On-Line Raffle Ticket Sales

Saskatchewan
Liquor and Gaming
Authority

Table of Contents

Introduction

The Saskatchewan Liquor and Gaming Authority (SLGA) is responsible for the regulation of gaming in Saskatchewan as mandated under *The Alcohol and Gaming Regulation Act*, *1997*. This document outlines the integrity certification requirements for the sale of raffle ticket(s) through the Internet. All systems used for the sale of raffle tickets through the Internet must meet the requirements contained within this document and the terms and conditions set forth by SLGA for the sale of raffle tickets through the Internet.

Background

These standards were developed from consultations with Gaming Laboratories International, LLC. (GLI) Lakewood, New Jersey, referencing GLI standards: GLI-19 Interactive Gaming Systems and GLI-31 Electronic Raffle Systems.

Purpose

These standards are intended to provide regulatory guidance to manufacturers, suppliers and gaming operators and licensees regarding technical gaming integrity requirements in Saskatchewan. Where variations from these standards are proposed, SLGA will review to determine acceptable practices.

These standards provide the basis for consistent public policy. They are founded on objectives that meet the test for: fairness, accountability, security, honesty, reliability, and safety.

1.00 GENERAL

1.01 Ownership and Control of Technical Gaming Integrity Document

The ownership and control of this document and all subsequent amendments rests with SLGA.

1.01.1 Document Revision

Technological change in the industry may require SLGA to issue corresponding amendments and changes to previously approved standards. Reasonable notice will be given to all manufacturers, suppliers, testing laboratories, and operators, for implementation.

1.02 Parameters of Document

To create a standard which will ensure that raffle ticket(s) sold through the Internet are fair, secure and able to be audited and operated in accordance with SLGA as the regulator. This document is intended to outline those standards that apply to the sale of raffle ticket(s) through the Internet.

1.03 Technology

SLGA recognizes that game technology changes. New technology will be evaluated, as required, and the standards amended accordingly, as per **1.01.1 Document Revision** of this document.

1.04 Regulatory Requirements

General

All on-line raffle ticket sales systems, software and database requirements must be tested by an independent test laboratory approved by SLGA to meet the applicable requirements set forth in this document.

Manuals

Operation manuals and service manuals must be expressed in broad terms that are directly relevant to the system used to sell raffle ticket(s) through the Internet and must be provided at the request of SLGA.

a) Operational manuals associated with the applicable system;

b) Technical Service manuals which:
   i. Accurately depict the system for which the manual is intended to cover.
   ii. Provide adequate detail and be clear in their wording and diagrams to support interpretation by SLGA personnel;
   iii. Include a maintenance schedule outlining the elements of the system that require maintenance and the frequency at which that maintenance should be carried out;
   iv. Include a maintenance checklist that enable appropriate staff to make a record of the work performed and the results of the inspection; and
   v. Include a complete list and samples of available reports that can be generated by the system.

c) Technical documentation that must provide adequate detail and be sufficiently clear in wording and diagrams to enable the review /evaluation of the system used.

d) Complete documentation for programming patches, fixes and any upgrades made to the system.

2.00 GEOLOCATION

The Raffle System, Online Purchasing Platform and/or the Patron Device must be able to reasonably detect the physical location of an authorized patron attempting to access the service. Third parties may be used to verify the location of patrons as allowed by the regulatory body.

3.00 ON-LINE RAFFLE TICKETS

3.01 Inventory

When issued a charitable gaming license to conduct a raffle, the charitable organization will provide the number of raffle tickets available for sale through the Internet. The Raffle system software is required have the ability to set time limits for which tickets may be purchased. Upon completion of the sale of the final raffle ticket for a charitable organization raffle, the raffle must close.

4.00 SYSTEM REQUIREMENTS

4.01 Due Diligence

Systems used by the Purchaser to obtain raffle ticket(s) through the Internet must be designed to be as impervious to communication errors as possible. Personally identifiable information, sensitive account data and financial information must be protected over a public network. Every effort must be made to provide documentation for specific actions or precautions that can be undertaken to further limit communication errors.

4.02 Asset Management

All assets housing, processing of communication controlled information, including those comprising the operating environment of the Raffle system and/or its components, should be accounted for and have a designated "owner" responsible for ensuring that information and assets are appropriately classified, and defining and periodically reviewing access restrictions and classifications.

