WHO'S LISTENING

presented by

Ian A. Murphy, President & CEO
IAM Secure Data Systems Inc.
1225 North Second Street
Philadelphia, Pa 19122-4314
(215) 925-2928

Who's Listening

Over the years, there has been a number of different studies and discoveries that would alter personal and electronic security over time. Devices able to "listen" to almost any form of communications have become commonplace and are available "over the counter" from a varied number of sources. Such units range from ten to fifteen dollars to expensive set-ups that employ microwaves and lasers for the interception of almost any audio signal in the spectrum. But now with somewhat needed protection from outsiders in reference to this problem, a number of solutions have been put in place and global protection is insured in environments that have such need. But the coverage of environment has had a a major change in protective attention now being place on the actual electronic emmanations that are so common with todays standard electronic apparatus. Electronic telephones, computers and communications networks, ATM's, radio and television stations are just part of the overall electronic bubble that we have placed our society into with the hopes of providing better and faster methods to make daily life a bit easier. But with such a fragile structure as the electronic bubble, we have new opportunities to discover secrets never before possible due to the lack of technology. The same technology that helps us in one way or another may also be helping others unbeknownist to those who are protecting the environment in the first place. Signal leakage, either by design or by accident may lead to total collapse of protective measures due to "wide open spaces" in the protective sphere. In this particular paper, we will discuss the possible problems of common office technology may bring in un-securing your installation.

Our main focus will be in the areas concerning with the emmanations or transmissions of "Tempest" frequencies. "Tempest", is the code name given to a specfic area concerned with radio frequencies radiated by computing equipment by the U.S. Dept. of Defense. This "concern" from such equipment dates back to the late 50's. The concern ranged from the possible interception of "informational information" by sources other than the intended users of such. The problem is more easily reconigized by the current requirement of normal electronic equipment having to conform to emmision standards put forth by the Federal Communications Commission in reference to the amount of electronic "noise" generated by common standard technology so that such signals do not interfer with other such pieces of equipment or their operations.

To describe in simple terms, Tempest frequencies are almost straight through from commerical AM stations to the upper reaches of 600 Mhz. They are generated or transmitted by any number of different common daily life electrical and electronic systems. Your TV puts out one frequency, the stereo another, the common electronic telephone, cordless phones still another, the microwave oven puts out another and the wireless alarm does it to, and story goes on. So just as all of these pieces of equipment emmit a signal, so does the personal computer.

We will describe two possible examples of such informational information and the abilty for some with directed intent to cause potentially fatal results due to the use of directed "noise". It should be noted that the current specifications for "Tempest" approved systems is considered classified by the DOD and these specs were not available to the author. But if one was to look at the specs for normal computing equipment and reduce the allowed emmission output by at least 50 percent, that may be a realistic emmission standard accepted by the DOD.

Example 1

"We had better "Czech" this out!

In 1987, a very strange occurence concerning forgein nationals from an Eastern bloc nation entered this country in a large camper-like truck via the border checkpoint at Niagra Falls, New York. The visitors numbering 4 or 5, were in the country under tourist visa's and were reported to be representives of the countries automobile and truck industries here on a promotional tour to garnner interest in their exportable products. The one problem with the "visitors" is that none of them had any connection with such industries in their home country. In fact, the visitors were far from what they supposedly represented. The group descripton read like a Whos' Who of mid-level management of Eastern bloc intelligence operations. The group reportedly consisted of a nuclear physists, a specialist in aerial map-making complete with a small ultra-light powered aircraft, a communications and computer expert and two communist party officals.

Over a 5 month period, the group was reported to have visited 17 states looking at 40 to 48 sites dealing with military and defense contractor sites. The vehicle and its occupants were reportedly followed by over 100 agents of the FBI, NSA, Secret Service and State department and at least one over flight of a military reservation was reported. Even though the overflown site was not identified, one site was. This site, was the "sensitive" naval communications center for the Pacific Fleet located in San Diego. It was reported that the truck and it's occupants were parked a few hundred yards from the facility for several days and according to law, were in no violation of any current statute at the time. The group was also at or around at the 2800 acre North Island Naval Air Station based in Coronado, California. The spokesman for the base stated that you could not see much of anything going on except for the take-off and landing of aircraft which you could see from almost any place.

Common sense states that you do not have to be inside the facility in either a physical or electronic standpoint to collect information. You can park in any lot or street close enough to your supposed target and stick up your antennas. No property violations, no photo restrictions to comply with, no restrictions at all because you are sitting in a public place, parked or having coffee with your "ears" on. A good example of such parking was reported in a paper published in Computers and Security 4, titled Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? by William Van Eck, copyright 1985.

He stated
that when they were conducting their experiments in the open on public roadways, with a van and antenna system that was quite noticable, no one asked what they were doing or had any thought about the time spent doing such things.

The end of this particular story is as follows: At the end of the suspect journey, the truck was searched at the Nosgales, AZ border checkpoint and was then released. Nothing considered illegal was found in the search and the truck and it's passengers were released and entered Mexico. Now even though the truck was suspected of performing passive "eavesdropping" operations, the federal goverment had no legal right to hold either the truck or crew. And the possible intercepted information was then released from the country. It should be noted that the truck could have a number of standard "off the shelf" items. These items could have consisted of 2 general coverage radios with a combined tuning range between 100 Khz to 2 Ghz., an IBM personal computer clone, various cheap video and signal enhancment equipment, printers and modems, and other such complement devices.

