The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables

Peter Smulders

Eindhoven University of Technology, Department of Electrical Engineering, Eindhoven, The Netherlands

Electromagnetic radiation arising from RS-232 cables may contain information which is related to the original RS-232 data signals. The seriousness of eavesdropping risks is shown by estimates of bit error rates feasible with a standard radio receiver as a function of the separation distance. In addition to this, results of experimental eavesdropping are presented.

Keywords: RS-232 cable, Electromagnetic radiation, Eavesdropping risks.

Caution: Failure to detect intelligible emanations by the methods described in this paper do not mean an installation is secure against interception by sophisticated and resourceful opponents.

1. Introduction

It is a well-known fact that electronic equipment emits unwanted electromagnetic radiation, which can disturb radio reception in the vicinity of the equipment. Until recently it was less generally realized that radiation arising from data processing equipment may contain private information which may be interceptable by an interested party.

Research into the possibility of picking up the electromagnetic radiation originating from video display units (VDUs) made clear that this type of information theft can be committed very easily [1]. It is not only this type of equipment which is vulnerable to interception at a distance; experiments on eavesdropping RS-232 cable signals prove that it is possible in some cases to intercept data signals running along an RS-232 cable, by picking up and decoding the electromagnetic radiation produced by the cable. This report gives the results of these experiments and research into the underlying mechanisms. These results show, that compared with the VDU case, RS-232 eavesdropping has significantly different consequences with regard to information security.

When an RS-232 interface cable connection [2, 3] forms part of the equipment configuration, then there are many factors acting in favor of the eavesdropper; the most important being the following:

0167-4048/90/$3.50 ~ 1990, Elsevier Science Publishers Ltd.

• The bit amplitude of an RS-232 data signal is relatively large compared with the levels of the logic signals used in the inner circuits 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 unbalanced with respect to earth. This inherent unbalance will contribute to a high level of radiation.

• In many cases, the RS-232 cables are not shielded, or the shield is not adequately connected to the equipment, so that those cables behave like unshielded cables.

• Inner walls (without metal grids) do not affect radiation levels significantly at frequencies of interest (below 200 MHz).

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

• The data are often structured by the legal user; therefore they are easily interpreted.

• The data signal is transmitted at bit rates which are low (300, 600, 1200 bits^{-1}) compared 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 with the help of a standard pocket radio receiver. At the same time the data can be recorded on tape with the help of an ordinary cassette recorder.

In addition to these risk factors, there is an important reason for looking into the interception of RS-232 data; it may contain very sensitive information such as passwords, user codes and financial transactions.

This paper gives an analysis of the bit error rate of intercepted data, feasible with a radio receiver, as a function of the separation distance. The analysis is based on a model of a simple communication system that consists of a transmitter, sending RS-232 data along an unshielded cable to a receiver. In addition to this, results of experimental eavcsdropping are presented.

2. Mechanisms

A possible mechanism by which information bearing emanation may occur is an unintended conversion of the transmitted (differential mode) signal V_t into a common mode current I_{cm}. This current forms, together with the circumferencing area, a magnetic dipole which radiates in the uncontrolled environment. This mechanism is shown in Fig. 1.

In this figure, a communication system (i.e. a terminal-terminal or a PC-modem connection) is represented by two boxes (transmitter and receiver) and an interconnecting RS-232 cable. The cable conductors associated with the signaling have been omitted. A second simplification is the absence of the coupling between the two resulting signal conductors. For the most commonly used RS-232 cables this omission makes no significant difference to the field strength calculation presented below. Furthermore, we have assumed that the transmitter is grounded and the receiver is not. "Grounded"

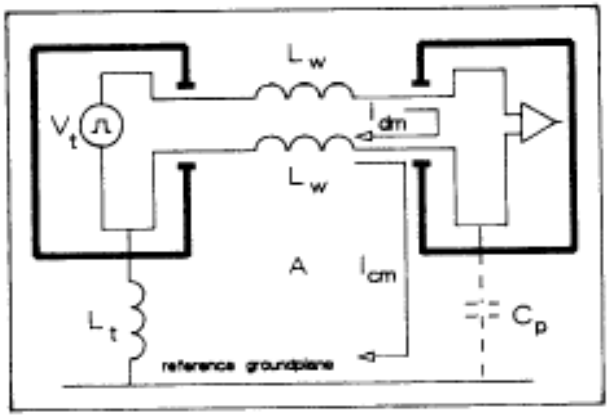

Fig. 1. Two-box representation of a communication system.

means, that a galvanic connection to the reference groundplane exists. This is often the case in practice.

