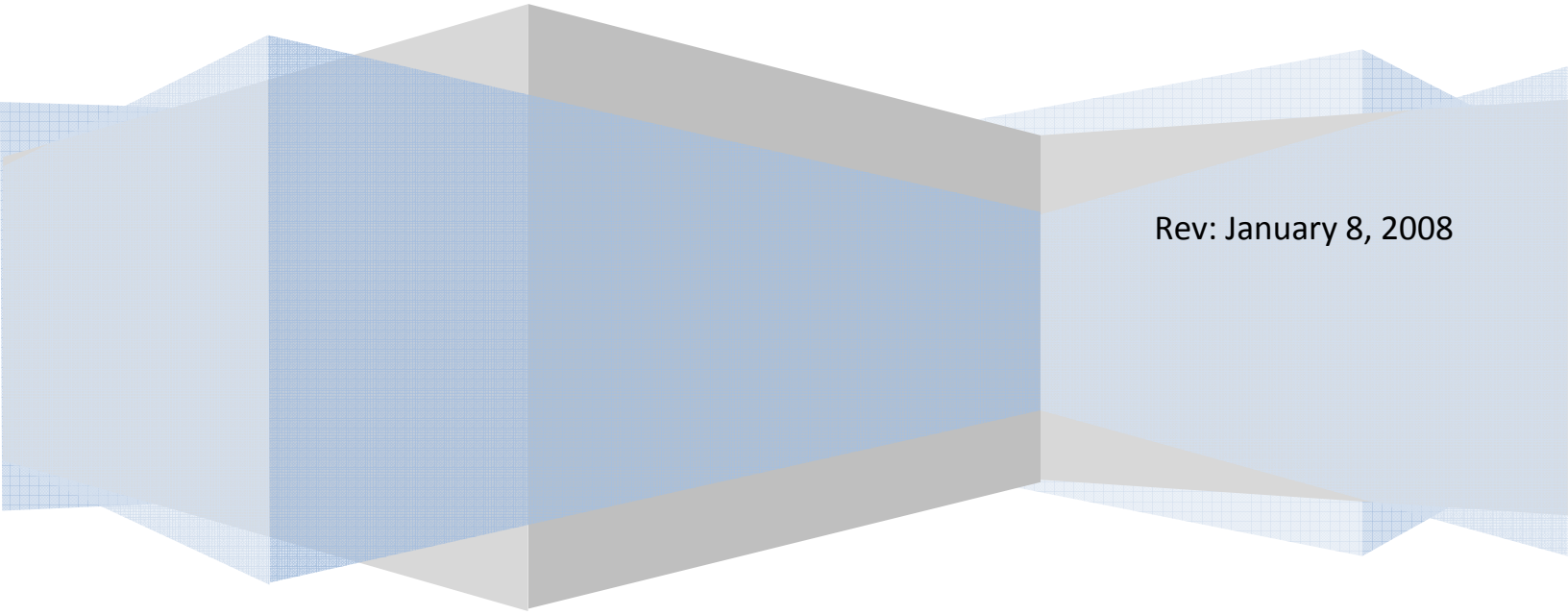
ISA
Information Security Associates, LLC.

Information Security Associates, LLC

ETA-3

Telephone Analyzer

OPERATOR'S MANUAL



Rev: January 8, 2008

Table of Contents

Section 1

Introduction

The ETA-3A is used in evaluating telephone instruments and cabling for the presence of a variety of eavesdropping attacks and devices.

Eavesdropping using a telephone can consist of:

1) the interception of telephone calls
2) the gathering of room conversation by bringing it out of the area on the telephone wiring.

Interception of telephone communications can be done in a variety of ways. Virtually all of the attacks that will be covered in this manual will be located within a business setting, generally between the telephone and the telephone switching equipment. Because of transmission techniques and types and methods of cable installations, the likelihood of an eavesdropping attack being installed between the office site and the telephone company central office is remote, except as described later in this manual.

The ETA-3A will detect many different types of attacks, but telephone testing is complex enough that a thorough understanding of telephone electronics may be required to detect the more subtle ones. There are certain sophisticated eavesdropping attacks that cannot be detected by any sort of test equipment. Telephone testing is often not a red light-green light sort of activity. Many of the tests are open to interpretation. When faced with uncertain or conflicting results, try to use a logical process to determine other types of tests that can be used to confirm the assumed results.

When testing business telephone systems please keep the following in mind:

Caution:

The ETA-3A has voltages that may be harmful to electronic telephones used in business telephone systems, as well as other telephone instruments incorporating solid-state electronics in the telephone instrument. The ETA-3A can be used to safely test these telephone systems and instruments. However, it is the responsibility of the user to know what type of instrument is being tested and to ensure that the ETA -3A is being used accordingly for that type of phone.

Introduction to Telephony

Users of the ETA-3A are likely to be required to test a variety of different types of telephones. In order to do the testing thoroughly, a bit of background on telephony is required.

Telephones can be broken down into two general categories: phones that are connected directly to a telephone company central office (usually a single line phone at a residence or in a type of business telephone service typically called Centrex) and telephones that are connected to a telephone system within a business. There are, of course, instances where single line phones are found connected to a business telephone systems and instances where a phone with more than one line is found in a residential installation.

These two categories of telephones are considered different as involves eavesdropping detection and the types of threats they face.

RESIDENTIAL OR SINGLE LINE PHONES

How a telephone works

A single line phone in a residential setting is connected to a pair of wires that reach from the telephone all the way to the telephone company central office, usually no more than a few miles away.

The telephone central office contains the switching equipment for the system and also contains the power to run the telephone. This power is called a Central Office (CO) battery. It is charged to between 48-52 volts. Since this is a battery, the voltage is direct current (DC). When the phone is taken off-hook, current flows from the one side of the battery, through one wire in the cable, through the telephone, and back to the CO battery through the other wire in the cable. How much current flows is dependent on several factors: gauge or thickness of the wire used in the telephone cable, the length of the cable, and the resistance of the telephone itself.

Telephone cabling is usually 22,24, or 26 gauge wire. The higher the number, the smaller the diameter and the smaller the diameter, the more resistance the wire has per foot. Telephone instruments vary in the actual amount of resistance they have. Speaking into the microphone also changes the resistance proportionally to the frequency and amplitude of the sound reaching the microphone.

When the phone is taken off hook, these resistances come into effect. They cause the CO battery's voltage measured at the telephone to drop to a range of approximately 6 to 10 volts.

Generally there is enough resistance between the wiring and the telephone to cause about 30 milliamps of current to flow when the telephone is taken off-hook .

No current flows when the phone is on-hook.