None of the equipment would be any "James Bond" type of gear and the basic suspected set-up would cost the operation less than 10,000 dollars if budgeted correctly. And if possible, use of other simple off the shelf type radios like the 200.00 unit available from Radio Shack that covers 150 Khz to 30 Mhz is not at all unheard of due to some budget constraints. And since most emmanated signals generated by logical devices are within commerical AM and FM frequencies, the use of a standard auto radio antenna would suffice to use as a pickup.

So the major concern with such actions comes from the ability of simple equipment to detect, register and decipher such emmanations with relative ease. The ability of such persons and possible actions able to penitrate the electronic fog of our society should be a clear distinct warning to those concerned with security in general.

In addition to all of the above, the author contacted various federal goverment agencies in reference to this information and was told that they had no knowledge of such an investigation and could not tell where such supposed counter-intelligence operations were controlled from or who to contact in reference to supplying such information. Current "Freedom of Information Act" requests for information concerning this supposed federal project are underway.

An interesting note about filing the forms for access to information about the Czech incident is described to give guidance to others who may wish to investigate this incident and seek help from such elected officals.

When the papers were filed for the desemenation of information through the Freedom of Information Act, members of the U.S. Senate and Congress were contacted in reference to this matter. The first contact was placed through Senator Arlen Spectors office in Philadelphia, Pa.

We were first rebuffed by persons who refused to identify themselves with the statement " I am sorry, but that information is covered by the 1974 Privacy Act, Click! Well we called back and informed the person who answered the call of the situation and then were re-connected and informed them that Czech citizens were not covered by US privacy laws and that there was no invasion of privacy.

They called the FBI and asked if they were the way such things were handled, and were told yes or no. But they had no answer for any question put forward and said " They were sorry!", but we don't know how to help you!. Our second contact to Senator Spectors office in Philadelphia as in essance like the first, they would not assist nor would explain why they took this position in the first pace. During our second contact we spoke to a Miss or Mrs. Anderson. She stated that such requests were not in the senator's perview and they could not assist in this matter. When asked why it as not in the senators preview, we were informed that they do not have to give a response. When asked for an offical response, we were informed that no offical response would be given. But as a side note, Senator Hienz office said that they would forward the requests to Spectors office in Washington. One other thought on this matter: I am sure that if the good senator wants to get some information, his staff jumps through hoops to get him all he wants and then some! A pre-publish copy of this article will be delivered so that even he (or his office staff, who were of no help at all due to a tough question placed to them by a citizen) may learn of what may be going on in his own country. So much for gaining assitance from a senator who sits on a judical panel. We visited next the office of John Hienz. Again, funny looks about the Freedom of Information Act and they hemmed and hawed at the questions presented. They took the requests and said they would try and see what could be done. Our final visit was to our local congressman, Tom Foglietta, whos office still stated the 1974 Privacy law, but took the requests when presented in person. It pays to visit your elected representives working areas. So much to do (if you work there!) in a goverment office. Other federal agencies including the FBI were most helpful in complying with the requests. Of course we found this most interesting. Is it so they could possibly reclassify the information to a "Secret" status instead of what it may be now.

Other agencies contacted in reference to FOIA requests include the CIA, NSA, NRO, Customs, State Dept., Army Automated Intelligence and Military Police, FBI, FCC .

Example 2

"Breaker, Breaker, Wally Gator!"

During the 70's, the United States had a short term love affair with the Citizens Band radio. What were once clean channels were suddenly crammed with persons who wanted to be able to communicate with any number of persons who also had such capabilities. Suddenly, everyone had one of these radios in the home or car and some were know to have both. Numerous persons ran such rigs with varing illegal applications

To give a brief explanation of CB's, we will keep it simple. CB's transmit in the upper reaches of 26 Mhz to 27 Mhz or 11 meters band. CB's are allowed to operate with a maximum output of 5 watts radiated power. Of course this limited power was not sufficent for some users and the use of linear amplifiers or "heat" was commonplace. Stations were known to be transmitting 50 to 2 thousand watts to their antennas which in turn would increase such signals to a power of over 2 hundred thousand watts. Some operators were known to show the intense power outputs with the use of flourescent lightbulbs and the abilty to "light" these tubes from a distance without electrical connections with the amplified radiated power of their antennas.

Some persons were known to have full control of channels in their respective areas and would blank out anyone who would not conform to the channels establised rules or procedures. Others set-up pirate stations that would broadcast commerical music for all to hear complete with news, weather and sports. Such actions would tie up frequencies and caused a general crackdown by the FCC in the later years. But the problem still continues and the FCC has all but given up on the idea of any enforcement of regulations concerning such operations on the 11 meter or 27 Mhz band.

The craze of CB's left the general populace by the late 70's and was back in the hands of those who would truely use such radios. Those who would use such radios best known, would be the persons called truckers since that is what they do. They "truck" goods from one place to another and are concerned with time and travel conditions as most of us are. The truckers always had some "heat" on-board for those times when they could not get their signal "out". It was and still is considered an insurance policy by most who have this technology and is widespread in its use.