When no ground connection exists, there will be a certain amount of parasitic capacity (C_p) between equipment and groundplane (in the case of table top equipment typically 100 pF). In practice, the inductance of a conductor is not zero but about 1 μH m^{-1}; therefore the differential mode current I_{dm}, will flow partly through L_w and partly through C_p and the reference plane. The latter part (I_{cm}) circumferences an area A. We assume that the wave lengths λ of the frequency components of interest in V_t are large compared with the dimensions of the system configuration. In that case it is permitted to base our calculations of the currents which act as sources of radiation on network theory. In addition the radiating source can be considered as a magnetic dipole consisting of I_{cm} circumferencing area A. This radiator will cause an electric field in the free halfspace above the conducting earth plane with a spectrum according to

$$E = 2.6 \times 10^{-14} \frac{I_{cm}(f) A f^2}{r} \text{ for } r > \frac{\lambda}{2\pi}$$

where r is the separation distance in the direction of maximum radiated power. The bit information of V_t appears in the radiation via I_{cm}. The maximum value of $I_{cm}(f)$ appears at the resonance frequency

$$f_r = \frac{1}{2\pi\{(L_t + L_w) C_p\}^{1/2}}$$

It appears from network theory that for $f \approx f_r$ the relationship between I_{cm} and V_t is approximated by

$$I_{cm} \approx \frac{V_t}{2\pi f L_t - (1/2\pi f C_p)}$$

It should be noted that I_{cm} is independent of the source impedance of the transmitter and the load impedance of the receiver.

The transmitted signal V_t consists of trapezoidal bit pulses. Assuming a quasi random sequence of bit pulses, the amplitude intensity spectrum can be written as

$$V_t(f) = 2U\tau \frac{\sin(\pi f \tau)}{\pi f \tau} \frac{\sin(\pi f \tau_s)}{\pi f \tau_s}$$

where U represents the bit amplitude with a typical value of 15 V, τ_s represents the rise/fall time being typically 0.8 ps and τ represents the bit time. This spectrum consists of neighboring lobes. Each lobe takes up a bandwidth of l/τ Hz which equals the bit rate r_b It appears from the first Nyquist theorem that each lobe contains all bit information.

To calculate the bit error rate P_e of the intercepted data we assume that the bandwidth of the intercepting radio receiver equals n times the span of one lobe. In addition, we assume that the receiver filter characteristic matches the shape of the received lobe within this span In that ease we may use the following well-known expression for P_e [4]

$$P_e = Q\left(\frac{\gamma}{2}\right)$$

where Q is the gaussian probability function. If the receiver is tuned at the resonance frequency f_r we can write

$$\gamma^2 = \frac{2}{\eta} \int_{f_r - n/2\tau}^{f_r + n/2\tau} |E|^2 \, df$$

η is the power spectral density which is assumed to be additive white gaussian noise of value 3 x 10^{-15} W Hz^{-1} which complies with the electromagnetic ambient noise in urban areas at the frequencies of interest [5].

As an example we suppose the bit rate r_b to be 1200 bits s^{-1} and $\eta = 4$; in that case, the total bandwidth roughly equals the bandwidth of a standard AM radio receiver Additionally, the mains connection of the transmitting equipment is assumed to be 2 m long. In Fig. 2, the bit error rate of the intercepted data signal is shown for the typical values of the signal and system parameters.

The two curves correspond to 5 and 10 m lengths of the RS-232 cable. We see that in the case of $A = 10$ m^2 the original data stream is interceptable very well at a separation distance of 7 m. This conclusion holds also for the situation where both transmitter and receiver are "floating" (i.e. they have no galvanic connection to the reference). On the other hand, if both terminals are "grounded" no significant resonances will appear, and the radiation level seems to be safe at all frequencies for typical values of the source impedance of V_t and the load impedance of the receiver (5 kΩ). However, for values that deviate (for instance much lower values of source and load impedance), the radiation may reach an intolerable level too.

It has to be emphasized that these conclusions have been based on a theoretical model of a typical equipment configuration only. As such they are not suitable for the evaluation of individual configurations as installed in practice, because in practice the system parameter values may differ significantly among different systems and because *Pc* is very sensitive to these parameter variations. The main reason for this analysis is to demonstrate the potential danger of RS-232 eavesdropping in general.

