-=-

RULES FOR INSURING PRIVACY IN AN ORGANIZATION.
CONSTANT AWARENESS OF THREATS.

-=-

Written by: -Q-

-=-=-=-=-=-=-=-

The following is a brief abstract on the topic of privacy and the awareness
of threats and vulnerabilities. I shall in this text discuss some of the
common rules that security experts and countermeasures technicians live by.

I have found that the best set of rules published to date is by
Glen H. Whidden which he draws upon from his 28 year career with the CIA.
Mr. Whidden, noted as one of the countries most knowledgeable surveillance
countermeasures experts details these rules in the books which his company
Technical Services Agency (TSA) publishes.

I shall simply reprint these rules from his book "A GUIDEBOOK FOR THE BEGINNING SWEEPER". Mr. Whidden has lovingly given his rules a name, and that is: "THE MOSCOW RULES". I dont know what it specifically means.. Nothing really, just a clever slogan.. but anyway the rules are as follows.

MOSCOW RULES FOR COUNTER ESPIONAGE INVESTIGATIONS
==========

(1) Assume that all LN's are hostile.
(2) Assume that an approach by a non-LN is hostile until proven otherwise.
(3) Assume that there is always hostile physical surveillance unless
    counter-surveillance proves otherwise.
(4) Assume that all telephone conversations are monitored by LN's.
(5) Assume that all enclosed areas are bugged unless they are 'secure' rooms.
(6) Assume that incoming and outgoing mail will be subject to hostile
    examination.
(7) Assume that anything that is left unattended will be subject to
    examination by LN's.
(8) Assume that locks left unguarded or unprotected will be manipulated
    or bypased and the material they protect will be compromised.
(9) Assume that simple traps will not deceive LN's.
10) Assume that any guard can be recruited by LN's or is himself
    an LN agent.
11) Assume that a pair of guards can be recruited by LN's or are
    themselves agents of LN's.

MOSCOW RULES FOR COUNTERMEASURES INSPECTIONS
==========

(1) Assume that the eavesdropper is listening in the sensitve areas.
(2) Assume that an eavesdropper has an agent near the sensitive area.
(3) Assume that the eavesdropper is watching the entrances of the facility.

(4) Assume that the eavesdropper can maintain a low vulnerability status when he is not listening.
(5) Assume that the eavesdropper is guarding the NLJD band of frequencies.
(6) Assume that the eavesdropper is watching for sweep receiver radiation.

TRANSLATION INTO ENGLISH
==========
Mr Whidden, then goes onto explain what each one of the above rules means in detail, but it is rather long-winded and I wont reprint it in this text. Most of the rules are very simpe to understand, but a few points warrant explanation which I'll put into my own words so I can explain it in more simplistic terms.

First, Mr. Whidden uses the term "LN" (which stands for Local National) which means a person who is indigenous to a specific area. This term has a greater meaning in the field of world intelligence as it means a citizen of a foreign country who may be an agent or informer of that country or it may be a citizen of another country that you recruit as an "agent" or "asset" to work for you. However, in the context of the Moscow Rules it is simply a term of convenience which is not nearly so grande. In such context of the rules it merely refers to a person who may work for an organization or a corporation who is either acting on their own accord or under the direction of others and the purpose of that individual is to infiltrate and or compromise the corporation or organization usually in a covert manner (such as to steal business secrets in industrial espionage), but can be done in an overt manner also if the intent is to destroy or cause harm or embarress the organization.

MOSCOW RULES FOR COUNTER ESPIONAGE INVESTIGATIONS:
(1) Rule 1 which states that you should assume that all LN's are hostile roughly translates to the philosophy of "trust nobody!"
This is extended to include the very person who hired you!
As unlikely as it may seem, if you look at the rules it is a very logical conclusion, especially in a corporate situation. It is very common for the "security department" to be the one to request that a TSCM countermeasures sweep be performed, this can be done to please the bosses and make the executives feel that since the sweep was done all the confidential conversations are secure.
In a real world situation it is likely that one or more individuals in the 'security department' itself may be the actual perpetrator and they thusly will be well aware of the search for eavesdropping devices and they will have the ability to easily deactivate or remove the clandestine devices before the search, wheras they can be replaced promptly after the search was performed. This tactic of infiltration