Now over time, with the continued expansion of these radios, the truckers began to switch to marine band radios in the 10 meter band and were conversing just as before. Since the 10 meter band would permit such radios and the increased power output, the switch to 10 meters was only a matter of time. Now, it is reported that most truckers are using and abusing such frequencies and their is little that can be done to stop such occurances from happening. To add to all of the mess, such radios have the ability to switch operating frequencies with the touch of a button. In brief, the 10 meter radios can switch to the 11 meter (CB) band with minor modifcations. And back and forth frequency hopping is as easy as tuning in the average auto radio.

One other interesting aspect of these 10 and 11 meter radios and their use of 10 meter amplifiers, is the problem of interference generated by the amplifiers due to the lack RF chokes and filters for the simple reason that the unit is designed for use on the 10, meter band, not the 11 meter band and thats what the chokes and filters look for, 10 meters, nothing more, nothing less!

Enter the common travelling person with a late model vehicle. Most vehicles today have some form of directed artifical intelliengence working under the hood. The "brain" controls any number of common operations ranging from air / fuel mixtures to how and when braking systems will perform. Microprocessors in todays cars are as common as seatbelts and are now required to assist in normal operations of said vehicles. And this is where the problem begins. Since the auto must have such control circuitry to function, then the possible interference of such operations becomes a real threat. But what sort of threat could be possible with a car, its control systems and a high powered transmitting radio? Well, if one was to examine the idea of overriding or shuting down said operations, the car would cease to function in any proper manner. Such a shutdown could very easily cause fatal accidents and the cause would be un-known due to all "looking" fine in any aftermath examination.

Now we add to the scene, your common average trucker with such a radio in his poccession and the ability to transmit high powered signals as one chosses. One example of such high power hijinks would be the specfic targeting of autos on the highway with a points / scoring system based on performance, price, make and if the car was built in the U.S. or not. What would be the outcome? To answer, it would be the shutdown of of the cars electronic logical systems causing other systems on-board to do likewise in successive order. How can this come about? Well the answer is quite clear, the high powered signal causes the logical centers to conflict or ignore basic operational commands from the microprocessor in turn causing the microprocessor to close down, then cause a halt to basic actions and the car stops running.

Other known occuring incidents that have had some humerous and fatal results have been reported in the past years by the press. Examples are:

1. As early as the mid-seventies, Volkswagen developed a computer controlled fuel injection valve control system. The car worked perfectly in Europe, but had some unexplained engine failures in the united states. The problem of engine failure was intermintent and very short lived when happening. The alleged cause of such failures were the transmission of Citizens Band radio frequencies from either mobile or base stations near by and causing an induced current sufficent to cause a malfuncition.

2. It was reported that some GM cars were having problems with the use of two meter radios and the electronic control systems. Other cars are reported to have some problems with cellular phones. Reports from England even indicate such problems occuring in a wide spectrum of autos in the area around Daventry due to RFI from the transmitter used by Radio Four, a commerical station transmitting on 1500 meters along with local AM and FM broadcasts. It seems that the station base was using a very high wattage transmitter and that when the transmitter was transmitting, the cars that passed close to the station would sometimes shutdown the engine causing minor overall problems and some angry motorists. If you look at this problem, you may see possible small scale urban electronic warfare possibilities. Two such areas might include the use of directed radio energy against late model autos by law enforcement or worse, by terroristic factions seeking to do the same thing. And one more example of such reports concern the sudden acceleration problems with some imported cars in the U.S. An interesting point to mention is that HONDA is offering owners of the 1988 Civic a replacement chip because of such reported problems.

3. On the lighter side of the problem, it was reported in the November 24th, 1987 edition of the Baltimore Sun, that some residents of Frederick, MD were having problems with the use of their electronic garage door openers. Owners of such devices returned them to places of purchase and found that the units worked perfectly. It was noted that nearby, the U.S. Army operates a major communications center for both domestic and international traffic. An Army spokesman stated that they are not radiating anything that should lock up the garage door recievers. It is also reported that when the Army turned off certain transmitters, the garage door openers would work again. While the Army stated that they were not the problem, the "problem" did disappear as stated by the Army. You be the judge on this!

On the fatal side of this problem, incidents were more deadly than funny. Although the cause of such incidents was all not due to an "Alligator" radio, but it was caused by the same type of over poowered raidiated radio emmissions. The cause was high wattage again and was to effect a new type of attack helicopter in use by 2 different U.S. armed services. The helicopter, known as the AH-64, Blackhawk or the naval version named Seahawk is considered, operational state of the art in low level air combat situations and is highly electronic in its basic make-up and operations. The problem was two fold in nature and both were to contribute in the final discovery.

The first cause was due to the need of the design to employ a unique horizontal stabilizer to help the helicopter improve it fly-ability.