When a telephone rings, another voltage is applied. This is 70-90 V AC at approximately 20 Hertz; Hertz is the ring voltage in this situation.

When the phone is answered, or taken off hook, the CO can sense the flow of current in the line and connects the call to the cable going to the called telephone.

Speech on the line is carried as minute fluctuations in current flow that are created by the microphone (called a transmitter) in the phone. A small amount of this signal is fed back into the telephone's earpiece (called a receiver). This is called side-tone.

Telephone Wiring

The telephone wiring in a residence connects all of the phones together. Residential telephone wiring follows two types of configurations when there is more than one telephone. It can be a star or a loop.

Star wiring configuration is where a separate cable connects the protector block (where the telephone cable from the CO enters the residence) to each telephone outlet. This can be seen at the protector by the presence of as many cables as there are phone outlets.

A loop configuration is where one cable connects several outlets. This is identifiable at the protector by finding only one cable entering the premises.

Frequently, residential installations are a combination of both configurations, particularly if some remodeling has occurred.

Telephone cabling at the residence almost always contains four conductors. Sometimes cables with more wires are used, but this is infrequent. In North America, the standard wire colors are red, green, yellow, and black. The wires connected to the CO are the red and green. On a RJ-11 modular connector, these wires are located on the center two pins. The yellow and black wires will be the outer two pins.

Outside North America, this same configuration may be encountered, or there may be others. One frequently found is the British Telecom (BT) standard. The BT standard uses four wires, blue, white, red, and green. The blue and white wires are connected to the CO. They appear on one of the outer and one of the inner pins on the BT modular connector.

The telephone wiring in the residence joins the telephone company wiring at a point called the "demarcation point" or demarc. This point is located either inside or outside the residence, depending on the age of the installation. It is usually near where the electric power enters the residence. At this point will be found a device called a protector block on older installations and a network interface unit on newer installations.

The protector block protects the telephones and internal wiring from dangerous voltages caused by lightning strikes or high voltage electric cables falling on the phone cable in the street.

Cabling from the telephone company to the demarc point consists of one of the following types:

- Aerial drop wire. This cable is almost always a 2-conductor cable coming from a splice boot on the multi conductor cable on a telephone pole installation. If more than one line is brought to the residence, more than one drop wire will be installed. Occasionally, a multi conductor drop wire will be installed .
- Direct burial cable. This is usually a multi conductor cable. The number of conductors varies from one installation to the next depending on the size of the residence. It is usually large enough to accommodate future expansion needs.

The aerial drop wire joins the telephone cable in the street in a splice boot called a ready access enclosure.

A direct burial cable may be underground only to a nearby service pole or may be underground all the way back to the central office.' Underground installations are joined at "pedestals" nearby the residence. Pedestals are usually installed to provide service to several residences.

BUSINESS TELEPHONE SYSTEMS

Business Telephone Systems Fall Into Three Categories

The first is a PBX (Private Branch Exchange), which functions as a small central office (CO). A PBX has many lines coming to it and can handle, depending on the design, from a few dozen up to several tens of thousands of phones and up to several thousand lines. Modem PBXs use proprietary phones, phones that are designed to work only with that particular system. PBX phones can be multiline (or multi-button, as they are often called) or can be single line instruments, or fax machines, or modem lines. Usually, "9" has to be dialed to make an outgoing call. Most large businesses have PBXs.

The second type of business telephone system is called an electronic key system. An electronic key system is relatively small, usually 4-20 incoming lines and 8 to 200 instruments. Outside lines are accessed directly by pushing a button on the telephone instrument, rather than by dialing "9". Most key systems do not operate single line phones or fax machines or modems.

These are connected to lines that bypass the key system control unit and are not extension of the system.

Originally, the term "key system" referred to the multi-line standardized 1A2 systems made by AT&T among others. These systems use a 25-pair cable to connect the telephone to the system and use electromechanical switching systems. Every telephone line was hard-wired to every telephone. The ET A- 3A is not designed to test this type of system.

The third type of business system is known as Centrex. This is a business service offered by the local telephone company as a substitute to owning a PBX. Centrex phones are essentially phones that are not very much different from standard single line phones found in a residential setting, but they have lots of features and functions that can be accessed by certain dial codes, such as conference calling, call forward, intercom, etc .. Switching and other functions that would be provided by an on-site PBX are done by the local CO. Centrex phones can be single line instruments, multiline key sets like the old 2565 and 2830 types, or "digital" Centrex phones that use digital signaling for all of the features and functions, though have analog audio, or ISDN Centrex phones, where the phone is connected to the CO via a digital ISDN trunk.

Centrex phones are popular in businesses that occupy multiple locations within the same city and with government agencies. Occasionally, a small key system will work with Centrex phones to provide local features and functions not available from the telephone company.

Business Telephone Types

There are three types of telephones that are found in business telephone systems, whether they are PBXs or key systems. The phones are: single line phones, hybrid phones, digital phones.

The first group includes not only single line phones but fax machines and PC modem ports, too. All of these phones operate in a manner described in the residential and single line section.

The second group of phones is "Hybrid" phones. A hybrid phone can be defined as a multi-line electronic telephone that use digital information sent back and forth between the telephone and the switch for all commands and to access features and functions. Audio on a hybrid phone is transmitted in an analog form.

Digital phones are the third variety of phone found in business systems. A digital phone has no analog audio between the instrument and the switch. Audio coming into the switch from the telephone system is converted to a digital signal and transmitted up the wiring to the phone. The telephone user's speech is converted inside the phone into data for transmission to the switch. There are digital to analog converters in the phone and in the switch to convert the digitized speech back into analog signals.

One very important concept to remember is that a multiline electronic telephone, whether it is hybrid or digital, uses only one or two pairs of wires for all operations regardless of how many lines it appears to have. A multiline electronic phone with 20 lines uses the same number of wires as does one that has only two lines.

Operation

The following section provides an over view of the typical operations of business telephone systems. Most PBXs operate using similar concepts and most key systems operate using similar concepts as well. As to the actual operational details of such systems, there is virtually no uniformity. Every system manufacturer has engineered their system to have certain properties and features that are unique to their product line. This is particularly true with the protocol under which the data is transmitted between the telephone and the switch.

To understand the functioning of an electronic telephone system, the first concept that has to be grasped is that the telephones operate in a manner completely different from the single line phones described previously.

On a single line phone it is the current flowing through the wires that makes the phone work, allows it to place a call and alerts to the presence of an incoming call (through the application of the ring voltage).

Hybrid and digital phones should be thought of as more like data terminals than like phones.

