Soft Tempest – An Opportunity for NATO

Ross J. Anderson and Markus G. Kuhn

University of Cambridge, Computer Laboratory,
New Museums Site, Pembroke Street,
Cambridge CB2 3QG, United Kingdom
{rja14,mgk25}@cl.cam.ac.uk

Abstract

NATO countries spend billions of dollars a year on electromagnetic security, of which the Tempest shielding of personal computers, workstations and peripherals is a large component. In the absence of a capable motivated opponent such as the former Soviet Union, this burden on both traditional and new members is increasingly difficult to justify. As a result, many systems at a medium level of sensitivity are migrating from a shielded to a zoned mode of protection.

Over the last year, a new technology has emerged which complements zoning in an attractive way. Soft Tempest consists of the use of software techniques to filter, mask or render incomprehensible the information bearing electromagnetic emanations from a computer system. This may give complete protection to some system components, and while the level of protection available for others is only of the order of 10–20 dB, this translates to a difference of about one zone, which can still give a very significant cost saving. It is already available in COTS products; here we discuss its introduction into NATO systems.

1 Introduction

NATO and its member states have been concerned for decades about the electromagnetic emission security (emsec) of computer and communications equipment [1]; the threat was mentioned in the open literature as early as 1967 [2] and became widely publicised in 1985 [3, 4]. Emsec is commonly understood as consisting of Tempest (the interception of stray information bearing RF emissions from equipment), Hijack (the interception of sensitive information that has somehow contaminated an electrical signal accessible to an attacker, e.g. a power line or ciphertext feed) and Nonstop (the interception of sensitive information that has accidentally modulated secondary emissions of an RF carrier such as a mobile phone or radar signal). Each of these three terms is also used to refer to the relevant defensive techniques [5, 6, 7].

These definitions do not exhaust the space of emsec threats; it is possible, for example, to extract information from some equipment by illuminating it with a microwave beam and studying the return signal [8]. Other equipment can be caused to fail and leak information by an attacker who inserts transients in the power supply [9, 10]. Such active attacks tend to be given less attention by military equipment suppliers but are likely to become more important with the increasing use of COTS products; they can interact in nasty ways with protocol and algorithm design [11].

Nor is emsec an exclusively military problem. Banks are worried about Tempest attacks on automatic teller machines; the ease with which the stray RF from an RS-232 line can be monitored has been documented in the open literature [12, 13], and such lines are used to connect the ATM CPU with the magnetic card reader and PIN pad. A number of sources report the capture of both PIN and card stripe contents at a distances of up to 8 m (e.g., [14, 15]). There have now been at least two unclassified conferences on emsec protection [16, 17].

A growing concern is that many security processors sold to the commercial market are vulnerable to emsec exploits. Smartcards are a case in point; by observing the current drawn by the card, it is often possible to distinguish different instructions being executed and even the Hamming weight of the data words on the bus [18, 19]. Even where the implementation detail is unknown, the execution of a block cipher such as DES can be observed as a 16-fold repeated pattern [18, 20], and by comparing the current drawn when different blocks are encrypted under the same key, the key may be found. In the case of DES, this typically takes about 1000 blocks [18]. Although security processors with a larger form factor can incorporate capacitors or other filters to limit the bandwidth of information leakage through the power supply, this is a hard problem with single-chip processors and is a subject of serious research.

Finally, although emsec attacks in the commercial sector are still relatively specialised, the development of software radios may change this. Whereas developing an attack today may require equipment such as the HP 3587 Signals Analysis System [21], which costs about $100,000 and whose export can be controlled, the same functionality will probably be available in ten years' time in low-cost PC peripherals providing a range of RF services such as UMTS and GPS using software radio techniques [22].

So attacks remain a threat, despite the disappearance of the USSR; indeed, the threat environment will become more complex and diverse. But the traditional countermeasure – metal shielding [5] – is expensive and likely to remain so; the existing alternatives, which include jamming [23] and specialised hardware techniques such as scanning a VDU raster in a random order [24], have a number of disadvantages. This motivates us to ask whether there are any other alternatives.