not only gives the eavesdroppers the advatage of knowing when a sweep is to be performed but also provides a form of 'cover' since the security employee (really an LN "agent") will seem all the more legitimate since he is the one that ordered the sweep. One can reference Moscow Rules 10 & 11 to realize that "guards" and "security" should not usually be given 100 percent trust. The "SWEEPER" MUST obey what the security staff says, even if the sweeper suspects the guards or security staff as being the actual perpetrators, and once actual proof is established to concurr that fact, the sweeper should convey that possibility to some other person within the company who the sweeper feels is trustworthy.

(4) Rule 4 is an especially important one. Although it needs no elaboration, I cannot stress how important it is NEVER EVER to discuss anything sensitive over a telephone (that is even more so true if you have a cordles or cellular phone).
Also, it should also be noted in my personal opinion, that not even encrypted phones/faxes should be beyond suspicion. Their exists many ways to defeat such encryption. The easiest is simply to compromise the keys which is not a difficult task if your target is unaware. A simple blag-bag job is all that is needed to either liberate the codes from the encryption unit itself or from a locked safe or drawer which can then be copied to floppy and the original code returned to its position undisturbed. Modern encryption units such as the STU phones do help to some small extent to guard against such attacks by the uses of "ignition or code keys" which can be physically taken from the unit to help secure the units key integrity, but their are ways around that.
Then of course, it is never beyond reason to doubt that the encryption itself can be cracked if it is deemed a priority. This is a mere simple task which can be done in a half a second if your using weak encryption on your phone such as simple "inversion" chips or other simple encryption units which are widly sold in catalogs. It is also not out of reason to realize that even DES is not safe anymore, although its a hell of alot safer than "inversion chips" which can be cracked with a $50 kit available in the classifieds of most electronic magazines.

(5) Rule 5 states that all conversations should be considered vulnerable unless conducted in a "secure" room. Personally, I hold to the philosophy that THEIR IS NO SUCH THING as a "secure" room, but then one must realize that this is reality and you cannot be completely paranoid.

A "secure" room is a complicated term to define as their are many degrees of what is considered "secure". The ultimate "secure" room would be completely RF (Radio Frequency) proof and would thusly attenuate completely all RF transmissions from "bugs", but the

security must be extended to insure that no wires/fiber enter the room or leave the room as they can carry clandestine signals hidden on that wire (or at the very least all wires must be monitored for hidden signals). The room must have no loudspeakers which can act as microphones, the room preferable would have no windows and if it did would attenute any Infrared light so as to protect against RF/IR transmitters. And lastly the room would be acoustically secure which means their would be virtually no acoustic leakage (in otherwords no sound could be heard on the other side of the wall using any types of devices such as microphones and high powered amplifiers.) Also, to be acoustically secure, the room should have sufficient random masking signals present and continuously fed into the secure room. Their should be several of such masking generators in use at different points in the room and in addition all plenums and air vents should be masked as well. In addition, the walls as well as any windows should be masked using a transducer element which vibrates all windows and walls in a random fashion to further defeat any clandestine listening devices such as contact microphones, spike or tube microphones which are drilled into the wall from the opposite non-guarded side, as well as techniques of 'laser/microwave pick-off'.

(8) Rule 8 also warrants elaboration. All mechanical locking mechanisms are easily bypassed by persons with experience in such fields - which very often includes an eavesdropper himself - or on occasion, an eavesdropper may have a "keyman" which is a person who is an entry specialist (called "quick-entry" in the locksmithing field).

To properly secure a facility electronic locking mechanisms should be used which are much harder (yet not impossible to defeat). Preferably a secure installation should go beyond simple electronic locking mechanisms (such as key card system connected to an electric strike). A complete access system must be incorporated with full provisions for software logging of all entries and exits, as well as "anti-passback" protection to further enhance accountability and security and tracking.

