ATM Interfacing

Introduction

ATM (Automatic Teller Machines) are merely computers in a large secure enclosure that handle normal banking transactions. The sole purpose is to provide customer services 24 hrs a day 7 days a week 365 days a year at many locations dispensing money. These basic facts make ATMs targets for theft and violent crimes. With the use of CCTV and ATM interfaces most problems with ATMs can be solved.

ATM Interface

An ATM interface is an electronic device that monitors transactions made on an ATM machine and superimposes or overlays this data on the video picture of the customer making the transaction. The Time and Date is also recorded to verify when the event occurred. This video overlay along with the transaction data is recorded on a DVR for later review when a question arises.

ATM Fraud

There are many ways to defeat or fraud monies from ATM machines.

- **Fake Cards**
  Most bank employees can obtain internal records to produce additional bank ATM cards for themselves or their customers. With the use of this fake but functional card, the employee or accomplice can withdraw funds from any ATM. The only way to deter this type of fraud is to provide cameras, an ATM interface and DVR on the ATM.
- **Using the Law**
  Banking laws in the US protect the consumer when problems happen at the ATM. Our law states that if a customer has a discrepancy in their bank account the bank has a limited period to respond. In general if the bank can not proof the customer made the transaction, the bank has to absorb the loss and the customer only pays $50.00 total. A typical ATM fraud would be the following. You would deposit $5000.00 in a bank that had ATMs but no video on them. Everyday you would withdraw $200.00 or the maximum daily amount the ATM would allow. When you got your first statement you would protest it to the bank. If they could not prove it was you withdrawing the money you would get all the money back except $50.00. This scam would be repeated at the next bank.
- **Card Clips**
  Some ATMs are programmed that the money is not dispensed until the card is removed from the ATM. In this environment clever criminals have devised a clip that catches the card so it can not be ejected. The customer gets frustrated and leaves the ATM after not getting back their card or money after attempting a withdrawal. The criminal then quickly inserts the special release card and the customer card is ejected and so is the money. The criminal gets both card and money and reinserts the clip for the next customer. An added benefit to this technique is getting the ATM card also. Sometimes the criminal stands off to the side or across the street with binoculars and gets the customers PIN. Also “Good Samaritans” standby and pretend to help the customer or claim to be a bank official. They then watch them input the PIN code again to no use, but the criminal now knows the PIN number. He can then go to the same ATM or another and withdrawal funds with that card.
- **Fake Dispensers**
  Alternate plastic bezels for the money dispenser have been fabricated for certain models of ATMs. It is then attached over the internal dispenser with velcro. When the customer does a withdrawal the money is caught inside the phony dispenser. The customer again gets frustrated and leaves. The criminal then quickly removes the money and waits for the next customer.
- **The Hijack**
  Some bold criminals actual steal the ATMs from the installation they are in. This is done by front loaders clawing them out or trucks with chains destroying the kiosk and hauling away the ATM. They are later cut open with torches and the money stolen.
- **Violent Crimes Against Customers**
  The most common is obtaining a customers PIN numbers by standing behind them or via

binoculars. The customer is later pick pocketed, purse snatch or mugged. The criminal then withdraws as much money until the card is disabled.

More violent activities are when the customer, under threat of life, are required to withdraw money and give it to the criminal. If the criminal is not recorded on video or there exists no signs of forced withdrawal, the bank can sometimes comprise the position of the customer. The video would look like a normal withdrawal and the customer would be liable.

Sometimes customers are just robbed while leaving a ATM after a withdrawal. This is the reason most ATMs are in kiosks with outside cameras.

Other ATM Interface Uses

Alot of times customers withdraw money and just do not remember. Another major problem is family members or girl/boyfriends withdraw money from your account. This is easily forgotten or unknown. When the customer makes a protest and the bank replays the video, they are happy to know who it was and they remember. This is good customer service rather than just showing a ATM transaction log and expecting the customer to be satisfied.

- **Vandalism**
  The video in and around an ATM can also stop vandalism, spray painting and other types of juvenile type activity. ATMs are very expensive to replace and the repair of this type of damage is usually not covered under service policies.

How ATM Interfacing Works

An ATM interface connects between the video camera in the ATM and the recorder. The interface also taps the data from the ATM going to the modem which in turn connects to the central network. The interface extracts the transaction text from the data going to the modem and overlays that text on the video image of the customers face. Some ATMs have auxiliary ports that can connect directly to the interface.