2 Soft Tempest

It has been known for some time that the information bearing RF emanations from a computer can be modified by its software. For example, the first author learned to program in 1972 at the Glasgow Schools Computer Centre on an early IBM machine which had a 1.5 MHz clock; a radio tuned to this frequency in the machine room would emit a loud whistle. A colleague wrote a set of subroutines of different lengths such that by calling them in sequence, the computer could be made to play a tune.

A modern re-implementation of this is described in [25]: a PC monitor with a pixel frequency of 70 MHz can be fed video signals which implement a 10 MHz radio signal, amplitude modulated with different tones. This can be used to attack computers that are not connected to networks and have good physical security: the computer is infected with a virus which searches the disk for keys or other interesting material and then transmits it to a nearby receiver. (A more sophisticated implementation could use spread spectrum rather than simple AM.) Indeed, there has been speculation that such a 'Tempest virus' has been used in at least one actual incident of espionage [26].

Such phenomena led us to consider whether software techniques could be used for defence as well. We conducted a series of experiments in late 1997 and early 1998 and tried a number of possible approaches. For example, we tried to mask the Tempest signal from a VDU by generating a jamming signal with a dither pattern in the background; this did not work too well as the jamming signal usually ended up modulated fairly conspicuously with the screen contents we were trying to hide. Eventually, we evolved a set of techniques that do appear to work reliably, and these are described in detail in [25, 27]. We will now describe two of the techniques briefly.

Figure 1: Standard black on white text image.

Figure 2: The same text after horizontal low-pass filtering.

2.1 Filtered fonts

The technique which has attracted most publicity, and which is already fielded in two commercial security packages [28, 29], is font filtering. We discovered that most of the information bearing RF energy from a VDU was concentrated in the top of the spectrum, so filtering out this component is a logical first step. We removed the top 30% of the Fourier transform of a standard font by convolving it with a suitable $\sin(x)/x$ low-pass filter.

Figure 1 shows standard black on white text; figure 2 shows the same text after low pass filtering; figure 3 shows a section through the original text; figure 4 a section through the filtered text, whose background is set at 85% white; figure 5 a section as received by the monitor if a cheap low-pass filter is installed in the VDU cable; figures 6 and 7 show the same text (normal and filtered) as it appears to the authorised user on the PC monitor; and finally

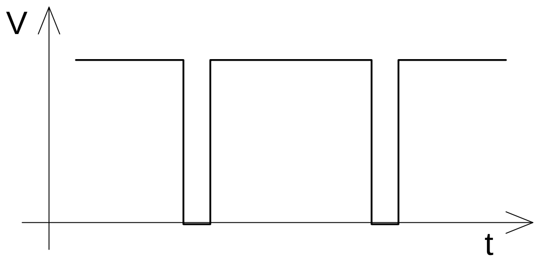

Figure 3: Video signal of a normal font

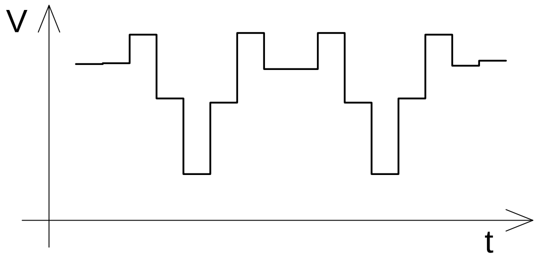

Figure 4: Video signal of a filtered font

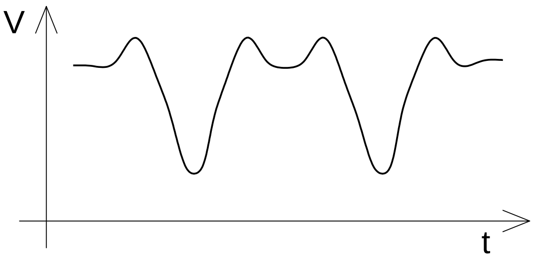

Figure 5: Video signal of a filtered font after analog HF suppression

figures 8 and 9 show the normal and filtered text as it appears to the unauthorised viewer using an ESL model 400 Tempest monitor [30].

