Traxcom Technologies LLC

AccessGuard 500

Application Brief

1. OVERVIEW

Internet Protocol (IP), which is the de facto standard for transmitting data over the internet, has set new visions and directions for 21st century payment system network architecture. As the industry is converging to IP-centric products and services, more financial institutions, insurance companies and businesses around the world are using the internet to offer products and services or otherwise enhance communications with its members. Internet based transactions have many obvious advantages over traditional telephone line based transactions. The potential to reduce the transaction costs, improve transaction time, and increase the payload size are regarded as a major driving force for financial institutions to switch over to the internet.

However, the internet is a public network and the basic IP protocol lacks even the most basic mechanisms for security, such as authentication, message integrity, and data confidentiality. Financial institutions need to make good choices with regards to security without compromising the performance and the safeguarding of the information it collects to avoid scams and costly surprises. Therefore, the network infrastructure they choose must be highly secured.

The solutions from UTStarcom deliver these fundamental security capabilities to enable safe and convenient ways to conduct financial transactions, data collection, security verification and custom applications over the internet any day, any time.

This application brief focuses on the UTStarcom solution for the next generation financial transaction market. This solution interconnects the existing legacy bank host systems to the internet based Point of Sales (POS) terminals.

2. CHALLENGES IN INTERNET BASED TRANSACTIONS

As usage of the Internet for business and financial transactions increase, their lack of built-in security has become more and more problematic.

Any security product portfolio for financial services over the internet should address the following fundamental security issues, such as

- Authentication (Person’s identity is ensured)
- Authorization (Person is allowed to have access to data)
- End-to-end Encryption (data confidentiality)
- Digital Signatures

In addition to the fundamental security services, knowledge in each application is very critical to provide a cost effective solution. As an example, in Point of Sale (POS) networking it is common for some of these systems to require specific implementation and customization. Due to this, a generic product that provides just internet security may not be suitable for financial transactions.

When evaluating systems for transaction processing, we should look for which technology or system is best suited for this need. When replacing the existing system with newer technology we should evaluate if we just interconnect and integrate this existing system with just new services. There is a significant business risk and costs associated with just simply discarding the legacy system and replacing it with a brand new system. For example, in financial transactions where the legacy hosts works on X.25 network moving the transactions to over the internet requires the host server to support all the security requirements of a next generation IP infrastructure.

Other challenges include adding scalability and redundancy without sacrificing overall performance. Security transactions include cryptographic encryptions which impacts on the CPU. This would limit the number of transactions and response time required.

3. TECHNOLOGY

3.1 Secure Sockets Layer (SSL)

SSL is a cryptographic protocol which 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.

SSL involves a number of basic phases:

- Peer negotiation for algorithm support
- Public key encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

3.2 Encryption Algorithms

The most widely used encryption algorithms for SSL are RC4 and 3DES.

RC4 is a stream cipher developed by RSA Data Security, Inc. The key-length is variable but typically used are 40 bits and 128-bit.

DES is a block cipher algorithm developed by the National Institute of Standards and Technology (NIST) Data Encryption Standard. DES has a fixed key length of 56 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.

3.3 Key Exchange Algorithm

Symmetric key cipher requires a key to be used to encrypt the communications. This means, the two parties that have no prior knowledge of each other have to jointly establish a shared secret key for encryption over an insecure communications channel.

The most widely used algorithms for exchanging or generating shared key at both ends of the communications link are RSA and Diffie-Hellman.

Diffie-Hellman is a key agreement protocol, where the algorithm generates a shared secret at both ends of the communications link.
RSA is a public-key cipher, which work as a key transport protocol, where the algorithm sends out a secret key to the other end of the communications link.

3.4 Digital Certificate

Key agreement or key transport schemes are vulnerable to man-in-the-middle attacks. A solution to this problem is to send the public key over the communication link using a signed certificate.

A certificate is a document that contains, along with the public key of the sender, the name of the certificate holder as well as the digital signature of an independent and trusted third party, called certification authority (CA), to ensure the validity of the transmitted information. The certificate format is usually based on ITU-T recommendation X.509.

During SSL negotiation, certificates are exchanged for public key information. These certificates validated with CA. Upon validation, this public key is used for ‘shared key` generation for symmetric encryption.