On a hybrid or digital phone, there is continual communication between the instrument and the switch. On a hybrid instrument, there are at least four conductors in use. One pair is for audio and the other is for power and data. On a digital instrument, these functions are contained generally on only one pair of wires. The CPU in the switch interrogates or polls each telephone in the system requesting change of state information. When change of state information is sent, the switch acts on the information.

The polling speed is very quick. One small key system polls each telephone every 100 milliseconds. Some systems are much faster.

The flow of events on an electronic system goes like this:

Incoming Call:
An incoming call is detected by the switch.
At the next polling cycle, or query, an instruction is sent to the desired telephone instructing it do perform a number of activities. These include the illumination of an LED next to the appropriate line key push-button on the phone, the activation of the ringer circuit, and display of information on the phone's LCD display (if so equipped).

The user takes the phone off-hook and pushes the line key.

At the next query, the telephone informs the switch of its current status, that it is ready for the call.

The switch then connects the audio of the call to the instrument.

When the call is finished, the phone is placed back on hook. At the next query, the switch acknowledges that the instrument is idle.

Outgoing Call:
The user takes the phone off-hook and pushes a line key (if required).
At the next query, the switch acknowledges this condition and instructs the instrument to illuminate the appropriate LED by the line key and will transmit dial tone to the phone.

Receipt of dial tone at the phone will initiate the dialing sequence. The DTMF dial information is converted to data and sent to the switch. The switch processes the call based on a series of pre-programmed set of instructions that vary depending on what type of call is being placed.

All of the switching and communication functions are very complex and happen at remarkable speed, since they appear to be instantaneous.

The important concepts of business systems to keep in mind are:

- Nothing happens on an electronic telephone until instructed by the switch.
- Sounds heard in the hand set- DTMF, etc., are not (usually) communicated to the switch as DTMF.
- Since the telephone is in constant communication and, hence, electrically connected, there may not be much change in voltages. Current continually is flowing through the instrument. The voltages read at these phones can be considered to be the equivalent of off hook readings.

- Regardless of how many lines appear on a phone, there is only one audio pair on a hybrid phone and only one data path on a digital phone. All of the connections of various audio sources occur in the switch.
- Since the phones are essentially data terminals, and data communication cannot occur between more that two devices (the switch and the phone); additional phones cannot be connected as extensions to an electronic phone.
- Different phones that share the same extension numbers are not connected together. Connections are through the software instructions in the switch.

Section 2

TELEPHONE EAVESDROPPING ATTACKS

Telephones are subject to a wide range of eavesdropping attacks. Some attacks can be made to work on any type of phone; some attacks cannot work on electronic phones. Some attacks are very easy to detect; others are virtually impossible to detect.

When testing a telephone, it is important to keep in mind what the vulnerabilities are of the particular type of system being tested. It is important to also keep in mind the symptoms of the various devices.

Telephone testing is not an exact science and the ETA-3A is not a "red light-green light" tester. It provides results and it is up to the user to interpret its indications.

A description of eavesdropping attacks current with the publication date of this manual is described below.

Radio Transmitters:

There are two types of telephone radio transmitters: Series and Parallel.

Series Transmitters

Series transmitters use the current of the telephone line for their power source. They are installed by cutting one of the wires in the telephone pair and splicing in the transmitter. Some series transmitters are built into various types of modular adapters. Installation is a matter of simply plugging in the adapter.

Series transmitters can be installed anywhere- in the telephone, on the wiring in the business or residence, or on the telephone cable in the street.

Series transmitters typically transmit 300 feet to 1 mile.

Since series transmitters use telephone power, they have a noticeable affect on the telephone voltage. For a series transmitter to operate, current has to flow through the phone line; the phone has to be off-hook. When the phone is on-hook, no current flows. Any affect created by a series transmitter will only be noticeable in an off-hook condition.

A series transmitter will lower the off hook voltage between .5 and 2.5 volts if it is connected on the CO side of where the ETA-3A is connected. If the transmitter is connected on the telephone side of the ETA-3A, the off hook voltage will increase dramatically.

A series transmitter connected to an electronic telephone in a PBX or key system will transmit continuously.

Parallel Transmitters

Parallel transmitters are telephone RF transmitters that are generally not powered by the telephone line. They are powered by an external source, usually a battery. Identified by the term "parallel", they are connected to both wires in the telephone cable. In order to activate, some detect current flowing on the line; others are sound activated.
Parallel transmitters may or may not have a measurable electrical affect on a telephone line.

Tape Recorder Switches

Tape recorder switches are used to connect a telephone line to a tape recorder and to turn the recorder on and off when the phone is in use. There are several types.

One type is called a "drop-out relay" switch. This type uses an electromechanical relay to activate the recorder. The CO on-hook voltage holds the relay open. When the phone goes off-hook and the voltage drops to an off-hook level, there is not enough power to hold the relay open. It closes and the recorder starts. When the phone goes back on hook, the CO voltage opens the relay and the recorder stops.

Drop-out relays have a resistance of approximately 15,000 ohms. They will cause a drop of approximately 10-20% of the on-hook voltage.

Another type of tape recorder switch is a high impedance switch. High impedance switches detect current flow or sound on the line to turn on the recorder. They typically have a resistance of upwards of 2 million ohms. These switches are very difficult to detect.

When trying to detect tape recorder switches, keep in mind that:

- The tape recorder switch is not terribly small, usually about 4-5 cubic inches.
- The tape recorder will likely be within a few feet of the phone line
- Small tape recorders have a very finite amount of recording time, usually no more than a couple of hours.
- Tape recorders that have a longer recording capability are fairly large: approximately 5" by 7" by 1 'is''
- Tapes must be retrieved relatively frequently; batteries must be changed, too.

Inductive Pickups

The theory behind the inductive pickup is that when the phone is off hook and current flows, there is a magnetic field created around each wire of the telephone pair. The magnetic field varies with respect to the minute changes in electrical current that occur when a conversation is carried on the phone line. The telephone wire pair is a twisted pair and when both wires of the pair are taken together, the field cancels out and does not effectively radiate. This means that the attacker must put a pickup coil around one wire of the pair. This will usually unbalance the pair and 60 cycle ac hum may be noted on the telephone line.

At best, the radiating magnetic field around a telephone pair, whether carrying voice or data, is only at a useful strength for a radius of approximately two inches from the wire. If a pair is within a large cable, no useful magnetic field can be found outside the cable. In addition, the cable will be carrying other conversations and their associated magnetic fields, so separating the target pair is critical to the performance of the tap.

Inductive pickups have been used but have enough drawbacks that they have all but vanished from use. It just does not make sense to use an inductive tap when it would be just as easy to connect directly (hardwire) to the telephone line.