4.03 Raffle Equipment Security

Raffle system servers must be located in server rooms which restrict unauthorized access. Raffle system servers shall be housed in racks located within a secure area**.**

4.04 Network Security Management

To ensure Purchasers are not exposed to unnecessary security risks by choosing to participate in raffles. These security requirements must apply to the following critical components of the Raffle system:

a. Raffle system components which record, store, process, share, transmit or retrieve sensitive Purchaser information, e.g. credit card/debit card details, authentication information, patron account balances;
b. Raffle system components which store results of the current state of a Purchaser's purchase order;
c. Points of entry to and exit from the above systems (other systems which are able to communicate directly with the core critical systems); and
d. Communication networks which transmit sensitive patron information.

Networks should be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link.

a) The failure of any single item should not result in denial of service;
b) An Intrusion Detection System/Intrusion Prevention System must be installed on the network which can:
    i. Listen to both internal and external communications;
    ii. Detect or prevent Distributed Denial of Services (DDoS) attacks;
    iii. Detect or prevent shellcode from traversing the network;
    iv. Detect or prevent Address Resolution Protocol (ARP) spoofing; and
    v. Detect other Man-in-the-Middle indicators and server communications immediately if detected.
c) Stateless protocols (e.g. UDP) should not be used for sensitive data without stateful transport; ***NOTE: Although HTTP is technically stateless, if it runs on TCP which is stateful, this is allowed.***
d) All changes to network infrastructure (e.g. network device configuration) must be logged;
e) Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses;

f) Network security should be tested by a qualified and experienced individual on a regular basis; and
g) Testing should include testing of the external (public) interfaces and the internal network.
h) Testing of each security domain on the internal network should be undertaken separately.

4.05 Communication Protocol

On-line raffle ticket(s) offered for sale by a licensed charitable organization must support a defined communication protocol(s) that ensures Purchaser(s) are not exposed to unnecessary security risks when using the Internet for this purpose. Each component of a Raffle system must function as indicated by the communication protocol implemented. The system must provide for the following:
a) All critical data communication shall be protocol based and/or incorporate an error detection and correction scheme to ensure accuracy of messages received;
b) All critical data communication shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication;
c) Communication between all system components must provide mutual authentication between the component and the server;
d) All protocols must use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent eavesdropping and tampering. Any alternative implementations are to be reviewed on a case-by-case basis, with regulatory approval; and
e) All data communications critical to raffle ticket sales through the Internet shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.
The Secure Sockets Layer (SSL) and Secure Hash Algorithm (SHA-1) are commonly-used protocols for managing the security of a message transmission on the Internet and are considered a minimum requirement by SLGA.

4.06 Remote Access

Remote access is defined as any access from outside the system or system network including any access from other networks within the same establishment. Remote access shall only be allowed if authorized by the regulatory body and shall have the option to be disabled. Where allowed, remote access shall accept only the remote connections permissible by the firewall application and on-line raffle ticket sale(s) settings. Remote access security is to be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the local regulatory body. In addition, there shall be:
a) No authorized remote user administration functionality (adding users, changing permissions, etc.);
b) No authorized access to any database other than information retrieval using existing functions;
c) No authorized access to the operating system; and
The raffle system must maintain an activity log which updates automatically depicting all remote access information.

4.07 Error Recovery

The system used by a licensed charitable organization to offer the sale of raffle ticket(s) through the Internet must be able to recover messages when they are received in error. This would include inaccurately inputting personal/banking information which would result in the Purchaser being notified that the information is invalid and must require review and corrective measures. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system information from the last viable backup point and fully recover the contents of that backup, including, but not limited to:

a) Significant events;
b) Accounting information;
c) Reporting information; and
d) Specific site information such as employee file, raffle set-up, etc.

4.08 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for bi-directional data. With the requirement of "two-way communication" where personal/banking information is transferred bi-directionally through a communication link, the security of the system is paramount. Any system used to sell raffle ticket(s) through the Internet shall ensure that:

a) The physical network is designed to provide exceptional stability and limited communication errors;
b) The system is stable and capable of overcoming and adjusting for communication errors in a thorough, secure and precise manner; and
c) Information is duly protected with the most secure forms of protection via encryption, segregation of information, firewalls, passwords and personal identification numbers.

4.09 Encryption

Security messages that traverse data communications lines must be encrypted using an encryption key(s). The intent is that communications be demonstrably secure against crypto-analytic attacks. The encryption key(s) used to provide security to the system that provides for the sale of raffle tickets through the Internet must be monitored and maintained:

a) There must be a documented process for obtaining or generating encryption keys;
b) If encryption keys expire there must be a documented process for managing the expiry of the encryption keys;
c) There must be a documented process to revoke encryption keys;
d) There must be a documented process for securely changing the current encryption keyset;
e) There must be a documented process in place for the storage of any encryption keys; and
f) There must be a method to recover data encrypted with a revoked or expired encryption key for a defined period of time after the encryption key becomes valid.

