

frm 'the threat of information theft by reception of electromagnetic radiation from rs-232 cables.' computers and security, 9(1990) 53-58 (factors effecting reception are grounding/coupling, data rate (baud), and cable length.) I am not entering any of the math, and alot of the tech stuff - If you want to do this get ahold of the paper.

...experiments showed that RS-232 data signals can be intercepted several meters away from a target system, even when a shielded data cable is used. This can be done w/ the aid of a very compact commercially available and therefore cheap gear such as a walkman provided w/ a recording facility and some minor modifications. This means that although the seperation distance at which interception is possible is limited to several meters, in many cases eavesdropping can be done without attracting attention. On the other hand, when more sophisticated equipment is used such as a communications receiver in combination w/ a directional antenna, eavesdropping might be difficult close to the target system...however larger and therefore quite safe seperation distances may be feasible.

(I get the impression that one needs to place the receiver a specific distance frm the cable, mutch akin to having 2 receivers tuned to the same frequency a set distance apart that is a factor of the wavelength of the tuned to frequency and being able to send morse by tapping on the speakers - frequency entrainment, But i'm not shure about this.)

...When an RS-232 interface cable is connection is part of the equip configuration, then there are many factors acting in favor of the eavesdropper, the most important being the following:

>the bit amplitude of an RS-232 data signal is relatively large compaired w/ the levels of the logic signals used in the inner circuities of the equipment.

>the rise and fall times of the data signal are very short. Consequently they correspond to high frequency components resulting in considerable radiation.

>the RS-232 interface connection is unballanced with respect to the earth. This inhearent unballance will contribute to a high level of radiation.

>in many cases, the RS-232 cables are not shielded, or the shielding is not adequetly connected to to the equipment, so that those cables behave like unshielded cables.

>inner walls (without metal grids) do not effect radiation levels signifficantly at frequencies of interest (below 200MHz).

>the data are serially transported along the RS-232 cable, which makes it easy to recognise the individual bits. Usually the data are coded in well known character sets (like ASCII). This makes it very easy to to decode the reconstructed bits.

>the data are often structured by the legal user, therefore they are

TEMPEST.TXT

easily interpreted.

>the data signal is transmittted at bit rates which are low (300, 600, 1200 bits) compaired with the nyquist rate corresponding to the bandwidth of a standard radio receiver (AM = 5 kHz, FM = 75 kHz). Therefore. in principle, the data signal can be detected even w/ the help of a standard pocket radio receiver. At the same time the data can be recorded on a tape w/ the help of an ordinary cassette recorder.

...a simplification is the absence of the coupling between the two resulting signal conductors. For the most commonly used RS-232 cables this ommision makes makes no significant difference to the field strength calculation. further we have assumed that the transmitter is grounded and the receiver is not. "Grounded" means that the galvanic connection to the reference groundplane exists. this is often the case in practice. When no groundplane exists, there will be a certain amount of parasitic capacity between equipment and groundplane (in the case of desktop equip. typically 100 pF)...

(2 experiments using a pocket radio receiver @ 7meter's picked up the signal at 16 MHz (short wave band), and 98 MHz.(in the FM band at harmonics of the system clock))...a standard AM/FM radio receiver equiped w/ a whip antinna 1m long. A hard limiter circuit was used to reconstruct the detected data...

...only at one site was shielding effectivness signifficant. Radio signals could be detected at a distance in all cases, virtually correlating w/ the the orriginal data stream. however at 3 sites the data could not be reconstructed w/ just the aid of a simple level detector (he doesn't say what was used to reconstruct the signals beyond a level detector). At the remaining sites, the data could be reconsructed w/ level detection at distances of 6-9m A PC-modem connection could be be intercepted in the bedroom of an adjacent house...

(data received @ 98 MHz will be too week to to be heard through the the speaker, must use a simple level detector.(pre-amp/filter?), it seems like proccessing is going to be the biggest pain in getting one of these systems up, it being highly desirable to condition the signal so that it can be fed into a computer and storred on disk.

Downloaded From P-80 Systems 304-744-2253