The stabilizer was controlled through a series of electronically activated hydraulic systems run through a microprocessor that in turn was controlled from the cockpit through a series of other logical and electronic relay systems. There was no physical connection between the crafts flight controls and the pilot of the craft. What is meant, is that the fly by wire method was replaced by a set of relays and hydralic attenuators instead of cables and pulleys. It may not a been as smooth as the electronic flight, but it took an explosive charge to bring the control to a dead stick and at the same time could be fixed with a pair of wire cutters and clamps instead of a soldering iron and electronic parts.

The second problem, being more unknown and deadly, consisted of radio frequency interferance stemming from a number of different sources. One such source was found as a common citizens band radio with major illegal power output. Another incident of the same type of nature was discovered when one of the helicopters flew to close to a commerical radio stations transmissions towers. Both times the flight ended in fatalities for the crews. It was discovered that strong radio was the cause. According to published reports, 5 UH-60 Blackhawks have nosedived into the ground killing 22 serviceman since 1982. And the U.S. Army instructed it's pilots that flights near microwave antennas or shipboard radar may cause "uncommanded" altitude changes. In English, it translates to crashing into the ground at 600 miles per hour! So, this basic simple problem was not thought of as one that was possible even with the current concerns of systems management in the now fully electronicisied battlefield.

So, the first problem was that the controls of the craft are being directed by impulses instead of physical controls. The second was the use of un-protected electronics from both background and now, potential directed uses of radio frequency energy as weapons of warfare or even better, as stated before limited urban actions.

So now we take the approach of normal radio environment and place an active thought to possible options no available to a direct force. If reports of these natures are known to the general public, then what is to stop the directed force from becomming a new invisible tactic that can cause major disruptions of computer / communications systems currently in use.

Lets take the current state of electronic protective measure in force and used by the different defense agencies throughout the country. First off, we have the problem of large Electro-Magnetic Pulses, (EMP's) being able to disrupt command and communications links with the use of one nuclear device detoneated at a unknown range above the continential united states.

Another example comes from outside theoretical research concerning the SDI programs. One thought, from Thedore B. Taylor, a retired nuclear weapons designer and father of the largest yield fission bomb, the S.O.B., was quoted in an interview published in September, 1987. He stated that if you explode a one-kiloton device in space and directed the energy into a 3 centimeter beam of radiation, you could deposit enough energy to wipe out electronic and electrical equipment - computers, antennas, power lines, over an area larger that Washington, D.C. He was also quoted as saying that microwave weapons are more than likely being developed too.

Now weapons of this nature are on a very large scale and require vast amounts of energy too start with. But in a directed small beam aimed at normal general construction type buildings, a directed beam of energy cuts through walls, doors, and windows as if they were not even there. Your example is some of the local television or radio stations in your area. If you look at all or most of the stations, you might find a small shack atop of their building. It may contain the microwave dishes for the studio to transmitter links. The glass and wood are nothing to the in-comming or out-going signals. Brick walls mean nothing to a radio signal either. Just tune in your desk radio and listen to your favorite station.

So this pulse would be able to short out almost all commerical electrical, telecommunications, computer operations, and any other devices that contain transistors or semiconductors for a circuit path. These basic examples show what such types damage that these emmisions may pose.

The second part of this problem is with the protection of such circutry. Great amounts of technology protection comes in the form of deep trenches, standard and special grounding of buildings and equipment, cable and support runways, and concrete encasements. Now this is all wonderful and good from a military viewpoint where money is no object, but in the real world, the use of such protective measures is not possible even for the most prestigieous of corporations.

Now if such large pulses can destroy equipment on a global scale. Then the idea of using such forces becomes a better local tool for the destruction of security and measures taken to protect such devices and facilities from a physical standpoint.

Ok now we know that the possibility of directed energy may be used to disrupt the communications and operations of logical devices. There are numerous ways to use such technology to gather and alter electronic impulses. Another group of examples comes closer to the common man and is happening all to frequently to the owner / operators or mass communications systems. Best know, is the interruption of signals from a Home Box Office satellite and the insertion of a message that stated its subscripton rate was to high. That one incident struck fear in the hearts of the communications industry and showed that anything was fair game.

Other actions placed against commerical stations include the interception and signal override of 2 television stations in the Chicago area. One such action was placed against a Public Broadcasting station and the other was directed to one of the "Super Stations" in the same area. The first pirate transmission lasted 15 seconds and the second, two hours later, lasted 90 seconds. The Pirate, dressed in a Max Headroom facemask, uttered some statement, although garbled and during the second incident, bent over and exposed his / her rear and was struck on the behind with a fly swatter to the shock of the viewers. Of course the FBI and FCC were called in to investigate, but investigations of this sort led to nothing more than an empty trail.

Now to perform such deeds, one would have to contact either the station or the local office of the FCC to find out what the transmit and studio to transmitter frequencies are. (And this goes for any transmitter registered with the FCC. They will supply the name and location, frequency, and the maximum legal output of such sites.) There are two frequencies used for each television channel. One for the Audio and the other for the Video, or the other option, to listen or watch the station until it sign's off for the day (night). This one method does not lead to possible discovery and the frequencies are given at sign-on and sign-off. A good example of such frequencies is with a station located in Philadelphia, Pa. The station, WPVI, transmits its audio signal on commerical FM frequencies. The frequency is 87.8 Mhz. Now anyone with a good transmitter could add anything to the signal and no one would be the wiser until they did.