All safes should be of the electronic type, NOT the mechanical combination type of yesteryear. It is not a difficult task to bypass combination safes nowadays. The top expert safecrackers can ply their trade in an hour to two hours time, and a device now exists on the market which cracks safes automatically using a computer controlled mechanism and does so in approximately 1 hour. Electronic safes are virtually 100 percent secure and are the current standard on all government facilities where classified information is stored. The electronic safe itself should preferably have accountability and logging features built-in with seperate access codes for multiple users of that safe.

MOSCOW RULES FOR COUNTERMEASURES INSPECTIONS:

(3) Rule 3 is a most important one and is something both the countermeasures technician as well as his client should keep in mind and previously discuss during the initial client contact. Although it does not suit every situation, but in many cases it would be wise not to be recognized as a countermeasures technician for obvious reasons. One does not want to spook the eavesroppers into either shutting their devices off, pulling them out temporarily or at worst "skipping town" never to be heard from, and unlikely to be caught.

How does a countermeasures technician arrive at his clients office in a discreet manner?

When it is deemed necessary, a simple "disguise" is in order. The TSCM Tech should blend in to look like all other employees, he should look and act like all employees, and in fact NO EMPLOYEES except a select few should even know the TSCM techs are who they are. The TSCM tech should arrive in a vehichle preferable a "work" vehicle which can be disguised as either a maintenance or utility company vehicle.

All equipment should be carried in, under concealment. This means that some type of discreet yet common bag should be used to carry the equipment in. It is obviously suspicious for a person to carry in 5 briefcases (some of them being oversized cases indicating to the eavesdropper that its no "ordinary" briefcase) into a building.

One tactic I have personally used myself when doing the occasional sweep for a client, is to arrive in a borrowed van which bears the name of some maintenance company. My typical motife is to arrive as a "painter" and when I enter the office if its a large office I announce myself as such to the secretary. This of course must be made clear in advance to the client so that the secretary knows that the "painter" (or "plumber" or "carpentry contractor" will arrive), again it should be stressed that not even secretaries should be made aware of the TSCM Techs identity or purpose of visit. All equipment I carry in discreetly in a painters spackle bag which is just large enough for most of my sweep gear. And for my spectrum analyzer which is too large for the spackle bag, I just haul that into the office discreetly wrapped up in a large painters cloth tarp.

Usually I strip the plates off of the van and I remove the inspection and registration sticker so as to avoid being "checked-out" by an LN agent who may find your van "suspicous". This in actuallity IS NOT THE IDEAL METHOD. I merely do that for convenience purposes. (because I am not rich I cant afford multiple vans and vehicles registered to multiple legitimate "ghost" companies which all must pay taxes and be registered with the state you do business in.) In fact its better to arrive in a van which has license plates

and registration which is legitimate as well as the company
logo painted on the side of the truck belonging to an established
legal business. This provides a better degree of cover.
Although it is very very rare, it should likewise not be considered
out of the question that an LN might ckeck out the validity of
your company (a simple check of the yellow pages should turn up your
company name.. and if not.... suspicion..) It doesnt take a genius
likewise to figure out that if you see a white van marked "Acme
Painting
Company" parked in front of your target building which you are
eavesdropping upon, you should become suspicious.

(4) Assume that the eavesdropper can maintain a low vulnerability status
when he is not listening.

What rule number 4 deals with, is the eavesdroppers ability to make
himself "invisible" to the TSCM Technician, Security Staff and his
intended "targets" by various methods too detailed to describe here.

This mainly includes 2 tactics..
[1] shutting the taps or bugs off remotely (and)
[2] having an LN agent remove the taps/bugs after they are
no longer needed and then promptly replacing them when they
are needed again. It merely takes seconds for an agent who
has access to the facilities to install such devices in the
compromoised area.

(5) Assume that the eavesdropper is guarding the NLJD band of
frequencies.

This one is a bit esoteric to the laymen, but the term NLJD refers to
a device which is used by countermeasures technician to locate
clandestine listening devices which may be buried under concealment
inside of a wall, desk, drawer, behind books, buried covertly inside
a piece of wood or other structural material which could not be
inspected
by any other means.

