Payment Transactions Security & Enforcement

A REPORT FROM NEWNET COMMUNICATION TECHNOLOGIES, LLC
NewNet Payment Systems & Transaction Security Enforcements

NewNet offers payment transaction transport solutions for secure transaction aggregation, routing & switching of the card/wallet based transactions originating from dial, broadband and mobile POS/POI devices or web/mobile web based payment devices and securely transport these transactions to authorization servers for timely approval of these transactions utilizing the most secure means for transport.

Security is handled with paramount importance on NewNet Secure Transaction Transport products, services and applications for all types of innovative mobile, broadband and legacy dial transaction services. This involves the data security as well as the network security and barriers to prevent, deter and detect attempts to intrude. With applications having full know how of the transaction protocols and applying advanced methods of deep packet inspection and verification of transaction protocols and data, NewNet products ensure that the mobile, broadband and dial transaction users and providers can be assured of the security of the transactions. NewNet systems are fully compliant to PCI DSS standards to enforce high level of commitment to security compliance.

Transaction Security Enforcement Mechanisms

Broadly the security mechanism is enforced in several layers including the following categories involving location facilities and system controls.

- **Device Security** – physical locks/camera/room enclosures
- **Data Security** – Encryption/data integrity checks/source verification
- **User Security** – user logins/password
- **Network Security** – access controls and logging of user action
- **Storage Security** – access restriction to stored data
- **Transport Security** – security throughout the way
- **Session Security** – end to end session security from originating device to the final authorization server

The system security measures are further qualified in terms of the nature of the security applicable and their nature like

- Key strengths
- Reversibility of encryption
- Brute force attack resistance
- Sustained attach resistance
- Attack detection
- Deterrence mechanism
- Alternative defensive mechanisms
- Alerts & time sensitivity
- Logs & Audit Trail scans

NewNet systems employs a wide array of security processes, transaction user data safety and monetary loss avoidance procedures which make the best use of the industry standards and beyond the industry specifications including digital certificates, PIN numbers, TLS/SSL sessions, userid & passwords, multi-factor authentication, split key authentications, advanced cryptographic standards, longest key length encryptions, dynamic access controls, SSH access, multiple device verifications, real time reporting, transaction verifications on-the-fly, transaction value based verifications, end to end encryption, secondary data encryption, IPSec tunneling, multi-layer user approval requisitions, 2D barcode tokens, PKI procedures etc.
The following elaborate process as part of NewNet solutions establishes security of transactions:

- Data encryption support and secure sessions from POS
- Strong encryptions support
- POS/POI device Authorization using Certificates
- Tokenization of sensitive data at first presentment
- Point To Point Encryption of transaction data
- Extending PIN encryption process to card data security
- User authentication from POI/POS devices
- Notifications on clear text availability of sensitive data
- User access restriction to network and transport systems handling payment data
- User access logging of all systems accessing payment data
- Alarm notifications for sensitive data access in transit
- Memory and File monitoring systems
- Network security and perimeter fencing of sensitive environment
- Blocking of all application execution outside of core payment application
- Stoppage and alerting on all other executables attempting execution
- HW processor usage for all cryptographic operation
- Non retention of sensitive data in memory even during transient stages
- Permanent blocking of sensitive data in raw form
- External firewalls to prevent probes and injections
- TCP port restrictions and service restrictions even on permitted ports
- Data masking and avoiding system storage
- Physical device protection including restriction of physical ports for connecting devices/cables/connectors
- Security standards compliance and periodic validations based on PCI DSS requirements

Transaction Security – Relentless Practice & NewNet Methodology

Most fundamental aspect of security is that it is not a one off process or not something to be set in place and forgotten, but it is effectively a way of doing business, just as important as it is to conduct business. Cost of implementing and maintaining security in practical estimations based on the emerging risks presented by newer malware when used against aging systems at retailers, merchants, acquirers, processors and banks etc turns out to be far lesser than the cost of overcoming a data breach if it were to happen. Apart from the cost which could be huge depending on the volume of business that an enterprise may be conducting and the volume of card data that may be traversing the merchant’s information technology systems, the additional non tangibles damages in terms of the loss of confidence by partners, business associates and the very aspect of being an example to be referenced forever as a stunning example of criminal negligence on security practices will render a long standing scar on such enterprises which could be targeted and fall victims to such data breaches, and which is at best avoided.

NewNet recommended high level practices for sensitive payment information includes:

- Encrypt card data at the point of presentation with strong encryption
- Never decrypt the card data at any point in the transport network
- Avoids the need to store credit/debit card data on POI devices or associated systems
- Prevents the transfer of sensitive card data across public networks
- Leaves no card information with the merchant terminals
- Ensures that card data remains on secure databases and accessed over secure private networks
- Clear delineation of sensitive data boundaries and hardened controls on all systems within this boundary
- Firewalled fences for any and all access to systems in the sensitive zone and real time monitoring of such access
The following processes listed below as part of NewNet solution deployments ensures that the established security is remaining intact:

- Monitor the systems handling sensitive card data and block all user access and permit access on need to know basis
- Establish responsibility matrix for systems and users operating in card data environment with daily review of audit logs
- Prevent all unencrypted exposure to sensitive data and shutdown and report any such gaps
- Review the dataflow path and data resident locations in the card data environment and networks and sanitize all applications remotely interacting with this traffic
- Apply patches and protection software and maintain the systems and environment updated periodically
- Enhance the solutions in real time as better, stronger methods of security, encryption, data masking are introduced
- Continuous security process verifications based on PCI DSS and similar security standards bodies

**NewNet Transaction Security Solutions**

NewNet payment transaction solutions specifically addressing security of transactions are listed below:

**P2PE (Point To Point Encryption)**

NewNet’s TransKrypt security server system offers the P2PE solution for Acquirers/Processors and Service Providers working in conjunction with approved point of interaction devices that are certified for usage in a P2PE environment. The P2PE solution supported by NewNet’s TransKrypt Security Server is based on ANSI X9.24 standards specified DUKPT mechanisms.