Examples of such transmitters and persons capable of doing this type of transmission is best described by the incident in the summer of 1987 concerning Radio New York. This radio station was considered a "pirate" station and the federal goverment decided to move in and shut them down. An interesting note to all of this, was that the station was located on a ship anchored off the coast of New York outside US boundarys. Still the US goverment with agents of the FBI, FCC, Customs and the Coast Guard boarded the vessel, closed down the station, arrested the persons on-board and the ship was taken in tow. End of that particular story.

On the other hand, two other stories of interest deal with the possible and real way some may be able to jam or possibly damage state of the art satellite communications. The first dealt with a group who call themselves the American Technocratic Association based in Wilmington, Delaware. This groups thought revolve around the scrambeling issue in use by the pay TV companies. The background of the members of this group claim to have a good working knowwledge of military radar communications systems. The group claims to have the capability to jam a satellite with a few mobile systems it has. One operation that the group hopes to undertake was called "Operation Sunspot". The group claims to have areas mapped out that have no treaty, regulation or statute dealing with the jamming of a geo-stationary satellite. The one problem with all of this is that such a thing could happen very easily. Now there are some who say that such things could not happen, but if one is to look in a number of magazines for such information on frequencies or locations, you could find it.

So you say to yourself that you want to try this experiment. Well we will not supply exact details of such techniques, but will say that HAM radio operators have the ability to contact both American and Soviet repeater satellites and if you wanted to you could do the same thing. Now for your basic uplink to such systems, you would need a transmit dish and the power behind the signal. So for a ten foot dish, you would need 91 watts, a six foot dish, 280 watts. It may not be dirt cheap to generate high powered signals in the mid range of 1-10 Ghz, but it does not present a great techincal obstacle and surplus gear is so easy to obtain.

You don't need large dishes with great amounts of power to do this. All that is needed is a moderate size dish, a few tens of watts at microwave frequencies, and Bingo! You've got an effective satellite jamming station! And then you have to address the issue of the telemetry channel. THey may not be able to overtake the signal, but if jam the signal with another, it may be possible to affect the operation, stability or orbit of the target. Frequencies for such channels are available from a number of sources and for as little as $2.50 per frequency.

Now these examples and the reported stories dealing with television stations interuption's are fast becomming one of the most feared aspect of open air transmissions. Such transmitter frequencies are no longer the domain of commerical radio and television stations. Transmissions on any frequency are just a phone call away from suppliers who provide common or business radio transmission technology.

So if satellite and television stations can be interupted by such forces, six million dollar helicopters are taken down because of CB radios, and automobiles cease to operate due to a wide spectrum of emmited signals, then the possibility to intercept and harvest vast amounts of knowledge is available to those who wish to gather such.

Now to explain such basic interceptions are now commonplace with horrific results to those who do not believe that such things can happen. For a simplistic view of such emmited signals, take a standard "Walkman" type of radio and visit one of the many locations of ATM's or better known as "money machines". (This excerise may also be performed near any standard personal computer if such machines are not available.) and tune through the FM band. With careful tuning, one will be able to "hear" machine funcitions occuring. Taking basic simple electronics, one may have the ability to recieve and reconstruct such impulses to a readable form.

Or an example of larger scale and better know, would be with the use of back-yard home satellite dishes. Dishes range from 6 to 12 feet wide. Signals available include music, sports, news, movies, stock and commodity trading quotes, weather, education and other such information services. In addition to these services, a number of different multi-site conference services are available from a host of major hotel chains as well as privatly organized meetings held for specfic time periods and dates.

All may be tuned through the use of a dish and sensitive information that may not be available to someone, is then made available and no one is the wiser! Transponders are not private, and are rented out for only the time used. And one other thing that might bring you to your senses about such signals, is that the signals are transmitted by the satellite over a wide area to anyone who can recieve such signals.

One other development is the small Micro-Sat by Norsat. This complete system offers both satellite bands coverage, Ku and C, a small dish and circuit board that fits inside an IBM PC. The unit downblocks 950 Mhz to 1.45 Ghz, offers a maximum baud rate of 9600 bps, frequency, bandwidth, video and audio selectable formats and may be connected to the VideoCipher II, B-Mac and Oak Orion descrambling systems.

Some other such signal reconstruction devices are now also available through the mails. One such device is available in plan form from Don Britton Enterprises and is called the Re-Process Sync Amplifier. The device was developed to recieve signals emmanated from cable television systems. What the device does in essance, is to take a signal that "leaks" from cable tv systems and recieves such, adds a sync signal needed by the television set to display the recieved signals and then sends the signal to the antenna input of the set so that display may happen. Now if weak signal reception is available from leaking cable systems, then the ability to recieve weak signals from logical devices is also possible.

Interception and Weapons Possibilities

Think about possible interception points pertaining to logical security methods. Communications may be encrypted, data may be stored in an in-active form and access is only a matter of time while the interceptee is waiting for the dispersal. The next security concerned area covered would be for the encryption of the information in its stored and transmitted form. The encryption is all wonderful and good for the transmission and storage, but does nothing for the information as it is in its final stage to the human eyes! And you only have two ways to get it to the eyes, in hard copy or by a video screen.