Slaves

Slaves are intercept devices used by law enforcement agencies. The purpose of a slave is to bridge a call on the target line to a line connected to a listening post. They can be turned on either by remote command or when a telephone call is made on the target lines. The manufacture of these types of devices is not a simple task and their purchase is controlled by Federal Statutes. These devices cannot be located by testing of the telephone pair either with countermeasures test equipment or by Central Office tests because they are very high impedance. Their installation requires a court order and assistance from the local telephone company.

Slave-like devices are available in kit form. Kit type slaves also connect the target line to a line going to a listening post. However, they require the installation of an additional phone line to do so. They have auto-dialing circuitry that can call the number of the listening post where the conversation will be monitored.

The likelihood of a kit-type slave being used depends on the ease with which another phone line can be installed at the target premises. KIT type slaves tested to date appear to be powered by the target telephone's line and lowers its on hook voltage.

Tone Activated Devices

Tone activated devices, traditionally called infinity transmitters and harmonica bugs, are devices that enable an eavesdropper to remotely turn on a microphone to gather room audio and bring it out of the area to the listening post on a telephone line. These devices are usually installed on the telephone wiring within or nearby the target office.

The infinity transmitter is activated by a tone of a particular audio frequency that is transmitted on the phone line from the listening post by the eavesdropper. The tone will be somewhere between 300 Hz and 3500 Hz. These frequencies comprise the audio bandwidth of the telephone system. Frequencies higher or lower than these are not passed through the telephone system.

It should be noted that the traditional infinity transmitter as described here is no longer a threat because of the operation of the electronic central offices in North America. Understanding of the operational concepts is important however, because there are still situations and locations where it can be utilized.

To operate an infinity transmitter, the attacker places a telephone call to the target telephone. As the last digit is dialed, a tone is induced onto the line, probably from a tone generator neat the listening post's (LP) phone's transmitter. The tone is connected to the target telephone through a "sneak" path in the central office equipment. The central office also connects the ring generator to the line, but by this time, the tone has already reached the infinity transmitter. When the infinity transmitter detects the activation tone, it captures the telephone line and "answers" the telephone call. This signals the central office that the telephone being called has apparently answered and the ring voltage is disconnected. The telephone does not ring. All other callers attempting to reach the target telephone will get a busy signal.

Now the attacker is listening to the room conversation. When the attacker wishes to terminate the listening, the phone at the listening post is hung up and the telephone company terminates the call to the target phone in about 20 seconds through its supervisory process.

In today's CO’s that use electronic switching (AT&T's #5ESS & Northern Telecom's DMS-100 for example) there is no "sneak" audio path. The audio path is not completed through the CO until the called phone is off hook. This means that the phone has to ring and the eavesdropper cannot covertly activate the infinity transmitter.

This means in most instances, the infinity transmitter will not be a viable eavesdropping device. It is, however, still a threat.

In the business telephone environment, the infinity transmitter is still a concern because of "auto-answer" devices like fax machines and modem lines. It is common to have a fax machine in an office (or nearby) that could be used as a path for eavesdropping. Fax numbers are frequently misdialed, so no one pays attention when the fax machine rings and no fax appears. A fax line gives the eavesdropper a ready-to-use dial-up line for the infinity transmitter. The transmitter activation tone is sent after the fax machine answers the line.

There is another tone activated device that absorbs the first cycle of Jing voltage sent by the telco CO. This device is "armed by this first cycle of ring voltage. If the phone is allowed by the eavesdropper to ring only one time and called again within a short period of time, it will turn on microphones when it detects certain DTMF tones.

These devices are usually powered by the phone line voltage. They can be detached also by calling the target phone, letting it ring one time, and re-calling it.

Hook-switch Bypasses

The function of the hook-switch on a single line phone is to disconnect the audio of the telephone from the outside world and also prevent current from flowing while the telephone is not being used. A diode circuit called a "keep-alive diode" can be connected across the hook-switch. In this type of attack, a phone call is made to the target telephone. After the call is completed, the attacker simply lets the called party hang up first. The keep-alive diode then shorts out the hook-switch keeping the phone active and the attacker is now listening to the room conversation.

When the attacker no longer wants to listen, he hangs up and the Central Office supervisory sequence disconnects the keep-alive diode. Other attacks involving the hook-switch include putting a resistor and capacitor, an SCR (Silicon Controlled Rectifier) or other conducting device across the hook-switch. Rewiring of the instrument is also possible to bring the audio from the pickup devices (either the mouthpiece or the earpiece may be used as a microphone) around the hook-switch to the outside lines and to the listening post.

Hot-wiring

All telephones contain wires and microphones. Audio from telephone conversations and room audio can be connected to spare wires in the telephone cable within a facility. This audio can be brought out of the target office to a listening post where it could be recorded, transmitted out of the facility via a radio transmitter or listened to live.

Virtually all telephones have spare wires in the cable. Frequently these spare wires go all the way back to the telephone equipment. This means that a thorough investigation of the wiring must be made to be certain to detect or locate all of the worrisome devices.

In some installations, the spare wires terminate at the wiring distribution frame that serves the floor or the area. In this instance, cross connects and other attacks will be relatively obvious.

This is an attack that can be used on virtually all digital telephones.

An electronic telephone usually has several components that can be used as microphones. These include the microphone in the handset, the microphone in the speaker phone, and the ringer transducer. Modem telephones do not have ringers as we have known them in the past. Modem telephones use a small dynamic loudspeaker or a small piezo transducer that acts like a speaker. Frequently, these components can be used as microphones.

Electronic System Threat Overview

Electronic systems operate for the most part in a manner entirely different from electromechanical systems. It follows that the threats are somewhat different, too.

In an electronic system, there are hybrid phones with analog audio on the wires between the instrument and the switch. There are digital instruments that convert all sound to data and there is no analog audio on the wiring.

On most systems the instrument is "on-line" all the time, that is, it is communicating with the PBX continuously. Current is flowing continuously. Hence, there is usually little, if any difference between on-hook and off-hook voltages. Any differences are caused by additional circuitry becoming active when the phone is off-hook and causing a change in the total electrical resistance of the loop.

There is little, if any, standardization within the digital telephone world. Virtually all makers of electronic systems consider their data communication protocols to be proprietary products. Since there is very little information available about the transmission details of digital phones, it is technically very· difficult to create tap that can intercept digitized conversation on these phones.

Therefore, digital phones are fairly secure, at least compared to single line phones. They are not totally secure, however. Audio can be intercepted in the instrument prior to digitization. Then it can be connected to spare wires or broadcast via an RF transmitter built into the phone.