4.10 Cryptographic Controls

Cryptographic controls must be implemented for the protection of information.

a) Any sensitive or personally identifiable information should be encrypted if it traverses a network with a lower level of trust;
b) Data that is not required to be hidden but must be authenticated must use some form of message authentication technique;

c) Authentication must use a security certificate from an approved organization;
d) The grade of encryption used should be appropriate to the sensitivity of the data;
e) The use of encryption algorithms must be reviewed periodically by qualified Management staff to verify that the current encryption algorithms are secure;
f) Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical. If no such changes are available, the algorithm must be replaced; and
g) Encryption keys must not be stored without being encrypted themselves through a different encryption method and/or by using a different encryption key.

4.11 Firewalls

a) A firewall should be located at the boundary of any two dissimilar security domains.
b) All connections to hosts used for the sale of raffle tickets through the Internet must be housed in a secure data centre and must pass through at least one application-level firewall. This includes connections to and from any non-related hosts used by the operator.
c) The firewall must be a separate hardware device with the following characteristics:
    i. Only firewall-related applications may reside on the firewall; and
    ii. Only a limited number of accounts may be present on the firewall (e.g. system administrators only).
d) The firewall must reject all connections except those that have been specifically approved.
e) The firewall must reject all connections from destinations which cannot reside on the network from which the message originated (e.g. RFC1918 addresses on the public side of an internet firewall.)
f) The firewall must maintain an audit log of all changes to parameters which control the connections permitted through the firewall.
g) The firewall must maintain an audit log of all successful and unsuccessful connection attempts. Logs should be kept for 90 days and a sample reviewed monthly for unexpected traffic.
h) The firewall must disable all communication if the audit log becomes full.

4.12 Firewall Audit Logs

The firewall application must maintain an audit log and must disable all communications and generate a significant event if the audit log becomes full. The audit log shall contain:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

4.13 System Clock

The system used for the sale of raffle tickets through the Internet must maintain an internal clock that reflects the current date and time that shall be used for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of all sales.

5.00 ON-LINE RAFFLE TICKET SALES

5.01 General

Any system used for the sale of raffle ticket(s) through the Internet must have a device or facility that provides for the collection and accounting tools needed to determine all sales initiated through the Internet. The accounting information is subject to an operational and financial audit by SLGA.

5.02 Purchase Session

A purchase session consists of all activities and communications performed by a Purchaser during the time the Purchaser accesses the Raffle system/Online Purchasing Platform. Tickets can only be purchased during a purchase session.

5.03 Purchasing Tickets

A participant may purchase a raffle ticket from the website by following the instructions appearing on the screen and providing payment for the ticket(s). Each raffle ticket must be sold individually for the price indicated. Multiple discounted prices will only be allowed if a way of ensuring financial accountability is possible by the Online Purchasing Platform and/or Raffle system:

a) A ticket purchase via a credit card transaction or other methods which can produce a sufficient audit trail must not be processed until such time as the funds are received from the issuer or the issuer provides an authorization number indicating that the purchase has been authorized;
b) There must be a clear notification that the purchase has been accepted by the system and the details of the actual purchase accepted must be provided to the patron once the purchase is accepted; and
c) Purchase confirmation should include the amount of the purchase accepted by the Raffle system/ Online Purchasing Platform.

5.04 Disputes

The Raffle system/ Online Purchasing Platform must provide an easy and obvious mechanism to advise the patron of the right to make a complaint against the operator, and to enable the patron to notify the regulatory body of such a complaint.

5.05 Bearer Ticket Issuance

After the payment of a fee, the Purchaser shall receive a receipt through the Internet that the purchase of raffle ticket(s) is complete. Upon receiving the receipt acknowledging the raffle ticket(s) purchased through the Internet, the Purchaser can receive the raffle ticket(s) bought via e-mail. The receipt acknowledging raffle ticket(s) purchased and the issuance of the raffle tickets through the Internet must be processed as two (2) separate transactions.

5.06 Validation Numbers

The method used by the Raffle system to generate the bearer ticket validation number must be unpredictable and ensure against duplicate validation numbers for the raffle currently in progress.

5.07 Voiding a Ticket

If a ticket is voided, the appropriate information shall be recorded, which includes the draw numbers and the validation number pertaining to the voided ticket. Voided draw numbers shall not be able to be resold or reissued.

5.08 Raffle Drawing Requirements

A raffle drawing shall be held at a date, time, place and in a manner determined by the operator.