The NLJD works much like a metal detector, only the principle involved
is
ALOT more sophisticated. The device doesnt merely search for metal.
Rather, it searches for semiconductor junctions such as transistors and
diodes which would be present in all "bugs" (transmitters) as well as
in most microphones, etc.. The NLJD is mainly usefull for finding a
clandestine device which is NOT ACTIVATED! This has to do with one of
the rules above (Rule #4). The eavesdropper may have the ability to
turn the device off remotely or even manually and as such would not
be detected with normal RF "sweeping" gear which looks for an RF/IR
signal.
(since if the device is OFF, it thusly generates no RF/IR signal).

The NLJD works by transmittng a microwave frequency signal (between
800 - 950MHz [depending on the version, and the laws of the country
which the unit is sold in]. The signal power of these units is
relatively low 20mW - 300mW for non-government ("consumer"/industry)
versions [legal U.S.A versions a.k.a FCC approved] and 300mW to approx

3 Watts for law enforcement and government units. The greater output power
of the government models allows a higher degree of penetration into deeply
embedded or dense materials. The typical radiated ouput for a U.S.A. version
NLJD is 915MHz and for European versions is often 888.5MHz.

Since the unit emits a microwave it thusly radiates through the airwaves and the eavesdropper can thusly detect it using his scanner. A clever eavesdropper will continuously scan the band of frequencies, or a specific
frequency if the eavesdropper is relatively sure of the frequency on which
the targets NLJD uses. Once the eavesdropper detects the signal, he can then
remotely deactivate his clandestine devices.

It should be noted of course, that a clever eavesdropper has at their disposal, a number of uniquely different methods in which to "fool" an NLJD unit into not detecting the listening device completely, or methods to
fool the user of the NLJD into believing that the reflected signal is a false alarm.. One example is to modify the casing of the listening device,
and RF filter all the leads when done in such a manner that they clandestine
device will reflection a large portion of 3rd harmonics while keeping secondary harmonics to a minimum thus indicating to the NLJD user perhaps
that the unit is picking up disimilar metals (sheetrock screws, nails, rebar,
etc..) rather than semiconductors.
I shall not detail these particular processes as its irrelevant and unwise
but if anyone actually cares to know the methods are I can discuss that with
you in more detail if you ask.

(6) Assume that the eavesdropper is watching for sweep receiver radiation.

This is a bit more esoteric and its something which I dont feel is any great threat. But their might be some government experts in the field who are a bit more sophisticated who would say otherwise. But in a real life situation I dont see it happening unless the eavesdropper is himself a former government employee.

ALL electronic equipment generates EMI (Electromagnetic Interference) which is essentially spurious radiation emmited unintentionally. As such these radio wave emmisions are also generated from any type of "sweep" equipment which the countermeasures technician may use.
A sophisticated eavesdropper can detect these spurious emmisions and take it as a sign that sweep equipment is being used and the sweep is now in progress. The eavesdropper then shuts his clandestine devices off remotely.

In reality the ability to do this is actually quite simple. Its just that I find it unrealistic and I dont think many buggist in this country go to all that trouble. Not unless its a super sophisticated operation, or unless the eavesdropper is being payed well to take such precautions. But then super sophisticated operations are not the norm. Not even close.
Usually the bugging is done by amateurs using crude bugging equipment which is easily detected, and is not even concealed well on top of it. Most bugging devices are usually not even remotely activated and likewise
their usually not protected against NLJD sweeps either, unless the person
who is doing the eavesdropping is a pro which is rarely the case.

MOSCOW RULES FOR TELEPHONE SYSTEM INSPECTIONS
==========

(1) Assume that the eavesdropper is listening to room sounds through the telephone instrument until tests prove otherwise.

(2) Assume that the eavesdropper is listening across the line when the line is active.

(3) Assume that the eavesdropper may be monitoring the line when it is inactive.

(4) Assume that the eavesdropper is monitoring the line to detect TDR and RF tracing signals.