Some electronic telephones pass audio by themselves. In a single line phone, the hook-switch isolates the microphone from the line when the phone is on hook. In an electronic phone the

hook switch's function is to cause a signal that informs the PBX of the phone's status. It does not necessarily disconnect the microphone or other audio source. Some hybrid phones have been found where the microphone is live all of the time, regardless of the status of the telephone and there is always phone or room audio on the wiring.

Large PBX systems are controlled by a computer. All switching is done within the PBX by software command rather than by mechanical switching. Thus, it is possible to initiate eavesdropping attacks from within the system via the computer. The features that allow this vary from system to system, so they can not be specifically defined in this manual, but a review is in order. Threats can include:

- Bridged extensions. A software bridged extension does not involve a physical connection to the target extension as on an electromechanical system. It simply is an instruction to the system to connect any call to a specific extension to another one. This other one can be anywhere within the system, where the eavesdropper can monitor it.

- Bridge to voicemail. This connects a call in process to a voicemail box where, in a large system, it can be recorded and retrieved later.

- Executive override or Barge-in. This allows another phone to interrupt a call in process on another extension. In some systems, this feature activates the speaker phone and its microphone. The listener can hear telephone conversation and room audio.

These features, or class of service, as they are often called, are controlled by the telephone system administrator and anyone else who has access to the system via the administrator's terminals. On many systems, any activity at the administrator's terminal can be made from off-site by means of a modem installed in the PBX for maintenance purposes.

It is always prudent to make an evaluation of the system for these sorts of features in addition to the electronic testing done with the ETA-3A.

Section 3

TESTING WITH THE ETA-3A

The following tables provide a quick overview of the required tests on electromechanical and electronic telephone systems and instruments.

Required Tests:

Electromechanical Systems-Multiline & Single Line

Test	Vulnerability	Symptom
On Hook Voltage	Parallel line devices: Tape Recorder	Lowers voltage at least 4 volts. Dial-up listening devices and infinity transmitters may drop 8-12 volts
Off Hook Voltage	Series Line Devices: line powered radio transmitters	Lowers voltage at least 0. V. If installed in phone, voltage will be signifacnatly (50%) higher.
Phantom Load	Series Line Devices	Will seethe off hook voltage on that phone decrease.
Tone Sweep	Infinity Transmitter & Tone activated devices	Voltage will drop to off hook levels when activated. Will hear dial tone and room audio in headset. Alarm will sound on ETA.
High Voltage	Hookswitch bypass: keep alive diodes, high Voltage activated devices, SCRs	Current path around hookswitch causes HV to drop dramatically. Wil be less than 600 V on ETA.
All Wire Listen	Rewiring to connect mic or other audio source to spare pair. Installing additional mic on unused wires	Will hear room audio on two or more wires with phone on hook.

Required Tests:

Electronic Systems- Digital, Hybrid, Single Line Instruments

Test	Vulnerability	Symptom
On Hook Voltage	Parallel line Devices, esp on single line phones. Devices powered by phone system voltage.	Lowers voltage on audio pair. Phone powered devices may lower voltage on other pairs
Off Hook Voltage	Series line devies-transmitters, etc.	Lower voltage on audio pair. Voltage may be higher if device is installed in phone.
Phantom Load	Series line Devices in Single Line Phones only.	Different voltage on one phone from the others
Tone Sweep	Tone activateddevices on fax lines	Will hear dial tone & room audio. Voltage will drop to off hook
High Voltage	NOT DONE ON ELECTRONIC PHONES	
All Wire Listen	Rewiring to connect mi or other audio source to spare pair	Will hear room audio on two or more wires with phone on hook. Phone passes audio on hook.

Test Operations

The testing of telephones and lines using the ETA-3A is separated into two sections, On-line and Off-line.

The **On-line** tests are: on-hook voltage, off hook voltage, current, and tone sweep. These on-line tests are accomplished using the two 8-position rotary switches in the upper right corner of the ETA-3A.

The **Off-line** tests are: high voltage and all-wire listen. The Off-line tests are accomplished using the eight 3-position toggle switches in the lower right comer of the ETA-3A. Note that a toggle switch marked ON LINE/OFF LINE controls which section is active.

When the ON LINE/OFF LINE toggle switch and the function switch are in the in the right positions, a red LED will be lit next to the proper set of switches for the test to be done.

Set Up-

1. Check the battery. Turn on the on-off power switch. There are two batteries in the ET A-3A: a meter battery and a main battery. The meter battery indicator (BATT) will be lit if its battery needs charging. The main battery level may be checked by placing the Function Switch in the SA

IT position. A reading below 7.5 volts indicates that this battery needs recharging. Refer to the Section 6 for battery charging instructions.

2. Plug in the headset. Be sure to adjust the volume to a LOW LEVEL to protect your hearing.

3. Switch the HV (High Voltage) toggle switch to the off (down) position.

TESTING ELECTROMECHANICAL PHONES

Connecting the ET A-3A:

1. Disconnect the modular line cord from the telephone and connect it to the Line jack (J2) on the ETA-3A. Connect one of the 6-wire line cables supplied with the ETA-3A to the telephone and also the Phone jack (11) on the ETA-3A.

   Make note of how many wires are in the cable that was connected to the phone. It will have 2, 4, or 6 wires. The settings for the 8 position rotary switches and the Off-line toggle for different cables is as follows:

   - 2 wires, check only wires 4 & 5
   - 4 wires, check wires 3, 4, 5, & 6
   - 6 wires, check wires 2, 3, 4, 5, 6 & 7
   - 8 wires, check wire 1 through 8
2. If the phone is hardwired or the connector is not compatible with those supplied with the ETA-3A, the alligator clip cable can be used.

   To use the alligator clips, plug the alligator-clipped 8-wire connector into the line jack (J2). Open the telephone jack on the wall and connect an alligator clip to each of the wires in the wall box. Match the colors of the wires in the telephone cable with the colors in the ETA-3A's cable, if possible. Note that single line telephones will not require all of the clips since they do not have 8 wires. Proceed with the telephone testing.

On-Hook Voltage Tests

I. Place the Function Switch in the Voltage M position.

II. Put the On line/Off line switch in the ON LINE position.

III. Put one of the 8-position rotary switches in position 4 and the other in position 5. This connects the ETA-3A's voltmeter to the red & green wires in the cable. These wires are the phone pair on all telephones in North America. The meter should show 48-52 volts. If you are testing a 2 line phone connected to residential type service, one line will be found with the switches in positions 4 & 5; the other line is found on positions 3 & 6.