Now you think that interception is not possible since the information is encrypted, but the data must be decrypted so that the human connection may use the information. The human connection allows for the reception of said information by the afore mentioned devices and lets interception to happen through the clear or decryption points of the attacked devices.

And one other point to mention; other possible effects of reception / transmission to security in general, could affect other controls ranging from building energy management to security access and monitoring controls.

To give a better understanding of such equipment, we will discuss some of the devices known. One such device known as the Van Eck device and the other is called the Re-Process Sync Amplifier. Some may feel that there are two different systems involved in this discussion, but the author finds no major difference between the two, with the exception of the Van Eck device is built for operation on European voltages and has a built-in digital frequency meter. The one major difference found is with the dates of copyrights for the two devices. The Don Britton device is dated 1979, while the Van Eck unit is dated October,1985.

Note: Another unit, with plans for such devices, are available from Consumertronics, located in Alamorgordo, New Mexico. Besides the plans for a Van Eck type reader, one book offers information in reference to computer crime and countermeasures, how systems are penetrated, BBS advice, Password defeats, TEMPEST, crosstalk amplifiers and a 200 word phreaking terms glossary. All for only $15.00

We will begin with a basic understanding of the inner workings of the device. The one other major basic difference with the two reader boxes is that the Van Eck box is designed for use with tv's and VDT's used in Europe as compared with the Britton box built for use in the United States. This device in general, is designed to restore and regenerate the sync and colorburst signals and ignores all information appearing during either the vertical or horizontal blanking. Its basic result is reconfigure through the use of supplying artifical external signals inputed directly to any video monitor through a simple 10-50 dollar modification of the TV or video monitor, or in simple english, takes a weak video signal and tries to shape or match it and then boost its output to a normal television screen.

One other interesting thought comes to mind with the use of video tape copy protection methods. Since these methods use a means that makes it tough on the VCR not the TV from generating signals for tape duplication, there have been a number of devices that assist in the restoring and re-structure of the picture and sound. One device is known as the "Line Zapper". The device helps to adjust the brightness changes, vertical jumping and jittering, and video noise. It is available in kit or complete form. Pricing starts at $69.95 and complete tested units cost $124 95. Now if this unit can assist in the filtering and structuring of commerically induced weak signals, then it should be able to take a boosted signal presented to it and clean the picture to something of useable form. Some may see this only as a filter for video processing with a focal point on the actual copy-guard techniques, but such a device incorporated into the Van Eck type of gear should assist in the overall signal restructuring.

Now one other interesting point about possible video signaling re-construction methods was addressed in a multi-part series published in Radio-Electronics based on the methodology used for the construction of video signals scrambeled by different vendors of cable and over-the air pay television. The series dealt with all aspects and methods of video and audio, (complete with discussions on the DES methods used for the VideoCipher units and the like,) used in commerical systems in use.

One other thought comes to mind of an experimental nature. Since the screen of a computer is not always changing and for the most part stable in its display, why not take the recieved signal and digitize it! You could filter out signal noise clean up any true video signal present. This is no great techno-wonder, the basic gear could be put together with Radio Shack or the like types of equipment. And the cost is still most reasonable. If not available there, costs for home-brew gear would not be that high. The simple electronics blocks would consist of comparators, video detectors, data seperator gates, a to d - d to a converters, data amp and a signal level converter.

Or the better version, might be a modified slow scan television system with error correction and clean-up circuits. Such units work over normal phone lines or standard radio channels and since the units can take signals from these two different types of inputs, there should be no problem in adapting the unit to accept a cleaned up analog signal from a digitizer.

Away from the world of the experimental thoughts, we return to the point at hand....

Now there are two types of monitors used today. The first, called composite and the second using TTL logic to control the screen and its pattern. The composite screen is nothing more than a television set or Apple computer type of monitor. The construction of the picture is performed by a beam of electrons that are scanned across the screen at a rate of 525 lines per second. Since the majority of screens are of a composite nature (this is even true in most IBM environments) the ability to recieve the signal is very possible from a radio emmission standpoint.

The reception of such signals is not fairytales, but comes with reality attached through the use of simple electronics. The first part of the reception project is to have a method of signal acaquisition and amplifcation. Such gathering may be performed by the use of standard electronics store technology. For this example, we will use common Radio Shack electronics. The reason is due too the common variety electronics that are available to most persons needing such science to accomplish the required gathering.

To start, since a base station is out of the question due to the weak signals one would have to recieve. So the need for transportable equipment is a must. Antenna, amplifier, sync process unit and display medium must be powered in the transit unit. Depending on budget and (BEL) (Basic Equipment List) requierments a fully battery operated set-up can be constructured for under .....

Our two systems described here will be different only in basic construction and budgetary BEL's.