The filtered text looks rather blurred and unpleasant in the magnified representation of figure 2, but surprisingly, the loss in text quality is almost unnoticeable for the user at the computer screen, as can be seen from the magnified photos figures 6 and 7. The signal is in any case filtered by the video and monitor electronics and the impedance of the VDU cable (which typically contains a ferrite choke to limit RFI/EMI). When one adds in the limited focus of the electron beam and the limited resolution of the eye, the net effect of filtering is small. Indeed, some observers think that the image quality is slightly improved.

While there is little visible change for the user, such filtering causes a text which could previously be received easily to vanish from the Tempest monitor, even when the antenna is right next to the VDU. The Tempest receiver screen shots in figures 8 and 9 show that not only has the information bearing signal disappeared, but the receiver's automatic gain control has turned up, displaying the synch pulses as vertical lines (the text appears four-up here as the line frequency of the monitor in use is 70 kHz while our elderly Tempest receiver was designed in the era of the PC-AT and only goes up to 20 kHz).

Filtered text display requires greyscale representation of glyphs, but this technology is already available in many display drivers in order to support anti-

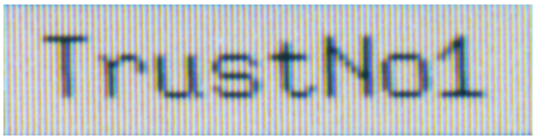

Figure 6: Screen appearance of a normal font

Figure 7: Screen appearance of a filtered font

Figure 8: Eavesdropper's view of normal fonts

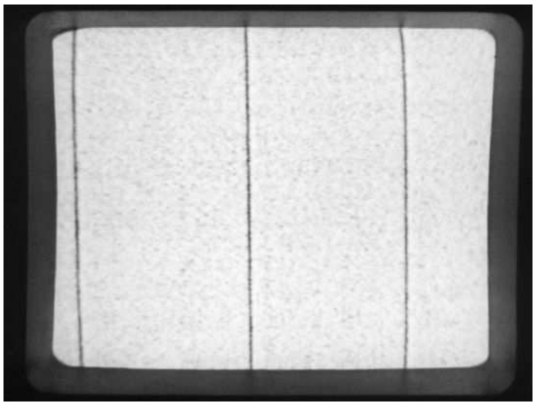

Figure 9: Eavesdropper's view of filtered screen content

aliasing fonts. The next generation of anti-Tempest display routines may also apply the opposite of the techniques used in OCR fonts: signal differences between glyphs of different characters can be minimized and there can be multiple representations of some glyphs with quite different signal characteristics. This should make automatic character recognition by the eavesdropper more challenging.

Eavesdropping text from a monitor is only one of the Tempest risks associated with personal computers. Nevertheless, we still consider it the most significant one, as the video display unit is usually the strongest source of information bearing radiation.

2.2 Securing a keyboard

Another possible application of Soft Tempest techniques lies in securing computer keyboards. Here there are two main threats: the passive observation of RF emanations at harmonics of the keyboard scan cycle, and active attacks in which the keyboard cable is irradiated at a harmonic of its resonant frequency and the scan codes are detected in the return signal which is modulated by the nonlinear junction effect.

Here our defensive technique involves reprogramming the keyboard microcontroller so that the scan cycle is randomised, and then encrypting the scan codes before they are sent to the PC. Thus for a given keypress, the number of keys scanned in a cycle will be a random and changing value rather than a known constant, and even although the value can be measured by an attacker, it should give him no information on the value of the keypress, on the user's typing pattern, or even on whether the keyboard is in use at all. The necessary system modifications affect only the PC's device driver and the firmware in the keyboard microcontroller.

Three features of this keyboard protection technique should be noted. The first is that, whereas font filtering may give only 10–20 dB of protection and thus be inadequate on its own in the most demanding applications, the keyboard technique may be sufficient even there (the exception is where complete shielding is needed for tactical reasons to prevent radio direction finding). The second is that the keyboard protection can be independent of other protection options. The third is that suitably modified keyboards can be supplied through existing trusted distribution chains (and can reinforce these controls as they will not work with an unmodified PC). Thus the savings of perhaps $500 per keyboard can be achieved independently of any decision to deploy font filtering techniques and in a way that appears compatible with current infosec management practices.