MOSCOW RULES FOR TELEPHONE SYSTEM INSPECTIONS:

(1) The eavesdropper has a variety of techniques at his disposal which enable him to listen to 'room sounds' ("room audio" [note 1]) from a remote location. I will not discuss that in detail, because all the techniques involved in telephone and wireline attacks could fill an entire book in itself.
Generally however, their are two main techniques that could be employed. [Their are actually another 3 or 4 techniques but I shant get into discussing those for the sake of brevity.]

[a] 'Hot-miked telephone' otherwise called a 'Hot-On-Hook telephone' is one method, which involves modifying an actual telephone which is in a targets location (in reality, the targets phone itself is not modified, but an identical replacement is brought in and switched
with the original [this technique of switching phones of course warrants caution as the target could possibly notice the difference
between the two by noting scuff marks, etc.. that were on the original phone]. The modification consists of a circuit that will allow the eavesdropper to listen to room sounds while the phone is still "on-hook". The modification "drops-out" once the phone

is picked up for use and is brought "off-hook" (in which case, the eavesdropper would then have a seperate circuit which could monitor the phone conversation.

[b] The second most common method is called an "infinity transmitter", which in the 'olden days' circa 1960/70 was called a "harmonica bug".
This is a slight variation of the hot-miked telephone. It is similar in that it allows a person to listen to room audio from a remote location, however the system employed need not be part of the actual telephone. The device could be hidden anywhere along the phone line in close proximity to the target where a seperate microphone can listen to room audio which is then sent through the phone lines while the phone is 'on-hook'. When the phone is lifted 'off-hook', the device drops-out. The device is activated remotely by the eavesdropper by simply calling the targets phone line and then activating the device.

Room sounds could also be monitored by simply placing a microphone across any line pair, preferably a line pair which is not currently activated for phone useage (ie: the second yellow-black pair.) This would allow constant monitoring of the room audio even when the target uses the phone (which would be on line pair 1 (red-green) and thusly would not conflict. The microphone could either generate its own signal 9which has the disadvantage of being easier to detect because the microphone transmits constantly , or could use a microphone element which requires an external voltage such as in a carbon mic.
In the case of carbon microphones, the eavesdropper need only apply a small voltage to the line and the microphone will activate sending intercepted audio down the line. The device has the advantage that it is slightly harder to detect (especially inadvertently) because the unit only operates when the eavesdropper has the device activated.
Countermeasures technicians can find the device (in its simplest form) easy enough by just applying voltage to the line. But more sophisticated set-ups would utilize a 4-layer diode, SCR, or a reverse polarity configuration or some other method to hinder and thwart detection.

(2) Rule 2 is fairly obvious and needs little explanation. Always assume that a phone line can be, or currently is being monitored.

It is very important for the laymen to make the distinction between the two facts in the above statement which are:

[a] the phone/line "could" be tapped.

[b] the phone/line "is being" tapped.

It does not make one paranoid to come to the conclusion and realization that a phone "could" be tapped. It merely makes one alert and an informed individual. That does not mean that one should insist that a line "is" tapped, but it should simply be considered a possibilty which one must take into consideration and act accordingly on.

Thusly, if one conducts confidential business in which it would be of important consequence to keep the conversation from prying ears of the eavesdropper, one should always employ end-to-end encryption through the use of telephone/fascimile "scramblers". [note 2]

One must make the decision for themselves regarding what is to be kept secret and what can be disclosed, and you must come to some sort of plan of action regarding what the different levels of confidentiality are. Some secrets are worth keeping more than others. In fact one might even say some secrets are so great that you should not disclose them to anyone ever. That would be the ultimate form of security.. As an example, if you had just murdered someone, obviously any sane individual should not announce that over the phone lines, no matter how secure you feel that phone line is. Because their is no degree of security which is worth 25 years in prison or death. Even encryption (phone scramblers) should not be considered secure in such cases as they can be compromised rather easily by simply bypassing the encryption altogether through modification by the eavesdropper, or by simply liberating the code keys from the unit (which is a simple task with some encryption units while alot more difficult in the better units.)