Data Connections

- **Modem Taps**
  The most simplest and common data connection is between the ATM and the modem. There is usually one modem for each ATM, but sometimes there are modem sharing devices for multiple ATM and/or teller terminals on one high speed modem line. Most vendors supply a tap cable that connects directly to the rear of the modem and the ATM cable is then plugged back into the tap. Most ATM interfaces are passive devices and do not interfere with the data communications. Usually the interface reads both channels of data and extracts information from both channels to give an accurate on-screen text message similar to the printed receipt. When installing a tap on a modem, the ATM must not be disconnected for too long or the ATM may go off line. This is not a major problem and most ATMs will automatically come back on line in a few minutes.
- **TCP/IP LAN Taps**
  The more popular method of connecting ATMs to the bank network is via Ethernet LAN via TCP/IP. Banks have high network security and use VPN routers which communicate via one port only to the ATM. Therefore tapping this connection is the simplest and monitor the printer information for display in the video or record to the DVR. Banks can also configure for mirror ports for a dedicated port for the ATM interface and the DVR sharing one port.
- **Auxiliary Ports**
  Some ATM manufacturers provide auxiliary ports usually to control older style film cameras. These ports can be programmed to send certain data from the transaction out of this port. This type of connection is not popular since special cabling and ATM programming is required. One advantage is that these ports are not on the network which is more desirable by networks providers.
- **Journal Printer Tapping / Emulate**
  For unsecure ATM networks or uneducated bank officials the journal printer interface is used. This is an extremely poor method of interfacing since opening the ATM is required and 99.99% of all

EFT networks are DES encrypted and security can not be compromised with any ATM interfacing. Many networks do not even support local print journaling since the host does this electronically. This also requires a large mix of various interface devices in one network since most banks use various vendors of ATMs and all have different journal printers.

Video Connections

- **Single Camera**
  Most ATM video systems consist of a single camera mounted inside the ATM itself to capture the full view of the customer's face. This camera is then connected to the ATM interface which then connects to the DCR. This camera is usually of high resolution and has BLC (Back light compensation) built in. A small monitor is connected and used normally for test and playback.
- **Multi-Camera**
  In outdoor or kiosk mounted ATMs it is more desirable to have multiple cameras for observing the violent crimes. Usually one is mounted outside on the street looking at the ATM for walk up ATMS. For ATMs mounted in a kiosk usually one camera looks at the outside, one on the inside of the kiosk and one in the ATM. These cameras are usually connected through switchers and DVRs.

  The ATM cameras can also be integrated into the entire bank surveillance system for economic systems. With real time recording DVRs complete integrated ATM and branch surveillance is common place.

- **Alarming**
  Normally the ATM interface is programmed to alarm or close a contact when the transaction data is on the screen. This allows the DVR to record the ATM camera for a few pictures to guarantee a good image of the customer is recorded. This alarm is also connected to the DVR to change the recording speed to capture more pictures per second. This alarm signal will also mark the tape for later searching.

DVRs

- **Time Date Search**
  Most DVRs used for ATM surveillance have Time/Date search. This is of benefit when a bank manager needs to find a transaction quickly on tape. The transaction log from the ATM will give the Time and Date the transaction occured. The operator merely keys in this T/D and the DVR finds the transaction quickly. The alarming function is used in this type of DVR to change the record speed.
- **Transaction Text Search**
  Modern DVRs have ATM Transaction Search capability. This means the entire electronic journal of that ATM is stored on the DVR HDD delivered to the DVR via the ATM Interface. Remotely or locally bank officials can search the DVR database and playback or print out the transaction in question for viewing by the customer or law enforcement officer. Finding a particular transaction number or customer name is as simple as keying in the text and commanding the DVR to search.

ATM Interface Functions

All manufacturers of ATM interfaces do basically the same functions with various features differing from vendor to vendor. Some features to look for are:

- **Auto Configuring -**
  This is where a limited amount of interface setup is required to connect to a particular data network. There is no standard for auto configuring and all vendors require some type of initiation to auto configure.
- **Data Formatting -**
  Some vendors have a set format for the way the data is displayed on the video. Others have programming that can split parts of the data to top or bottom and erase unwanted data from displaying.

