino operations today? Insider activity that aids or assists criminal activity is not a new occurrence in the gaming industry.

In February 2010 the Associated Press reported the hacker Christopher Tarnovsky had accomplished what many thought was nearly impossible: cracking the Trusted Platform Module (TPM). Described by some as a "digital Fort Knox," the TPM is a specialized processor dedicated to encrypting data and keeping sensitive information from prying eyes. The chips, found in many PCs, are an important line of defense for businesses and governments who need to protect their secrets. The Trusted Computing Group, the standards group that governs TPM chips, stood by the technology as an effective way to secure data. The group said that the hack was "exceedingly difficult to replicate." Of course, "exceedingly difficult" is not impossible, and it's only a matter of time before the AP expects to report on the first attack that circumvents this formerly foolproof security measure.

Conclusion

The global gaming software industry is making great strides at improving operational efficiency and offering new and improved methods for the operator to manage and control his casino floor. They are working towards uniform communications standards and enhanced overall gaming standards. Security and software verification processes however, seem to be falling by the wayside in this rush towards centralized gaming systems and intranet gaming solutions. Regulators need to maintain the same 100% assurance that all software running in their jurisdiction is tested and approved and need to mandate the use of 3rd party tools not reliant on MD5 or SHA1 exclusively. Kobetron has developed tools that meet these demands and stands ready to assist the manufacturers in integrating this security into their games and systems. Regulators such as the Missouri Gaming Commission have begun adopting standards requiring the use of independent 3rd party developed security tools. International jurisdictions such as those in Italy have denounced reliance on SHA1 and MD5 signature algorithms and have adopted more stringent regulations regarding software security and integrity verification. The result of efforts like these will be a higher level of confidence for end users in the quality and safety of software that underpins critical operations in casino and lottery gaming worldwide.

About Kobetron

Since 1984, Kobetron™ has been providing standard and specialized test equipment. Recognized worldwide as a prudent and innovative company, our mission is to develop and manufacture the most sophisticated, reliable, stand-alone or PC based test equipment, within our targeted industries.

Our commitment to leading edge technology, research & development, quality products, and customer service has firmly incorporated Kobetron in the forefront of the markets we serve. Principal to our success is the pledge to provide an exceptional level of customer service.

Kobetron recognizes that our future depends upon a strong base of satisfied customers, so we continuously strive to maintain a high level of customer satisfaction. Our Support Team provides customers with a complete service solution ranging from Training and Technical Support to Factory Authorized Service.

We are located on Florida's Gulf Coast and all our products are 100% made and manufactured in the USA.

Kobetron, Inc.
P.O. Box 5489
Navarre, FL 32566
USA

Sales: (850) 939-5222 x29
Technical Support: (850) 939-5222 x12
Fax: (850) 939-0490

About the Author

Todd Elsasser, has over 20 years experience in gaming regulation and technical compliance. He has worked for some of the leading companies specializing in testing and compliance matters including being the former Executive Director of Gaming Laboratories International (GLI) and former Director of Technical Compliance at Cyberview Technologies, Inc. as well as Managing Director of Gambling Compliance, Compliance Director at SIQ Test Laboratories and as a Technical Consultant for Kobetron Inc. Todd has experience in both casino gaming as well as video lottery system certifications and startups, and has coordinated with regulators and gaming agencies worldwide. Considered one of the industry's top regulatory experts, Todd has given numerous presentations and training seminars on everything from new technologies to game testing, security, and the drafting and adoption of gaming regulations.