Whenever a line pair is to be examined or traced (for maintenance purposes such as working on a phone or computer network in an office or home, or when a countermeasures search is being done, it is preferable that "audio" signals of a strange nature (line tracing signals) should NOT be placed across the line as they would be suspicious to an eavesdropper in which case the eavesdropper might deactivate remotely any devices which he may have installed which could put the devices in a low-profile status making them more difficult to detect.

So how then does one trace a line without using an "audible line tracer" as is the standard method among technicians? The alternative is to use either an RF (Radio Frequency) tracer system which is relatively inexpensive (and also has many advatages over audible tracers such as the ability to track wires through walls without having to open up the wall or structure for physical examination) or one could utilize an "ultrasonic" tracer device which sends an inaudible signal down the line. These aultrasonic tracers are an indespensible tool which come in two forms. The first is simply a aultrasonic tone tracer and merely produces a single tone for identifying line pairs. The second type of ultrasonic device actually modulates a voice signals onto a wire pair so that it

is inaudible and above both the range of human hearing and likewise cannot be picked up by either microphones of any type and cannot be demodulated by any type of standard amplifier unit which is not designed to amplify sounds above the standard human hearing/speaking range. Only a specialized matching ultrasonic demodulation amplifier can intercept and convert the signals back into the human hearing range.

Keep in mind with the above however, that rule #3 below shall apply. Rule #3 states that the eavesdropper "may" be able to hear your line tracing with the phone on-hook. So one has to balance this consideration out. Nine times out of Ten you would be better off sending these signals down the line because most eavesdroppers DO NOT monitor a phone which is on-hook, nor do they look for signals on inactive lines (not unless they are professionals, or are simply getting payed alot of money to do that extra work which is often unnecessary).
But if your up against a sophisticated eavesdropper and you know of his capabilities it would probably be wise in such case NOT to send any strange signals down a wire pair other than ordinary phone conversations.

(3) Most of the time, telephone surveillance, whether it be the interception of phone conversations where the phone is off-hook, or even monitoring of room conversations when the line is on-hook involves the use of some sort of "activation" device which records the conversations when and only when those conversations are present.
When the conversation ceases the device will shut itself off (usually)
so as to conserve tape (and in addition make it easier for the eavesdropper to find the conversations in the recorded tapes.

When dealing with recording telephone calls, a device is used which monitors the voltage on the line for off-hook/on-hook conditions and then activates a special tape recorder (with a remote activation jack) when the phone goes off-hook. [although a more clever eavesdropper
would not use such a device but would rather use a VOX (voice [sound level] activated unit as opposed a voltage sensing unit which can actually be "tricked" as well as "detected" alot more easily which should be coupled to an inductive pick-up coil (or at the least
a high-impedance capacitively coupled interface). VOX units too also have their problems, namely they can have havoc wreaked upon them by the use of masking devices or "telephone security units" which are
now widely sold on the market for a couple hundred dollars. These telephone security units have the ability to defeat most simple eavesdropping methods utilizing techniques such as masking as well as "Line Balancing". The latter technique of balancing performed by raising the voltage, while the current is simultaneously lowered. Such a technique does not interfere with the PSTN Central Office and will give the user a dial-tone when the line is raised off-hook(600 Ohms)
and will thusly defeats most voltage activated devices such as simple
telephone tap transmistters as well as drop-out relays (telephone

recorder controllers).

The foolish individual could conclude that if most eavesdroppers used a voltage activated device that only recorded audio when the phone was "off-hook", then the line should be secured in an "on-hook" condition. Example, a person could then transmit his voice within the household or office while the phone was still "on-hook" using a relatively simple circuit to do that and "supposedly" that would alow for safe conversation, and it would be safe "if" a voltage activated telephone recording adapter was used.
However, many eavesdroppers (sophisticated ones) may be a bit more clever than that. The clever eavesdropper may monitor a line pair even when it is inactive (such as when a phone is "on-hook".)
This would allow the eavesdropper to hear "AUDIO" [note 1] even when the phone is off-hook. Note I use the word AUDIO very carefully. Because in such an instance, the eavsdropper may NOT just be listening to secret conversations which occur "on-hook" but he may be listening to other audio which could be a potential threat to the eavesdropper such a the sounds of audible line tracing, ultrasonic line tracing or ultrasonic voice modulation, as well as RF tracing, and lastly the eavesdropper could be looking for the signals emmenating from a TDR (see rule #4 explanation).