5.09 Winner Determination

The operator shall conduct a manual draw procedure which ensures a randomly selected draw number as a winner from all the tickets sold. Each drawn counterfoil shall be verified as a sold and valid ticket. Voided tickets shall not be qualified toward any prize. This process shall be repeated for each advertised prize.

5.10 Official Drawing Results

Results of the drawing become official and final after the drawn number is verified as a winning raffle ticket for the respective drawing and is presented to the participants for the raffle. The winning draw number shall be made available on the raffle website for the participants to review. Operators may utilize any additional methods in presenting the winning draw number(s) to the participants.

5.11 Accounting Requirements

Any system used for the sale of raffle ticket(s) through the Internet must have the capability to log sales and to print reports detailing sales and accounting information for specific dates and time periods must be available. This information can include, but is not limited to; price of raffle ticket(s), number of raffle tickets sold, total sales, etc. The system or other equipment shall be capable of producing accounting reports to include the following information:

a) Data required to be maintained for each raffle drawing, including:
    i. Date and time of event;
    ii. Organization running the event;
    iii. Sales information;
    iv. Value of prize(s) awarded;
    v. Prize distribution;
    vi. Refund totals of event;
    vii. Draw numbers-in-play; and
    viii. Winning number(s) drawn (including draw order, call time and claim status).

b) Exception Report. A report which includes system exception information, including, but not limited to, changes to system parameters, corrections, overrides and voids.

c) Bearer Tickets Reports. A report which includes a list of all bearer tickets sold including all associated draw numbers and selling price.

d) Sales Report. A report which includes a breakdown of sales of raffle ticket(s) through the Internet, including draw numbers sold and any voided and misprinted tickets.

e) Voided Draw Number Report. A report which includes a list of all draw numbers that have been voided including corresponding validation numbers.

f) Event Log. A report which lists all events recorded specific to the sales of raffle ticket(s) through the Internet. This will include the date and time of the transaction and a brief description of the transaction and/or identifying code.
g) Corruption Log. A report which lists all Internet transactions that were unable to be reconciled to the system.

5.12 Sales and Accounting Report Requirements

Any raffle ticket(s) sold must be included in the sales and accounting reports and be detailed in all financial transactions on the system. In addition, a log relating to accounting and raffle ticket sales must be maintained on the system. The charitable organization conducting the raffle shall be given the option of printing this log on demand.

5.13 Backup Requirements

Any system used for the sale of raffle ticket(s) through the Internet must have a backup and archive utility to allow the licensed charitable organization, conducting the raffle, the ability to save critical data should a system failure occur. This backup can be automatically run by the charitable organization.

5.14 Data Alteration

The alteration of any accounting, reporting or significant event data related to the sale of raffle tickets through the Internet will not be permitted without supervised access controls. In the event any data is changed, the following information will be logged documented, stored and available upon request for review:

a) Data element altered;
b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and date of alteration; and
e) Personnel that performed alteration (user login)

5.15 Access Controls

The allocation of access privileges shall be restricted and controlled on business requirements and the principle of least privilege.

a) A formal user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services.
b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
c) The use of generic accounts shall be limited, and where used for reasons for their use shall be formally documented.
d) Password provision must be controlled through a formal management process.
e) Passwords must meet business requirements for length, complexity and lifespan.
f) Access to system applications shall be controlled by a secure log-on procedure.
g) Appropriate authentication methods, in addition to passwords, shall be used to control access by remote users
h) Any physical access to areas housing components used for the sale of raffle ticket(s) through the Internet application and any logical access to these applications must be recorded.

i) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be formally documented and must be included in the regular review of access by Management.
j) Restrictions on connection times shall be used to provide additional security for high-risk applications.
k) The use of utility programs that might be capable of overriding system application controls shall be restricted and tightly controlled.
l) A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

6.00 PURCHASER ACCOUNT REGISTRATION

6.01 General

The Raffle system/Online Purchasing Platform must employ a mechanism to collect (either online or via a manual procedure approved by the regulatory body) Purchaser information prior to registration of a Purchaser account. The Purchaser must be fully registered and their account must be activated prior to permitting ticket purchases.

6.02 Establishment of Purchaser Account

Once the identity verification is successfully complete, and the Purchaser has acknowledged all of the necessary privacy policies and the terms and conditions, the Purchaser account registration is complete and the patron account can become active.