3 Discussion

Our results on Soft Tempest are preliminary; our testing has been limited by the facts that we do not have a shielded room on site, and that we have avoided getting the security clearance needed for access to the AMSG documents because of the restrictions this would place on our research. Further testing should explore the extent to which the level of protection given by filtered fonts depends on the display technology; while we may get around 10–20 dB with the monitor used for most of our testing (model MT-9017E produced by *iiyama*), the effect may be less on other monitors. We therefore welcome any feedback from the government research community on how our Soft Tempest techniques fare in the test environments available to them.

As a general point, we feel that the time may have come for the declassification of at least some of the Tempest, Hijack and Nonstop test requirements. (The publication of the specifications of KEA and Skipjack is an encouraging precedent.) Even if NATO is unwilling to declassify AMSG 720B, the physical shielding of 100 dB or so which we understand it specifies is excessive for many real world applications [32], and so the reasonable first step might be declassification of the AMSG 788/799 which apparently relates to equipment used in zoned protection models [33]. The increasing reliance which NATO military organisations place on COTS components and systems, and the growing importance of defensive infowar, make it advantageous to enable commercial suppliers to use standards that are in harmony with at least some of the military infosec requirements. In the absence of a lead from NATO, we may have to develop separate, open, standards for Soft Tempest implementation and testing.

What sort of applications should use Soft Tempest? We suggest the answer is all of them. Where a high level of protection is needed, as in a diplomatic or intelligence system, 100 dB of shielding may be prudent – but this can always fail. One of us was asked to do an independent review of a shielded product and had no difficulty receiving a clear signal. The equipment manufacturer then stripped down the device, washed the gaskets in alcohol, and reassembled it carefully; the signal was now undetectable. If a new device presented by a manufacturer for hostile review was faulty, then what proportion of devices in the field are also defective? In applications which require the best possible protection regardless of cost, we suggest that Soft Tempest should be mandatory; otherwise, shield failure can leave critical data unprotected.

In less critical applications, where zoning techniques are used at present, Soft Tempest has the potential to make a difference of about one zone. NATO governments should consider whether the cost savings from this will justify adopting the technology. It should also be borne in mind that once adopted it can be extended to large numbers of systems at little marginal cost; this will provide some potential for extending protection against future attackers using low-cost software radios.

In the case of some particular components, such as computer keyboards, Soft Tempest may be the best protection mechanism for all but the most demanding tactical applications. Adoption of the technology for keyboards alone might save US$ 500 per device; and if the Bluetooth protocol for secure RF communication between devices is successful in the marketplace, then Soft Tempest might become the preferred option for many system components.

4 Conclusions

Soft Tempest techniques have the potential to save NATO governments a very large amount of money. They are already fielded in COTS products, some of which are already used by government agencies. In order to avoid the emergence of different, incompatible standards for COTS and military systems, we recommend that NATO declassify the relevant Tempest test standards. More generally, it is time that governments started looking seriously at a more systematic exploitation of Soft Tempest technology.

References

[1] D Russell, GT Gangemi, *'Computer Security Basics'*, O'Reilly & Associates, 1991, ISBN 0-937175-71-4; chapter 10 (TEMPEST)

[2] Harold Joseph Highland: Electromagnetic Radiation Revisited. Computers & Security vol 5, pp 85–93 and 181–184, 1986

[3] W van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" in *Computers & Security* v 4 (1985) pp 269–286

[4] E Möller, L Bernstein, F Kolberg, *'Schutzmaßnahmen gegen kompromittierende elektromagnetische Emissionen von Bildschirmsichtgeräten'*, Labor für Nachrichtentechnik, Fachhochschule Aachen, Germany; `http://www.etechnik.fh-aachen.de/1/www1407.htm`

[5] *'Electromagnetic Pulse (EMP) and Tempest Protection for Facilities'*, Engineer Pamphlet EP 1110-3-2, 469 pages, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31, 1990; `http://www.jya.com/emp.htm`

[6] *'Emission Security Countermeasures Reviews'*, Air Force Systems Security Memorandum 7011 (1 May 1998), `http://jya.com/afssm-7011.htm`

[7] *'Überkoppeln auf Leitungen'*, Faltblätter des BSI 4, German Information Security Agency, Bonn, 1997; `http://www.bsi.bund.de/literat/faltbl/004_kopp.htm`