IV. The reading obtained here is the ON HOOK voltage.

V. Record this voltage on the appropriate telephone test chart copied from the end of this manual.

Analysis:

On hook voltages can be lowered by eavesdropping devices installed in parallel across the phone line. Always compare several lines to be able to recognize differences. Differences of 10% or more indicate that there might be a problem.

Causes of problems:

Does the phone under test have a different prefix in its telephone number than the other phones? If yes, the phone may be powered by a different CO battery that is charged to a lower voltage. (At least 48 volts)

Is the voltage unstable or pulsing? Does the phone have a "message waiting" lamp that is illuminated? These are powered by a different voltage being applied to the phone wires. The ETA-3A is reading this.

Does the voltage start out at 48-52 volts and drop quickly to between 23 & 33 volts? If so, the telephone service is entering through a "Network Interface Unit" installed by the local telephone co. The NIU has a circuit to enable the telco to disconnect their cable from the house wiring for maintenance and test purposes. Measure the off-hook voltage on the CO side of the NIU.

Is the on-hook voltage higher than 52 volts? If 70 volts is present, the line under test is an off premises extension being driven by a remote CO.

Off-Hook Voltage Tests

Some telephones use carbon microphones. Some telephones use electret or dynamic microphones. If a telephone with a carbon microphone is being tested, the microphone must be removed to obtain accurate results. The carbon microphone will vary the off-hook voltage

enough to make readings inaccurate and deceptive. This is due to the continual change in the electrical resistance of the carbon element as a result of sound pressure in the area and orientation of the handset.

Carbon microphones usually can be removed by unscrewing the mouthpiece or by disconnecting the handset cable from the phone.

Electret and dynamic microphones have no such varying affect on the off hook voltage.

To Test:

1. Leave all switches as set for on-hook voltage readings.
2. Take the phone off hook.
3. Note the reading on the ETA-3A's meter. 0
4. Turn the handset over and note any changes in the reading. If there is a change, the phone has a carbon microphone. Remove it and be sure to re-install it when the test is complete.
5. Record the off-hook voltage.

Phantom Load Tests:

When testing single line or two line phones, particularly in a setting where there are a number of phones connected as extensions to the same phone line, it is not unlikely to have different off hook voltage readings on different phones. This is caused by slightly different circuitry in the various instruments drawing different amounts of current.

The Phantom Load switch connects a standard load across the wires selected by the rotary switches. Its purpose is to eliminate the variations in voltage readings on the same line caused by the different instruments. By putting the same resistance at each phone, if there is no device installed on the wiring to a specific extension, all voltages will be the same.

The Phantom Load test does not replace the off hook voltage test. It will not provide any indication of a device installed inside the telephone.

To Test:

1. Leave all switches as set for on-hook voltage readings.
2. Push the Phantom Load push-button switch.

3. Record this voltage.

Off-Hook Voltage Analysis

Changes in off hook voltage are caused by series devices. These devices increase the total resistance of the telephone loop. Their affect is seen only when current is flowing through the line. Most do not add a tremendous amount of resistance- a few hundred ohms at the most. This will be enough to lower the off hook reading by 0.5-3 volts.

If the series device is in the telephone, or on the telephone side of the ET A-3A, the off hook voltage will be much higher- two to three times what would be expected.

When testing extensions with the phantom load, the voltages should all be the same if there is no problem.

Measuring Current

Current and voltage are inter-related. Something that affects voltage will affect current, too. Current tests can confirm voltage test results. Some technicians prefer to measure current rather than voltage.

To Test

1. Place the Function Test Switch in the Current (I) position.
2. Place the Current Range toggle switch in the 2a position.
3. Place the On Line/Offline toggle switches in the on-line position.
4. Place both 8 position rotary switches to the wire number to be tested.
5. The meter will now read the current flowing in the selected wire. Both switches must be on the same number. The meter reads 2 amperes full scale. If the reading is less than .2, change the panel switch marked CURRENT RANGE. This allows the meter to read up to 200 milliamperes full scale.
6. If the single line phone is on hook no current will be flowing. If you have the rotary switches on one of the "talk pair" wires, take the handset off-hook and note the current. For a typical single line telephone, the current will be approximately 30-40 ma.
7. If there is a carbon microphone in the handset, notice the current changes that occur when the orientation of the handset is changed. This is due to the carbon granules in the carbon microphone packing and unpacking together, causing a change in the resistance which affects the current on the line.

Analysis:

Differences in current in excess of 5 milliamps are indications of a problem.

Be aware that devices drawing current installed on the CO side of the test site will not be detected with the phone on hook, since no current is flowing through the phone.

Tone Sweep Test

1. Place the Function switch in the Tone position.
2. Place the Unitone-Multitone switch in the Unitone position.
3. Place the 8-position rotary switches in the positions for the line pair (wires 4&5).
4. Depress the START switch in the set labeled TONE SWEEP. The tone will be heard in the headset. It starts at about 4000 Hz and descends to about 400 Hz. It stops automatically.
5. If a telephone call comes in, or if someone picks up an extension phone, or if an infinity transmitter is activated, the ETA-3A will automatically disconnect the tone and an alarm will sound. The voltage displayed on the meter will be lower, indicating an off-hook condition when the phone is picked up or an infinity transmitter is activated. Since the audio amplifier inside the ETA-3A is also connected, you will be monitoring the line and can easily tell if the line has a normal conversation or if you are hearing a room-listening device.

Once you have confirmed that the conversation is legitimate, place the Function switch in the Voltage position or change the rotary switches to different wires. Continued listening may be misunderstood as eavesdropping.

6. Place the Unitone-Multitone switch in the Multitone position and repeat step 4.

<u>Analysis</u>

Keeping track of the telephone numbers (lines) which have been swept can reduce the amount of time that it takes to perform checks on other telephones in the installation. When a telephone line is being swept, all extensions connected to that line are also being swept. If the infinity transmitter is on an extension of the instrument that is being swept, it will be activated and the alarm will sound. To find the phone with the device on it, make a sound in each room while listening to the ET A-3A.

High Voltage Pulse Test

NOTE: DO NOT HIGH VOLTAGE PULSE ELECTRONIC TELEPHONES.

The high voltage pulse tests the hook switch for any devices that are connected across it to either listen to the room conversation or hold the phone open after it has been hung up from a call.

On some telephones, the HV pulse is discharged across the ringer, rather than the hook switch. If the telephone has a mechanical ringer (one with a bell) and it activates, it may be necessary to disconnect one wire going to the ringer.