- **Alarming -**
  Contact closure output are available on most vendors equipment and is required to trigger VCRs or switchers. Some vendors have more than one for driving different devices.
- **Time/Date Genlock -**
  All interfaces display the T/D from the network when the data is on-screen. Some vendors genlock an internal clock to the host time and display it all then time. With this unit you can turn off the T/D on the DVR and be guaranteed the DVR T/D matches the ATM transaction log. Some DVRs can even gunlock to the ATM T/D.
- **Vertical Interval Encoding -**
  Some interfaces record the data in the vertical interval so as not to clutter up the video picture. The data can then later be read and reinserted into the video for printing. Others use this data for T/D or transaction number searching via special VCRs or multiplexers.
- **DVR Data Output -**
  Some vendors have auxiliary RS-232 ports that can send out the transaction data to the DVR to be recorded as an associated data file for later ATM Transaction data search.
- **Printer Output -**
  Some vendors have auxiliary RS-232 ports that can send out the transaction data to external devices like printers or phone line transmission equipment.
- **Exception Processing – Pre and Post**
  Some vendors have exception processing similar to cash register interfaces that alarm or export data only when certain conditions are met which is “Pre” exception processing. Other vendors can do “Post” exception processing so can narrow down the search parameters for specific search criteria.

ATM Network Communications

ATMs communicate with the modem via RS-232 type communications or Ethernet LAN connections. The serial communication can be one of the following types of protocol listed below. Modems are usually connected to dedicated leased telephone lines back to the network hub. Most ATMs and network communicate using a poll select technique. This means the host polls or asks each ATM in sequence if it has any data to send or tells a certain ATM the host has data to send it. If the ATM selects the host in response to a poll then the ATM transmits the data to the host. This is continuously repeated allowing multiple ATMs to share the same network.

- **Serial Communications**
  Serial communications are simply a series of voltage or current changes which are translated into the binary equivalents of 1 or 0s. After a series of this data is received, the computer reconstructs the serial data into its original binary format for computation.
- **Asynchronous**
  Asynchronous communications or simply assync , is usually called RS-232 communications. This generic RS-232 terms is over used because there are several types of asynchronous communications broken into electrical formats and/or protocol format. All assync communications consist of a pre-defined baud rate, a start bit, a defined number of stop bits and parity which determine the number of bits sent per frame or data packet.Standard RS-232 communications is most common in your home computers COM1-COM4 ports on the back of the computer. These ports connect to the mouse, modem or serial printer. RS-232 uses voltage swings from +12VDC to -12VDC to denote the transmission of 1s or 0s.
- **Synchronous**
  Synchronous data usually consists of a Data signal and a synchronous clock signal. With this format the baud rate is defined by the synchronous clock. The data stream is searched by byte by the receiver device and when the sync byte is detected the received is said to be in sync. At this type the receiver reads each successive byte to decode the proper data. This type of data is packetized, which means a sync byte heads up a certain amount of data.
- **Bisynchronous**
  Bisynchronous communications is very similar to synchronous, but varies in the protocol and packet information. This format has to detect two successive sync bytes or one word, for the stream to be in sync. The popular names for this format is 3270 or 3275. High Speed interprocessor communications can also be synchronous or bisynchronous. This is similar to the high speed assync method but the use of an external clock signal and sync bytes are used. This data rate can range from 38K to 10Mhz typically.

- **SDLC**
  Synchronous Data Link Communications (SDLC) is a high level communications technique that combines all of the above techniques. SDLC can contain high level protocol with multiple header and data identifiers. This format is similar to synchronous communications but searches the data stream bit by bit to identify a sync byte or word. Again this format is packetized with sync bytes and can contain packets from many sources and destinations.
- **NRZ/NRZI**
  None Return to Zero (NRZ) or None Return to Zero Inverted (NRZI) are common protocols for SDLC. These formats contain a separate clock signal for each data channel. Their electrical format is +12VDC to -12VDC similar to RS-232.
- **NRZId**
  None Return to Zero Inverted Derived Clock (NRZId) has the clock signal electrically embedded in the data signal. The receiver must lock on to this clock to generate the proper baud rate to read the incoming data stream.

LAN Networks

The trend in communications are Local Area Networks (LAN). These communications are usually high speed serial communications. Data and electrical format vary radically but most are based on variations of SDLC or HDLC. Some use carrier frequencies for high throughput. Some of the common ones are listed below with its typical transmission rates. Ethernet is now the defacto standard.

- Ethernet 10Mbs/100Mbs and 1000Mbs GigiBit
- Arcnet 2Mb=(Million bits transmitted per second
- Starlan 2-10Mb
- PC Baseband Lan 1Mb
- Token Ring Lan 10Mb (New 100Mb)

TCP/IP LAN Taps
The most popular method of connecting ATMs to the bank network is via Ethernet LAN via TCP/IP. Banks have high network security and use VPN routers which communicate via one port only to the ATM. Therefore tapping this connection is the simplest and monitor the printer information for display in the video or record to the DVR. Banks can also configure for mirror ports for a dedicated port for the ATM interface and the DVR sharing one port.