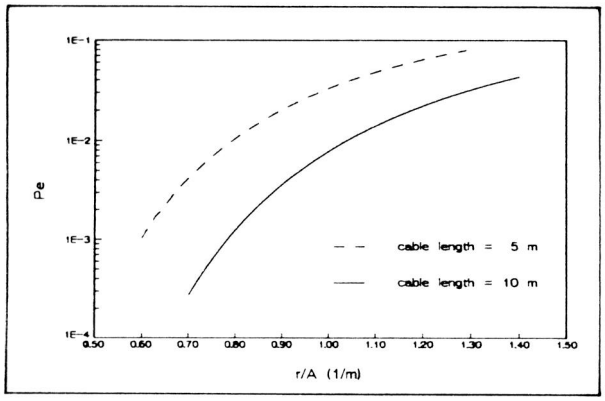

Fig. 2. The bit error rate of intercepted data.

3. Experiments on Eavesdropping

A test configuration consisting of two ASCII terminals communicating via an unshielded and twisted RS-232 cable of 3 m length was considered. Both terminals were placed on a table at 3 m apart and connected via a 2 m mains connection to the net. The transmitting terminal sent a sequence of subsequent ASCII characters "d" in "REPEATMODE".

Figure 3 shows the original signal that was transmitted and the signal detected 7 m away with a pocket radio receiver tuned to 16 MHz (short wave band).

We can clearly recognize the original data in the signal that was detected. Although the signs of the transitions have been lost by the AM envelope detection process it is clear that an eavesdropper will be able to reconstruct the received signal.

In addition to reception in the short wave band, it was possible to detect the transmitted ASCII characters in the FM band at harmonics of the system clock signal. The presence of these modul-

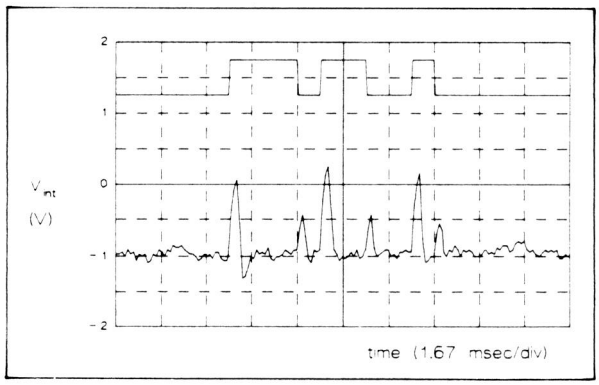

Fig. 3. Original and intercepted data signal at a distance of 7 m and at 1 6 MHz (short wave band)

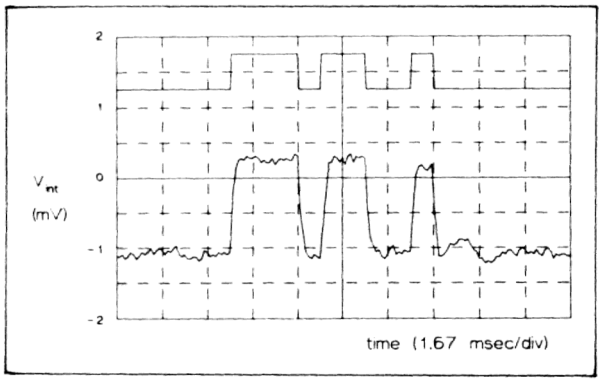

Fig. 4. Original and intercepted data signal at 7 m and 98 MHz (FM band).

ations of the data signal in the radiation cannot be understood by the previously described mechanisms. Because modulation is a non-linear process it appears from this phenomenon that this kind of information-bearing radiation arises from unintentional modulation of the clock signal by the RS232 signal owing to non-linear elements in the inner circuitry of the equipment and electromagnetic coupling of the modulated signal to the external cable. It is not feasible to evaluate the amplitude levels of these undesirable components by calculating every internal coupling. Therefore we must restrict ourselves to the pragmatic approach.

In Fig. 4, the intercepted signal received at 98 MHz is shown together with the original data signal. Again, the separation was 7 m. Although this signal will be too weak to be heard through the loudspeaker, it can be reconstructed easily by means of a simple level detector.