7.00 THIRD PARTY SERVICES

Any third-party service providers contracted to provide service involving accessing, processing, communicating or managing the sale of raffle tickets through the Internet must adhere to information contained in this document. The security roles and responsibilities of third party service providers should be defined and documented as it relates to the security of information.

a) Agreements with third party service providers involving accessing, processing, communicating or managing the purchase of on-line raffle tickets through the Internet/or its components, or adding products or services to the system used/or its components shall cover all relevant security requirements.
b) The services, reports and records provided by the third party shall be monitored and reviewed by SLGA upon request.
c) Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
d) The access rights of third party service providers to the system and/or its components shall be removed upon termination of their contract or agreement, or adjusted upon change.

8.00 DEFINITIONS

Access control is the restriction of access to a place or other resource. Locks and login credentials are two mechanisms of access control.

Address Resolution Protocol (ARP) is the protocol used to translate IP addresses into MAC addresses to support communication on a LAN (Local Area Network). The Address Resolution Protocol is a request and reply protocol and it is communicated within the boundaries of a single network, never routed across internetwork nodes (connection points, either a redistribution point or an end point for data transmissions).

Algorithm is a finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.

Authentication is a security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message or originator.

Bi-Directional is the ability to move, transfer or transmit in both directions.

Counterfoil is an electronic record or paper ticket stub, also known as a barrel ticket, which will be drawn to determine a winner and contains a player's draw number matching the bearer ticket purchased and may, depending on the type of raffle, contain the name, address, or telephone number of the player.

Crypto-analytic is an attack against the encryption key (refer to definition of encryption key).

Cryptographic is anything written in a secret code, cipher, or the like.

Distributed Denial of Service (DDoS) is a type of DoS attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Domain used to identify one or more IP addresses. A domain name is used in a URL (Uniform Resource Locator) to identify particular Web pages.

Encryption is the reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity.

Encryption Key is a sequence of numbers used to encrypt or decrypt (to decode/decipher) data.

Firewall is any number of security schemes that prevent unauthorized users from gaining access to a computer network or that monitor transfers of information to and from the network.

Geolocation refers to identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor.

Host refers to a computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal. A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IEEE 802 refers to a family of IEEE (Institute of Electrical and Electronic Engineers) standards dealing with local area networks (a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media) and metropolitan area networks(a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN).

Internet is an interconnected system of networks that connects computers around the world via the TCP/IP protocol. TCP/IP protocol is short for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in your system.

IP Address is short for Internet Protocol address and is an identifier for a computer or device on a TCP/IP network.

MAC Address short for Media Access Control address is a hardware address that uniquely identifies each node (a computer/printer) of a network.

Man-in-the-Middle (MITM) is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.

Message Authentication is a security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

On-line refers to being connected to the Internet.

On-line Purchasing Platform refers to the Raffle System hardware and software which drives the features common to all raffles offered, and which forms the primary interface to the Raffle System for both the patron and the operator. The On-line Purchasing Platform provides the patron with the means to register an account, log in to/out of their account, modify their account information, make ticket purchases, request account activity statement/reports, and close their account. In addition, any web pages displayed to the patron that relate to ticket purchasing offered on the Raffle System. The On-line Purchasing Platform provides the operator with the means to review patron accounts, enable/disable raffles, generate various raffle/financial transaction and account reports, input raffle outcomes, enable/disable patron accounts, and set any configurable parameters.

Protocol (Communication) is a set of formal rules describing how to transmit or exchange data, especially across a network. TCP/IP is the standard communications protocol of the Internet and most internal networks.

Raffle a form of lottery in which a number of persons buy one or more chances to win a prize.

RFC 1918 are standards related to the use of Internet addressing, private IP address space and the use in a private network.

SHA-1 (Secure Hash Algorithm) is a cryptographic hash function (an algorithm that maps data of variable length to data of a fixed length) designed by the United States National Security Agency and is used for the protection of sensitive unclassified information. The SHA-1 algorithm takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value.

Shellcode is a small piece of code used as the payload (cargo of data transmission) in the exploitation of computer security. Shellcode exploits a vulnerability and allows an attacker the ability to reduce a computer system’s information assurance.

Security Certificate is information, often stored as a text file, that is used by the SSL (Secure Socket Layers) Protocol to establish a secure connection. A Security Certificate contains information about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate. In order for an SSL connection to be created, both sides must have a valid Security Certificate, which is also called a Digital ID.

Stateful firewall is a firewall that keeps track of the state of network connections traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected. Stateful inspection, also referred to as Dynamic Packet Filtering, is a security feature often included in business networks

Stateless is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol which requires the keeping of internal state is known as a stateful protocol. Examples of stateless protocols include Internet Protocol (IP) and the Hypertext Transfer Protocol (HTTP).