To Test:

1. Disconnect the cable from the ET A-3A to the telephone system. Leave only the telephone instrument connected to the ETA-3A. Leave the phone on hook.
2. Place the Function switch in the HV position.
3. Place the On Line/Offline switch in the Offline position.
4. Place the HV toggle switch in the ON position.
5. Adjust the HV ADJ knob so approximately 1200 volts is shown on the meter.
6. Place the polarity toggle switch (next to the HV ADJ knob) in the + position.
7. The Off Line toggle switches are used for this test. All 8 switches are in the center position. The test is made using switches 4&5.
8. Move switch 4 to the right and switch 5 to the left. This connects the high voltage supply to the telephone.
9. Note any changes in the reading on the meter.
10. Reverse the polarity toggle switch and repeat the test.
11. If the meter changes during the tests, check to see if you have made an error:
    - I. One wire of the ringer may need to be disconnected
    - II. The telephone line must be disconnected.
    - III. The telephone hand set must be on-hook.

Analysis:

A quick change in the meter reading indicates a current flow in the wiring being tested. This charge will be more than 20 volts and usually several hundred volts.

NOTE: Some telephones with electronic ringers and telephone equipment with auto-answer capability (fax machines, for example) will not pass a high voltage test under any conditions.

Do not do a high voltage test on any telephone that does not have an FCC Ringer Equivalence Number.

ALL WIRE LISTEN-Electromechanical Phones

The ALL WIRE LISTEN test checks all of the combinations of the wires leaving the telephone to see if there is any audio present when the phone is on hook. The ETA-3A supplies DC voltage to operate carbon and electret microphones. Carbon microphones are not polarity sensitive. Electret mics are, so the AWL test has to be done twice to provide the proper voltage to any hidden electret mic.

Set-up:

1. Make sure the headset is plugged in.
2. Place the function switch in the AWL position.
3. Place the On Line/Offline switch in the off-line position.
4. Take the telephone off-hook to self-check the AWL set-up.
5. The Off Line toggle switches are used for this test. All 8 switches are in the center position. The self check will be made using switches 4&5.
6. Move switch 4 to the right and switch 5 to the left. This connects these wires to the ETA-3A's audio amplifier.
7. Keeping the switches pushed as in Step 6, adjust the headset volume so the room audio is clearly heard. If desired, use the sound source supplied with the ETA-3A. Turn it on and place it near the phone.
8. Put the handset back on hook.

To Test:

9. Hold switch #1 in the right position. In turn, hold each of the other switches in the left position and listen for audio. This compares wire 1 with all seven other wires to check for audio. If no audio is heard, release switch # 1.
10. Now push Switch 2 to the left and push in turn switches 3-8 to the right. Release switch 2.
11. Now push switch 3 to the left and push in turn switches 3-8 to the right. Release switch 3.
12. Repeat for all other switches, one at a time.

13. Now return to switch 1. Push it to the right and push switches 2-8 in turn to the left.
14. Repeat for all other switches one at a time. This step reverses the voltage supplied to the phone.

TESTING ELECTRONIC TELEPHONES

Some electronic telephones are sensitive to being disconnected. Keep in mind that electronic telephones are essentially data terminals. When they are disconnected, there is no communication with the PBX. Some PBXs interpret this as a failure of the telephone and disable the communication or turn off the port if the phone is disconnected for any period of time. Some systems restart immediately when the phone is reconnected; some take up to 20 minutes and some require a command from the administrator's terminal to restart.

Connection of the telephone analyzer should be made rapidly.

Cable Concepts

Electronic telephones may use a 2-,4-,6-, or 8-wire cable. The 2-,4-,and 6-wire cables use the same modular connector type, an RJ-ll. The 8-wire cables use a different connector, an RJ-45. As of the publication date of this manual, only AT&T/ Lucent Technologies telephone systems use the RJ-45.

Some electronic telephone systems may be susceptible to "Modular Cord Reversal". This is a term to describe the fact that some modular cords reverse the sequence of the wires on one connector and some do not.

Cord reversal is not a problem on many systems; it is on some, though. If the wrong type of cord is selected from those supplied with the ETA-3A, the telephone will not work when connected through the analyzer. Indications of a non-working phone are no dial tone or side tone, no display on the LCD screen if the phone has one, and no LEDs illuminated by the function keys.

The ET A-3A is supplied with "reversing" and "non-reversing" cables in 6-wire and 8-wire configurations.

When testing a system for the first time, it will not be known which type of cable will be required. Have "reversing" and "non-reversing" cables ready. The "non-reversing" cables can be identified by the BLACK band around each end.

Make the hook-up with the "reversing" cable first and see if the phone works. If it does, you are set. If it does not work, swap the cables. Be quick. Do not leave the telephone disconnected for more than 20-30 seconds.

Once the type of cable has been determined, it will be the same on all instruments within the system.

Connecting the ET A-3A:

1. Disconnect the modular line cord from the telephone and connect it to the Line jack (J2) on the ETA-3A Connect the appropriate cable supplied with the ETA-3A to the telephone and also the Phone jack (11) on the ETA-3A.

2. If there is no connector on the phone or the connector is not compatible with those supplied with the ET A-3A, the alligator clip cable must be used.

   To use the alligator clips, plug the alligator-clipped 8-wire connector into the Line jack (12). Open the telephone jack on the wall and connect an alligator clip to each of the wires in the wall box. Match the colors of the wires in the telephone cable with the colors in the ETA-3A's cable, if possible.

3. Plug in the headset and adjust the volume to a LOW LEVEL.

Determining Phone Type

The first step in testing electronic systems is to determine if the phone is hybrid or digital. This defines the vulnerabilities.

<u>Digital or Hybrid Phone?</u>

To determine the type of phone, check for the presence of analog audio when the phone is off hook. To do so:

I. Connect the telephone as described.

II. Set the function switch to Voltage (V).

III. Set the 8 position rotary switches to positions 4&5. These wires are the audio pair on most hybrid phones.

IV. Take the phone off hook and listen for audio, dial-tone, etc.

V. If audio is heard, the phone is a hybrid. If no audio is heard, check position 3&4. This is the audio pair on a few systems.

VI. If only a hiss, white noise, or static is heard on either setting, the phone is digital. What was heard was the sound of the data.

Voltage Tests

There is debate as to the meaning of voltage tests on electronic systems. Some electronic systems have a wide variation of voltages from one phone to another, sometimes as much as 3-4 volts. Most systems have a fairly steady voltage, however. If a steady system is being tested voltage measurements are meaningful because they will indicate the presence of any device inside the phone or on the line that is powered by phone voltage.