The NewNet TransKrypt Security Server utilizes FIPS 140-2 Level 2 HSM solution to store sensitive data like encryption keys securely and provide encryption and decryption capabilities. TransKrypt solution provides P2PE capability for Terminal Line Encryption using Derived Unique Key Per Transaction (DUKPT); working in conjunction with the NewNet AccessGuard and Total Control STG systems which aggregates, switches and routes transaction from POS devices.
Tokenization
NewNet’s secure transaction solutions provide an integrated cost-effective solution for tokenization of sensitive data. Tokenization is a process by which the primary account number (PAN) or other sensitive data is replaced with a surrogate value called a token. De-tokenization is the reverse process of redeeming a token for its associated PAN value. The tokenizer application provides an interface for tokenizing the input data string into desired length. Similarly the token can be converted back to the original data if required.

NewNet’s Tokenization application is an optional part of the Security Server provided by NewNet for its customers in order to enable them to tokenize sensitive data. The application can be installed as part of the Security Server platform which complies with the security requirements. Tokenization solution uses HSM module which is a tamper proof device to store keys used for the tokenization. The HSM module ensures that the encryption keys reside on a secure device and cannot be accessed or tampered with without destroying the module. The tokenization solution need to be installed in a secure location and will talk with other authorized systems using TLS/SSL with valid certificates. Merchants can use the tokenization solution to reduce the PCI-DSS scope by storing transaction data with a token instead of the PAN, as recommended by PCI.

Secure Server Sessions (IPsec/TLS/SSL)
IPsec is offered for secure connection between AccessGuard 1000 / Total Control STG (AG1K/TC STG) and peer Servers or Host Servers. This includes secure connections from AG1K/TC STG systems to Authorization Host servers, Network nodes, VPN servers etc or among AG1K system. IPsec is also employed between TC STG and AG1K systems in a secure IP connection model based network architecture that connects them from a remote site to central site with TC STG or AG1K in a remote site and AG1K in a central site.

Similar to SSL usage with client POS/POI devices, TLS/SSL may be used with Host servers as well. While for permanent connections with Host servers, typically IPsec is preferred. IPsec (Internet Protocol Security) comprises of a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of IPsec is to provide security between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway); it can also provide end-to-end, or host-to-host, security.
Secure POS/POI Sessions (TLS/SSL)

NewNet’s AccessGuard 1000 solution can aggregate thousands of persistent and non-persistent TLS/SSL/IPSec connections and transactions. TLS/SSL cryptographic protocol provides secure communications over the Internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. TLS/SSL involves a number of basic phases including peer negotiation for algorithm support; public key encryption-based key exchange and certificate-based authentication; symmetric cipher-based traffic encryption.

The NewNet AccessGuard 1000 solution uses next generation hardware acceleration encryption engines to achieve the performance required for the financial market. This implies that with AccessGuard 1000 TLS/SSL offloader the back end systems or additional network devices are not necessary for processing any portion of the TLS/SSL traffic. By processing the entire TLS/SSL transaction, AccessGuard 1000 uses a model of receiving encrypted data from POS, decrypting transaction data, routing the transactions data based on specific transaction protocols securely over TLS/SSL/IPsec sessions towards the host system.

Client/Server Certificate Authorization

NewNet’s Certificate Authorization system is an optional application package provided for customers in order to enable them to create and verify client certificates for their POS devices and other payment processing devices in conjunction with TLS/SSL. The package is used on industry grade Server system with secure storage capabilities.

Certificate Authorization system is intended to be used as special purpose certificate authority (CA) server for acquirers, processors and service providers. This is expected to be used within a payment processor organization to ensure that devices that talk to each other via secure connections (TLS/SSL, SSH etc) are authenticated via valid certificates and thus prevent man-in-the-middle (MITM) attacks. This server application consists of CRL distribution servers as well to track the certificate validity of client devices and servers.
Strong Encryptions
AES (Advanced Encryption Standard) is an advanced specification for the encryption that supports key size of 192, 256 and 512 bits. 3DES (Triple DES) is a version of DES that encrypts a message three times using the DES 56-bit key, which is effectively 168-bit key encryption. Couple with stronger encryption mechanisms, using larger key lengths for Certificates up to 2048 bits further increases the security of the sessions.

Considering the computationally intensive operations of these strong encryption methods, NewNet systems uses next generation hardware acceleration encryption processor engines to achieve the high performance and rapid transaction handling required for the financial market.

About NewNet Communication Technologies
NewNet Communication Technologies, LLC is a global provider of innovative solutions for next generation mobile technology. For over 25 years, NewNet has enabled global operators and equipment manufacturers to rapidly develop and deploy cutting edge, revenue generating solutions needed to build, grow and improve global communications.

NewNet specializes in Mobile Messaging, Secure Transaction Transport, Interactive Voice Response, Real Time Charging and Rating, Wireless Broadband and Network Optimization solutions that have reached millions of end users in over 90 countries.