(4) The last rule is a rather esoterical one which is of more concern to the countermeasures technician who is performing the search as opposed to concern of your ordinary individual or businessman concerned with the rules to insuring privacy.

Rule #4 is just a follow up to rule #3 which states that an eavesdropper could possibly be monitoring the inactive line pair. In rule #4 we get specific in saying that an eavesdropper may be looking for RF signals or TDR signals which may be an indication of a countermeasures "sweep" which is being conducted. This should concern the eavesdropper for obvious reasons, which are that he could possibly be discovered very soon if the technician is a competant one, or if the eavesdroppers set-up is crude or poorly installed in which case it could possibly be detected.

I have already explained ultrasonic and RF tracing above in rule 3, so I'll just deal with TDR's.

A TDR is common abbreviation for a device known as a Time Domain Reflectometer. You pronounce the units name by simply saying the letters.. "T" - "D" - "R".

The TDR is a common tool of anyone who works exensively with wires (or fiber optic cabling) of any type. The type of TDR we are discussing is only for the "wire" and not "fiber optic" type.
TDR's are used by cable company technicians, computer network

technicians, telephone lineman or repair personell, as well as surveillance countermeasures technicians.

A TDR is a device (usually a hand-held size device although slightly larger and more powerfull bench-top units are available) which emits a mild powered signal into a wire pair. This signal gets sent down a wire pair, or through a coaxial cable and gets partially reflected off of any discontinuity on the line pair. Herein, I'll refer to any discontinuous reflections as an "anomaly" on the wire. I use the word as opposed to discontinuity (because its easier to type) and because much like an anomoly it is indicative of the unknown. And thats what your looking for when doing a TSCM TDR sweep of a wire pair. Your looking for unknown or strange situations. It is these anomalies which the technician is looking for which are a possible source of the problem (or could even indicate that everything is normal if their is supposed to be an anomoly at some point).

The word "anomaly" is a generic term which refers to anything on the line which will interfere with the signal going through the line. To put it another way, it is something which causes part of the signal to literally reflect backwards from the point of origin instead of traveling freely and smoothly through the wire.

This "reflection" of the signal is what the TDR is looking to receive after it emits the original pulse. The reflection which could be of varying degrees of intensity depending on how large the anomaly is. The larger the anomaly, the larger the reflection, and occasionaly that means the bigger the problem. Ideally the signal is supposed to travel through the wire impeded as little as possible. Anomalies are caused by a wide variety of things too great to discuss here. They can be caused by imperfections in the wire itself, they can be caused by splices in the line, they can be caused by "connectors" on a wireline which join 2 wires together or a wire to a piece of equipment. Anomalies can be caused by "termination plugs" which are a dummy loads placed at the end of a unused wirepair. Anomalies can also be caused by physical hardware on the line such as splitters, filters, junction boxes, 66/110blocks, entrance bridges, and the list can go on and on.

The countermeasures technician is primarily interested in looking for things such as splices on the line which could be indicative of a telephone tap. Keep in mind, that the word "splice" does not necessarily preclude that a line was physically "spliced" (ie: cut and then

re-connected.) It also can imply a simple "tap" on the line where one wire (alligator clip, etc..) is touching upon the original wireline. TDR's have a typical range of 1,000 - 10,000 feet. A typical handheld TDR used by computer network installers will have ranges of 1,000 - 2k feet. Countermeasures technicians often utilize slightly more powerfull models extending 2,000 - 5,000 feet so they can have the ability to trace large amounts of wires present in office buildings. And benchmodel units which are usually the most powerfull (although some handheld units are capable of such) can extend upwards of 10,000 or more feet. These units can pinpoint "flaws" or "anomalies" on a wireline to a resolution of millimeters which makes them damned accurate devices which can tell you exactly where the flaw is down the line. (typically however in high powered devices the resolution is limited to feet or meters).