3.5 SSL Acceleration

SSL acceleration is a method of offloading the processor-intensive public key encryption algorithms involved in SSL transactions to a hardware accelerator. The SSL Accelerator solves the problem of server (host) slowdowns caused by running SSL in software using the host CPU. Typically, this is a separate co-processor, specifically designed for handling encryption algorithms using parallel processing at very speed.

3.6 SSL Offloading

SSL offloading may look very similar SSL acceleration. The term “offloading” is generally used to describe a completely separate computer that performs all SSL processing, so that the SSL load is taken off of the server completely. In a sense, an SSL hardware accelerator is performing SSL offloading, because part of the SSL processing is “offloaded” from the server’s CPU to the hardware accelerator. An advantage of an offloader, as opposed to the typical accelerator, is that it can do SSL processing for more than one transaction server, whereas the accelerator card is tied to a single server.

Traxcom Technologies LLC

4. ADDRESSABLE MARKETS

Internet security touches the very heart of the new economy and markets. UTStarcom's security solutions can be used in the following market to provide secure financial transactions, data collection and custom applications over the internet.

- Financial
    - Electronic fund transfer (EFT)
    - Electronic data interchange (EDI)
    - Electronic benefits transfers (EBT)
    - Electronic trade confirmations (ETC)
- Insurance
    - Data collection
- Health
    - Medical Records transaction
- Airline
    - Reservation
- Security
    - Pin encryption and verification for transactions
    - ID verification
    - Security verification
- General
    - Data collection
    - Custom applications

5. UTSTARCOM AccessGuard 500 SOLUTIONS FOR THE FINANCIAL MARKET

Traditionally, POS based transactions are initiated by POS devices dialing into the PSTN, which then transfer data via standard V, series modulations using VISA I, VISA II and similar protocols. As the industry moves to an all IP architecture and edge POS devices convert to IP only devices, the need to aggregate and securely transport this information back to a central server is required. UTStarcom AccessGuard 500 is designed to meet this specific market, as it will provide a secure means of connecting edge IP POS devices and securely transporting the information to hosts over the insecure internet.

In this next generation network, a merchant has one or more IP enabled POS devices sharing a high speed public internet link (Cable or DSL modem). AccessGuard 500 supports transaction protocols like VISA I, VISA II, ISO 8583, TPDU (Transport Protocol Data Unit), and Custom Protocols, which expedites the financial transactions. AccessGuard 500 terminates SSL sessions that are originated from the IP supported POS. In this model, the acquiring bank host system continues to operate in the same model as it was operating with the legacy transaction mode.

As such, AccessGuard 500 brings:

- Cost reductions of transactions
- Security to the insecure IP POS terminals
- Interconnect the legacy bank host computer with the next generation IP POS terminals.
- Aggregate the connections for saving host's resources.
- Simplified solution
- CAPEX savings to avoid hosts replacement using the public internet.
- Safe guard sensitive credit card data during its AccessGuard 500 over public internet.
- Offer opportunity to provide more value add services
- Faster transactions with the help of state of art hardware accelerator.
- Highly scalable for location based growth
- Redundancy for network disasters: record recovery

5.1 SSL Offloading

UTStarcom AccessGuard 500 solution uses next generation hardware acceleration encryption engines to achieve the performance required for the financial market. This means that with AccessGuard 500 SSL offloader, the host system is not responsible for processing any portion of the SSL traffic. By processing the entire SSL transaction, AccessGuard 500 uses a model of encrypted-data-in from POS to decrypted-data-out towards the host system.

5.2 SSL Aggregation

The UTStarcom AccessGuard 500 solution can aggregate thousands of persistent and non-persistent SSL connections and transactions. AccessGuard 500 can also support sessions re-use, introduced in SSLv3, which is used to reduce the burden of establishing a new SSL session by reusing previously established SSL Session ID's.

5.3 Redundancy & Load Sharing

UTStarcom AccessGuard 500 solution is designed to eliminate the single point of failure inherent in the IP environment. AccessGuard 500 can support VRRP (RFC 2338), which provides dynamic fail-over in the forwarding responsibility, should one AccessGuard 500 become unavailable. This provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every IP POS devices.

AccessGuard 500 can also be integrated with DNS server to support DNS round robin for load.

Traxcom Technologies LLC
621 Busse Road, N IL RT 83, Suite 260
Bensenville, IL 60106
Tel: 1-630-521-9630
Fax: 1-630-521-9642
www.traxcomtech.com