The "Radio Shack" Reader

1. The antenna could consist of a Radio Shack TV/FM # 15-1611 for 49.95

2. If needed, Radio Shack in-line signal amplifier 10 db gain # 15-1117 for 15.95

3. Radio Shack RF Video Modulator # 15-1273 for 26.95

4. The Britton or Van Eck unit (Cost unknown due to construction needs)

5. The tuning unit may consist different available FM,TV,UHF tuners available for the tuning of TV Sound & Picture reception and possible recording. Costs for such units range from 319.95 to 119.95 The 319.95 unit can operate on AC / DC, has audio / video input jacks and can operate on 9 "D" batteries. Other possible useable units would be # either # 16-109 or 16-111. The units cost 219.95 and the other 159.95 Both are able to tune in the full commerical AM / FM and VHF/UHF Television signals, The low end of the cost spectrum would be the RS # 16-113 at 119.95 This unit also has the same spectrum tuning abilities.

The Gold Plated Unit

1. The antenna could consist of a Radio Shack TV/FM # 15-1611 for 49.95 (Or due to the use of better reception electronics having built in antennas. But due to the need for amplified signals being inputed to the reciever we will still possibly use the RS amplified antennas.)
   a. It is also possible to use any number of amature radio antennas. For the purpose of maintaining a low profile, we will use one of the standard active recieving antennas that has a spectrum of reception from 50Mhz to 1 Ghz. Such units are available from mail order supply houses.

2. If still needed, Radio Shack in-line signal amplifier 10 db gain # 15-1117 for 15.95 It is also possible to use # 15-1105 Indoor FM Signal Booster with switchable 0,10 or 20 Db gain at a cost of 24.95.

3. Radio Shack RF Video Modulator # 15-1273 for 26.95

4. The Britton or Van Eck unit (Cost unknown due to construction needs)

5. Tuning units- The tuning units would consist of 2 seperate radio units. The units, both ICOM's have a combined tuning range of 100 Khz to 2 Ghz.

a. Unit 1 (R-71a) tunes from 100 Khz to 30 Mhz. This unit is nothing more than a shortwave reciever with excellent signal reception and frequency stability that offers far better overall signal interception quality. The unit offers 1 Hz tuning and has digital frequency readout. As an option, this unit may be controlled by an IBM or compatable PC. Cost for this unit is $949.00

b. Unit 2 (R7000) covers 30 Mhz to 2 Ghz. This unit is a general coverage reciever with excellent signal reception and frequency stability that offers far better overall signal tuning and interception quality.

Also this unit can be computer controlled through an IBM or compatiable. The unit offers .01 Hz tuning and has digital frequency readout. Additional abilities of the unit include signal output and a IF output of 10.7 Mhz with other frequencies available. The cost for the unit is $1099.99. This particular unit also has an option for the output of the video signal and connection of any standard video monitor for 130 dollars. For an additional 160 dollars the unit can have the ability to recieve signals from 20 Khz and go all the way to the specified 2 Ghz. The unit needed is called a Kuranishi FC-7000 frequency converter. With additional commerical television MDS tuning equipment, ranges can exceed 2.7 Ghz. Costs for this will range between 79 and 109 dollars. Since we will be mostly dealing in the lower ranges of frequencies, an added piece of gear may be used to gain the best signal reception points available. This is through the use a Radio Direction Finder available from American Electronics for 100 dollars.

Now with all this equipment for both systems, another basic system with minumum cost is readilly available to many for under 100.00 dollars. This we speak,of is the common Black & White Television set available in mass quanties from any number of sources. It has been reported that such interception capabilities are possible and have occured without the interceptee knowing until the Communications Commission have contacted the source of the emmited signals.

For example, some personal computers and their respective screen have been known to been picked up on the TV screens of their neighbors and through nothing more than rough or fine tuning the reception. The reason is due to the TV having the ability to automatically adjust the Sync signals to those close to the frequency of intercepted computer screens sync frequency. This "ability" is available through the use of a common manual type tuner on a standard Black & White set with a normal directional antenna and an standard antenna amplifier. All three devices in common life and attached to your own television recievers!

You have such devices if you have an antenna on your roof or attached to your set. Most have attached signal amplification due to the ever growing background noise generated by normal commerical stations and reception charictersistic In simple term, the guy next door can read your screen and you don't know it. Now take the number of personal type computers in a standard corporate environment, caulculate the possible dollar figures of the combined information contained in these machines, and substantial sums become more evident than ever before. If business plans, formulas or patent-trade information, client lists, or any other type of valuable information and since that information will be called up at any time or current work performed is wanted in the surveillance gathering operation and then you have a completely wide open way of monitoring the daily practices and transactional actions with complete impunity and securty of such areas is completely unguarded due to the lack of knowledge

For experimental purposes, we will use very simplistic computer systems to give an idea of what may be possible. The equipment shall be basic, over the counter, cheap, electronic systems to gather and produce the signals we which to collect.

The equipment list is as follows:

1. Franklin Ace 1200 (Apple II compatiable)

   a. Franklin Ace Serial / Paralell Card
      (Paralell card is in use for the 2 printers)

   b. Apple Super Serial Card (RS-232) for use with the communications modem

2. Franklin Video Monitor (40 or 80 characters display) 18 Mhz

   (Standard IBM monitors radiate at 15 to 16 Mhz)

3. Prometheus ProModem 1200 (External type)

4. Printers

   a. Okidata Microline 92

   b. Epson MX-80

Our basic reception / interception equipment consists of:

1. Bearcat 250 (50 Channel) Scanner

   (Coverage from 32-50,146-148,148-174,420-450,450-470,470-512 Mhz)

2. Soundesign FM Stereo Tuner (86.5 Mhz to 109.5 Mhz)

3. Electrobrand AM-FM-SW-CB-TV-PB-AIR-Weather

   The AM and FM are standard commerical band recievers.