The TDR is most effective when it is used on a routine basis and a day-to-day (or more likely week-to-week or moth-to-month) comparison can be made between the different or same results. Ideally, the results of the TDR should always be the same. Should a result be significantly different on one occasion, or something appears to have been spliced/tapped onto the line it will be readily apparent.

Of course for the TDR test to be most effective, it should be realized that the initial tests of the TDR must be done when the line was "clean". If the line was tapped in the first place the first time you tested it, then all subsequent comparisons thereafter are of little use because you cant compare a "clean" like with a "tapped" line.

However, that factor doesnt render a TDR test completely useless. One does not necessarily rely solely on the technique of comparison from one time to another. Other methods exist for using the TDR which are a combination of tracing the line physically with the TDR from the demarc point inwards to the telephone instruments and physically searching the line for taps/splices in conjunction with the use of voltmeters or telephone analyzers to search for imbalanced loops, or imbalanced lines to ground, crossed line pairs as well as suspicious line impedances. Likewise, the search should occur from the demarc point outwards towards the telephone company as far as one can go. The search should extend out the end of the customers property, but a countermeasures technician who does not mind breaking a few laws might feel free to extend the test point up to the neighborhood cross connect cabinets where the distribution cable meets the feeders.

[note 1]

In surveillance lingo, the word "AUDIO" is often used as opposed to the word "SOUND" or "CONVERSATION". The meanings are almost synonymous, but their is a slight difference. The word "audio" is used because it denotes any type of intelligence which could be collected and is not limited to intercepting spoken conversations (spoken words).

[note 2]

Even encryption (phone scramblers) should not be considered secure as they can be compromised rather easily by simply bypassing the encryption altogether through modification of the telephone instrument by the eavesdropper, or by simply liberating the code keys from the unit.

WHAT THIS MEANS TO YOU AND ME

One may ponder the question of "what the hell does this article have to do at all with me?"
How does this concern you if you dont run a company?
How does this concern you if you are not doing anything illegal?
How does this conern you if you believe your not a target being watched?

I have no answer. Take from this article what you will. It is provided for informational purposes. I have discussed not only quite a bit about surveillance as well as countermeasures, but also the some of the terms which is used by people who work in that field. These are terms which you may run across one day if you work in the field of general security, and you will thusly be able to speak a bit more authoritatively to your colleagues who may not know much about espionage.

But if you have any respect for your own privacy, then you should heed some of the advice discussed herein.

You need not be a corporate executive to realize the need not only for your privacy but the need to recognize how many people by their own acts contribute to the privacy violations. They do this by using cordless phones, cellular phones, by using paging beepers and even by holding confidential conversations on unsecured phone lines instead of in person.

I write this specific article for those people on computer bulletin board systems, and this is aimed SPECIFICALLY at those who refer to themselves as "computer hackers" or "telephone phreaks".. If you do not recognize the value in this article then you are a great fool indeed.

Remember folks.. Paranoia is our friend. You never know who is watching or listening. Always assume the worst and thusly disclose the least you can; even to so-called friends.

Never discuss anything illegal over a telephone be it landline or cordless.

Never keep any incriminating material at your home. Or at the very least any such information if illegal, should not be 'feloniously' illegal.

Never discuss any majorly illegal acts (in my book thats defined as anything
thats a felony) with anyone else, even friends. And if you do, then you should be sufficiently vague and even intentionally misleading to your friends so as to give the eavesdroppers "misiformation".

Never disclose to any friend the full capabilities of your power, your knowledge, etc.. If necessary intentionally mislead those friends by overstating or understating your capabilities or knowledge in order to feed misinformation to an eavesdropper. This can be done to "spook" your eavesdropper and make them enact a move prematurely, or to make them believe what you want them to believe for whatever reason you see fit. In addition, feed just enough thruthfull information so as to 'whet the appetite' of the eavesdropper and not give away your conversation as total obvious misinformation.