Further experiments were carried out to find out if the phenomena as described in this paper were just incidental, or whether other equipment operating in different configurations on different sites would radiate information in the same way. Seven different sites were examined; the maximum separation distance was assessed for a bit error rate of approximately 0.01 with the help of a standard AM/FM radio receiver equipped with a simple whip antenna 1 m long. A hard-limiter circuit was used to reconstruct the detected data. On each site, two situations were examined; in one case an unshielded RS232 cable was installed, and in the other case, a shielded cable. The results are shown in Table 1.

Only at one site was the shielding effectiveness significant. Radio signals could be detected at a distance in all cases, visually correlating with the original data stream. However, at three sites the data could not be reconstructed with just the aid of a simple level detector. At the remaining sites, the data could be reconstructed with level detection at distances varying from 6 to 9 m. A PC-modem connection placed in a living room could be intercepted in the bedroom of an adjacent house!

TABLE 1 Results of eavesdropping experiments at different sites

Configuration	*Environment*	*Separation distance* (m) *for* $P_e \approx 0.01$		*Frequency* (MHz)
		Unshielded	*Shielded*	
Terminal-terminal	Laboratory	8	7	121
Terminal-terminal	Laboratory	7	1	132
Terminal-modem	Laboratory	–	–	12
PC-modem	Office	7	6	15
Terminal-printer	Office	–	–	18
PC-modem	Home	9	7	12
PC-modem	Home	–	–	100

4. Conclusions

Data signals transmitted along an RS-232 cable connection may be vulnerable to interception at a distance. Eavesdropping 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 kind of eavesdropping can be done with the aid of very compact commercially available and therefore relatively cheap gear such as a Walkman provided with a recording facility and-some minor modifications. This means that although the separation distance at which interception is possible is limited to several meters, in many circumstances eavesdropping can be done without attracting attention. On the other hand, when more sophisticated equipment is used such as a communication receiver in combination with a directional antenna, eavesdropping might be difficult close to the target system because of its large physical dimensions; however, larger and therefore quite safe separation distances may be feasible.

Epilogue

As stated in the introduction of this paper, interception of RS-232 data signals has consequences with respect to information security which differ significantly from those of VDU eavesdropping; the distance at which interception of RS-232 data signals is possible is limited to several meters while in the VDU case separation distances may be much larger. On the other hand, the receiver and recording equipment necessary for intercepting RS-232 data signals are very small, simple and cheap compared with the equipment needed for the interception of video signals. Besides that there is another very significant difference; in the VDU case the intercepted information is limited to the information appearing on the originating VDU screen. As a security measure this video display information seldom contains passwords; passwords are normally entered in "echo-off" mode. Although passwords do not appear on the screen, they are (of course) always transmitted along the RS-2 32 cable. Because of this fact and the risk factors mentioned in the introduction, we have to take special account of the RS-232 eavesdropping possibilities in vulnerability studies.

Peter Smulders was born in Eindhoven, The Netherlands, in 1957. He graduated from Eindhoven University of Technology in 1985. In September 1985 he joined the Propagation and Electromagnetic Compatibility Department of the Research Neher Laboratories of the Netherlands PTT.
Since June 1988 he has been with the Telecommunications Division of Endhovcn University of Technology.
His current interests deal with EMC and compromising emanation from civil data processing equipment. In addition, he is doing research in the field of broadband in house radio networks.

Mr. Smulders is a member of IEEE and co-founder and present board member of the James Clark Maxwell Foundation.

Acknowledgment

I would like to thank Professor G. Brussaard and Dr. M. H. A. J. Herben for their valuable suggestions and comments. These contributions have considerably enhanced the clarity of this paper.

References

[1] W. van Eck, Electromagnetic radiations from video display units: an eavesdropping risk?, *Comput.. Secur.., 4 (1985*).

2] CCITT recommendation V.24 (equivalent to RS-232C from EIA), List of definitions for interchange circuits between data terminal equipment and circuit terminating equipment, Geneva, 1980.

[3] CCITT recommendation V28, Electrical characteristics for unbalanced double-current interchange circuits, Geneva, 980.

4] *K. Shanmugam, Digital and Analog Communication, Systems,* Wiley, New York, 1985, p. 389.

5] O. White, EMI Control Methodology and Procedures. Don White Consultants, Gainesville, GA, 1982, p. 2.39.