   SW is short-wave from 4 Mhz to 12 Mhz

   TV coverage is from audio channels 2 through 13

   AIR band from 108 through 135 Mhz

   Public Band is 145 through 175 Mhz

4. A Gould OS 1100 A Osocilliscope 25 Mhz range

Since we will not try to re-construct the actual video signal generated, as this has already been done, we will not have to explain what we recieve as a picture. What we will cover is the gross signal output of standard population computerized logical systems.

In our observations, we have seen a wide spectrum of emmitted signals with a strong signal between 9.0 and 9.250 Mhz for the display of standard text scrolling by. Better signal display was found at the lower frequencies of 9 Mhz. Monitor frequencies were found in the area of 11 through 19.5 - 20 Mhz. Printer frequencies are in the range of 140 to 200 Mhz. Disk operations were detected in the ranges of 88 to 250 Mhz. Overall frequency generation was from 4 through 500 Mhz. The modem was found between 28 and 300 Mhz. All in all, this easy discovery of radiated or transmitted signals by means of common radio technology could lead to.

An interesting thought comes up with the use of some common ham transcievers for such operations, and with simple, easy modifications, some can transmit on all frequencies from 1.6 t 30 Mhz. Such a transmitter would be the Kenwood 440. This transciever offers 100 watt output and as stated all frequency transmit. To perform the small modification, all one would have to do is cut one lead to a diode (Diode D 80) and as an added bonus for better frequency readout, you gain an additional readout of 10 Hz by snipping the lead to Diode 66. So the unit covers the range of IBM PC frequencys in use and all of the Apple systems too. Thats says it all! It can offer the possibility for disruption of internal signals used to process information and the possibility of causing other logic related systems to act or not without reason.

For example, would it be possible for the Soviets to sit under cover with a modified Kenwood 440 100 watt radio or better yet, a Radio Shack 40 channel AM / SSB and a 100 watt Firebird linear amplifier and a simple small antenna to disperse the signal. So the problem of the 6 million dollar helicopter comes down to a wholesale cost of 150.00 (190.00 to 200.00 for an average rip-stop nylon camping backpack unit) per man with a recommended dispersal of 3 manpacks per unit into the theater. Suspected effective ranging up to 3 miles per man pack unit is suggested.

Or even better, if such things were possible against military aircraft or normal commerical real world autos, then directed intent should be of now problem against civilian targets such as computer installations, bank and operations support structures, possible override of security systems and any other systems that may be affected by such forces.

Other uses of directed energy may be used in law enforcement situations for the apperhension of suspected persons in late model automobiles. If the truckers are using the radios for game playing, then why can't the police have the same type of device for the stopping of autos? There are a number of devices that will radiate such energies over the spectrum. One such device would be the Radar Speed Gun Calibrator (or better know as a radar jammer) for use with calibration of speed guns or for the deceiving of police radar units. The plans for such units were (are) available for a number of sources. One such source, is Philips Instrument Company or another such source was the Radio-Electronics issue in the spring or summer of 1987 with plans for the Radar Speed Gun Calibrator, that would allow you to transmit a signal that would equal the same type of reflected signal from an automobile traveling at the supposed testing

Some plans or kits come with instructions for the combination of radar jammer units with most commonly available auto radar detector units. In simple terms, the radar detector unit detects a signal and through its display or attention getting circuitry in turn activates the radar jamming equipment to deceive or jam the police transmitter / reciever units. Best know of such combinations, were the use of Escort radar detectors and jammer units with transmission horns mounted behind the front grill of autos. No ifs, ands, or buts, they work!

One other piece of equipment that may have devastating effects on overall security and support systems, deals with the generation of very high energy pulses that might be classified as being able to generate EMP's that could damage almost any piece of electronic gear. The claim from the designer is that this device can generate a pulse with an effective range of multi-millions of watts. The device on average will produce a pulse equal to 400,00 wats in a testing mode with the multi-million outputs available with full charging of the capacitor banks peaked. Also stated in this book is the ability of the unit to produce a very large inductance in near by electronic gear. Most interesting! And the only statement in this book about the device and it's short comming, has to deal with the in-ability of the device to produce sufficent output used in certain nuclear experiments. I wonder what that means?

So, in closing, the capability of these units is well within the range of any person with the intent comes closer to home than ever before. The equipment is nothing of major technical wonderment, just a few simple block circuits put together to each other so that they work together to do the final requested product. And all of the described gear or plans may be in the hands of everyday persons even if they don't know it! And while most do not have such knowledge about how such systems may be used to corrupt other systems, or even how the average telephone or toaster may work, they will still state that such described technology is not possible, and open the door to major disaster due to complete ignorance to the problem. In closing, to steal a phrase from someone else, "The truth shall set you free (or may keep you from being over exposed from free form energy)!

"Click!" And the last words spoken by the corporate DP offical were...

" Thats impossible! You could never do that to my operation!

Ahem, Sure sir, Sure!