[8] *Personal communication*, T Handel, 1998

[9] RJ Anderson, MG Kuhn, "Tamper Resistance – a Cautionary Note", in *Proceedings of the Second Usenix Workshop on Electronic Commerce* (Nov 96) pp 1–11

[10] O Kömmerling, MG Kuhn, "Design Principles for Tamper-Resistant Security Processors", USENIX Workshop on Smartcard Technology, Chicago, IL (10–11 May 1999) `http://www.cl.cam.ac.uk/Research/Security/tamper/`

[11] RJ Anderson, MG Kuhn, "Low Cost Attacks on Tamper Resistant Devices", in *Security Protocols — Proceedings of the 5th International Workshop*, 7–9 April, Ecole Normal Supérieure, Paris; Springer LNCS v 1361 pp 125–136

[12] P Smulders, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", in *Computers & Security* v 9 (1990) pp 53–58

[13] B Demoulin, L Kone, C Poudroux, P Degauque, "Electromagnetic Radiation of Shielded Data Transmission Lines", in [17] pp 163–173

[14] DE Denning, *'Information Warfare and Security'*, Addison Wesley 1998; pp 189 ff

[15] *Personal communication*, HG Wolf

[16] *'Sicurezza Elettromagnetica nella Protezione dell'Informazione'*, Rome, Italy, 24–25 Nov 1988, Fondazione Ugo Bordoni

[17] *'Symposium on Electromagnetic Security for Information Protection'*, Rome, Italy, 21–22 November 1991, Fondazione Ugo Bordoni

[18] P Kocher, J Jaffe, B Jun, "Differential Power Analysis", in Michael Wiener (Ed.), *Advances in Cryptology – CRYPTO'99*, LNCS 1666, Springer, 1999, pp 388-397

[19] S Chari, C Jutla, JR Rao, P Rohatgi, "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", in *Second Advanced Encryption Standard Candidate Conference*, 22–23 Mar 1999, Rome, Italy; pp 133–147; `http://www.nist.gov/aes`

[20] E Bovenlander, invited talk on smartcard security, Eurocrypt '97, May 11–15, 1997, Konstanz, Germany

[21] Hewlett Packard Real-time Signal Analysis System, `http://www.tmo.hp.com/tmo/datasheets/English/HP3587.html`

[22] RJ Lackey, DW Upmal, "Speakeasy: The Military Software Radio", in *IEEE Communications Magazine* v 33 no 5 (May 1995) pp 56–61

[23] B Audone, F Bresciani, "Signal Processing in Active Shielding and Direction-Finding Techniques", *IEEE Transactions on Electromagnetic Compatibility* v 38 no 3 (August 1996) pp 334-340

[24] W van Eck, *'Video terminal with image line disarrangement'*, U.S. Patent 4669117, May. 26, 1987.

[25] MG Kuhn, RJ Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in David Aucsmith (Ed.), *Information Hiding, Second International Workshop*, Portland, Oregon, USA, 15-17 April, 1998; Springer LNCS v 1525 pp 124–142; `http://www.cl.cam.ac.uk/Research/Security/tamper/`

[26] ER Koch, J Sperber, *'Die Datenmafia: Computerspionage und neue Informationskartelle'*, Rowohlt, ISBN 3-498-06304-9, 1995.

[27] MG Kuhn, RJ Anderson, *'Low Cost Countermeasures Against Compromising Electromagnetic Computer Emanations'*, UK patent application no 9801745.2, January 28, 1998; also filed as US patent

[28] STEGANOS II Security Suite, from DEMCOM, Germany; `http://www.demcom.com`

[29] Pretty Good Privacy v 6.0.2, from NAI Inc, USA; `http://www.pgpi.com`

[30] *'Operating Manual for DataSafe/ESL Model 400B/400B1 Emission Monitors'*, DataSafe Limited, 33 King Street, Cheltenham, Goucestershire GL50 4AU, United Kingdom, June 1991

[31] *'Bloßstellende Abstrahlung'*, Faltblätter des BSI 12, German Information Security Agency, Bonn, 1996

[32] D Whitworth, "Information Security and Electromagnetic Emission Control, Relating to Installations, and Integrated Approach", in [17], pp 31–38

[33] R Briol, "Emanation – How to keep your data confidential", in [17], pp 225–234