<u>To test:</u>

1. Make note of how many wires there are in the cable connecting the phone to the system. If it has:

    - 2 wires, check only wires 4 & 5
    - 4 wires, check wires 3, 4, 5, & 6
    - 6 wires, check wires 2, 3, 4, 5, 6 & 7
    - 8 wires, check wires 1 through 8

2. Connect the ETA-3A as described above.

3. Refer to the chart at the end of the instruction manual labeled ELECTRONIC TELEPHONE VOLTAGE READINGS. Do not use the original, but make several copies for future use. The chart is for recording of voltages on all combinations the telephone wiring.

4. Place top rotary switch in the first position as defined by the type of cable used by the phone in Step 1. Put the bottom switch in the next higher position. Record the voltage.

5. Leave the top switch in place and rotate bottom switch from its position through the last position, recording the voltages for each position. NOTE: There may be residual small voltages in some positions that will rapidly decrease to zero. Disregard these.

6. The blacked out portions of the chart indicate duplicates of other settings that need not be recorded.

7. Move the top switch to the next position and rotate the bottom switch through the remaining. Record any voltages.

8. Continue this until the top switch has been in all positions.

All Wire Listen- Unpowered

The unpowered all wire listen test will detect audio coming out of the telephone. The test is made on line through the Voltage testing section of the ETA-3A rather than by using the AWL section. The A WL section applies a low voltage DC source to the selected wires. This could harm electronic telephones. Do not use the A WL section to test electronic instruments unless you are certain of the wiring and are experienced with the phone system being tested.

To Test:

1. Set the Function Switch to the Voltage position, not the AWL position.
2. If the phone is a hybrid, set the rotary switches to the audio pair (usually 4 & 5). Take the phone off hook and adjust the Volume so audio is clearly heard. Use the sound source supplied with the ET A-3A if desired.
3. If the phone is digital, turn the volume up so the sound of the data Gall be heard.
4. Put the phone back on hook.
5. Follow the switching procedure described in Voltage Tests. Listen for audio as the switches are rotated.

Tone Sweep *and* High Voltage Pulse Tests *are not done on electronic telephones.*

Section 5

Additional ETA-3A Information

Data Out Connector

The BNC connector on the upper left comer of the ETA-3A can be used to connect other test equipment. DC voltage is blocked.

- A spectrum analyzer or low frequency radio receiver can be connected to detect very low frequency RF signals in the range of 5 kHz to 200 kHz on the telephone line.
- An oscilloscope can be connected to investigate the digital signals on electronic telephone systems.

The wires under test are selected by the two 8-position rotary switches. The function switch may be in any position.

Binding Posts

A set of three binding posts allows insertion of test devices in the telephone circuit. The rotary switches determine the wire or wires affected.

Series Connection

1. Set both 8 position rotary switches to the desired wire.
2. Loosen the black (TIP) and red (ETA-3) binding posts and slide back the shorting bar so it no longer connects the two jacks.
3. Connecting a device between the black and red posts places the device in series in the wire selected in Step 1.

Parallel connection across 2 wires:

1. Set the 8 position rotary switches to the 2 wires to be tested.
2. Connect the test device between the yellow (ETA-3) and the red (ETA-3) posts.

MAINTENANCE

Internal Rechargeable Battery

Power for the ETA-3A comes from internal batteries that are recharged by using the battery charger supplied with the ETA-3A. The charger has a 110/220 volt switch in the event that only 220 volt power is available.

There are two batteries in the ET A-3A: one powers the meter and one powers the electronic circuitry.

The meter has a built-in low battery indicator. When the battery voltage drops to 7.5 volts, the letters BATT are shown on the meter, indicating that the battery needs charging.

The level of battery that powers the electronic circuitry is tested by placing the Function switch in the BATT position. When the voltage drops to 7.5 volts, the battery must be recharged.

Charging the Battery

Plug the charger's cord into the BATTERY CHARGE jack on the ET A-3A. Connect the charger to a wall outlet. The battery will automatically charge to a full charge status. Overcharging will not damage the battery. Do not charge the battery for longer than 18 hours.

NOTE: The charger will not operate if the ETA-3A is left on. The ETA-3A must be turned off to charge the battery.

220 Volt Operation

When using the ET A-3A outside of North America, primary AC voltage is likely to be 220 V AC. The charger for the ETA-3A operates on either 110-12060 Hz or 220-240 V AC 50 Hz. The primary voltage must be selected by the user.

The primary voltage is selected by a rotary switch located next to the prongs that fit into the AC outlet.

To change the setting, note the small triangle molded into the rotary switch. This points to the primary voltage that the charger is set for. To set for a different voltage, use a flat blade screwdriver and turn the switch so the triangle points to the other voltage.

Be certain of the local AC voltage before plugging in the charger. Operating the charger on 220 volts while it is set to 110 volts will ruin the charger and damage the ETA-3A. If you are unsure of the local AC voltage, check with a voltmeter or find an electric appliance or light bulb and look at its voltage rating.

ETA-3A ACCESSORIES

AMOUNT	STOCK #	DESCRIPTION
2	41010	6 Wire Modular Cable - Reversing
1	41104	6 Wire modular Cable- Non-reversing (black stripe)
1	6500	9 volt Battery (NiCad)
1	23808	Screwdriver
1	41002	Tone Generator
1	41004	Headset
1	41014	8 Wire Modular Clip Leads Cable
1	41075	Accessory Pouch
1	41087	Instruction Manual
1	41089	Battery Charger
1	41095	In-line Adapter
1	41102	8 Wire Modular Cable - Non-reversing (black stripe)
1	41013	8 Wire Modular Cable - Reversing
1	41128	8 Wire In-line Connector

Warranty

Information Security Associates, LLC, warrants to the original user that its products are free from defect in workmanship and material for a period of one year from the date of purchase. Information Security Associates, LLC, under this warranty, is limited to correcting or replacing without charge, at its factory, any part or parts thereof which shall be returned to its factory, transportation prepaid, and upon examination by Information Security Associates, LLC, shall be found to have been originally defective.

INFORMATION SECURITY ASSOCIATES, LLC, SHALL NOT BE LIABLE FOR LOSS OR DAMAGE CAUSED EITHER DIRECTL Y OR INDIRECTLY BY USE OF ITS PRODUCTS. THIS WARRANTY SUPERSEDES AND IS IN LIEU OF ALL OTHERS EXPRESSED OR IMPLIED. NO OTHER LIABILITIES MAY BE ASSUMED UNLESS AUTHORIZED IN WRITING BY INFORMATION SECURITY ASSOCIATES, LLC.

For service, technical questions and problems contact:

Information Security Associates, LLC.
6 Spruce Brook Road
Seymour, CT 06483
USA
Tel: 203 736-9587
Fax: 203 736-9639
www.isa-technology.com
isa-hre@comcast.net