Turing Trust Policies on Data Sanitisation and Destruction

Objective

This White Paper discusses the issues regarding reliable data destruction and sets out the policies used by the Turing Trust to protect against data breaches when processing donated computer equipment and media.

Background

Whilst most computer users are aware that sensitive or confidential data may be stored on media within a computer it is often not understood that data remains on the media, even when apparently deleted, in a form that can be recovered using appropriate expertise and technical tools.

The Turing Trust refurbishes used computers for re-use in schools in Africa and has a duty of care to ensure that data is removed with an appropriate level of sanitisation commensurate with the sensitivity of the data stored on the media (hard disk, removable media, flash memory, etc.).

Computer (electronic or digital) documents are more difficult to sanitise than paper documents. In many cases, when information in an information system is modified or erased, some or all of the data remains in storage. This may be an accident of design, where the underlying storage media still allows information to be read, despite its nominal erasure. The general term for this problem is data remanence. Sanitisation typically refers to countering the data remanence problem. When the operating system is not active it is possible to use raw disk editors and recovery tools to view and recover data that the operating system has deallocated making it necessary to securely delete files to prevent this.

The only way to ensure that deleted files are safe from recovery whilst still retaining valuable disk media is to use a secure delete application. Secure delete applications overwrite on-disk data from deleted files using techniques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files. The Turing Trust uses a variety of proprietary secure delete tools including Paragon, Killdisk and Blancco or an inbuilt secure-erase function in firmware as appropriate to the equipment. Any disk that fails is physically destroyed, using our own equipment, to prevent recovery.

Standards

In the UK HM government defines **Information Assurance Standard No. 5**: Secure Sanitisation. IS5 is part of a larger family of IT security standards published by CESG; it is referred to by the more general Infosec Standard No.1. IS5 sets a wide range of requirements - not just the technical detail of overwriting data, but also the policies and processes that organisations should have in place, to ensure that media are disposed of securely.

IS5 defines two different levels of overwriting:

- Baseline overwriting of data involves one pass, overwriting every sector of the storage medium once with randomly generated data.
- Enhanced overwriting involves three passes; each sector is overwritten first with 1s, then with 0s, and then with randomly generated 1s and 0s.

IS5 is similar to DOD 5220.22-M (used in the USA).

The **National Industrial Security Program**, or **NISP**, is the nominal authority (in the United States but widely used internationally) for managing the needs of private industry to treat classified information.

A major component of NISP is the Operating Manual, also called NISPOM, or DoD 5220.22-M. The NISPOM establishes the standard procedures and requirements for all government organisations with regard to classified information. As of 2016, the current NISPOM edition is dated December 2014. This document is available free of charge in PDF format from

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
Data on magnetic media is normally overwritten by writing characters over every addressable area of the media. Historically there was a lot of discussion about whether a single pass or multiple passes of writing characters were necessary for data destruction. A distinction was also previously made between Clearing, Purging or Destroying data.

In 2006 NIST SP-800-88 stated that "Basically the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack." That same year DoD 5220.22-M removed all verbiage on single vs multiple pass. The standards were now leaning towards each entity making its own decisions based on its own risk and threat assessment. Essentially the message was "one pass is as good as multiple as long as it is verified as complete. If you are in doubt, or have something that is of a sensitive nature, physically destroy it."

Our Strategy

By default our technicians instigate at least a single-pass secure wipe on all donated disk media at no cost to the Donor or, in the case of a Manufacturer's HDD firmware secure-erase function, multiple passes. This can take many hours of processing using our industry-standard tools as they write characters across all addressable areas of the disk. For example a modern 1TB disk in a USB external enclosure can take up to 18 hours to wipe. This makes the data irretrievable for all intents and purposes from any keyboard-based or computer workshop operation.

We can also undertake other processes if requested to meet any standard of data security. However, we do ask donors to consider the extra time required to complete these processes so may ask for a fee to compensate for the expense of doing this and ensure we're able to deliver maximum benefit to our partner schools in Africa.

If data is considered so sensitive or confidential that it cannot be allowed to leave an organisation then disks should be removed by the donor and physically destroyed before donating the host computer to us.

We have an obligation under the Data Protection Act 1998 to ensure that confidential data about employees or customers is not disclosed without the consent of the individual concerned. The Turing Trust is registered with the Information Commissioner's Office under registration reference ZA062486 in accordance with the requirements of the Act.

Many PCs come with built in Recovery media that is often held in a hidden disk partition. Where a Manufacturer provides this and it is still intact at our receipt of the system we may first use the Manufacturers' own procedures to format the main system partition and recover the original Operating System and Programs then also instigate a Wipe Free Space procedure to ensure deletion of any residual data. This ensures that we get a working machine with the OEM license for whatever Operating System it was originally provided with.

Where systems are donated without such Recovery Media (typically from corporate organisations who build their own system images) we do a Full Wipe operation prior to any other activity. If we have appropriate Operating System Media we may then restore the machine from that and re-use the original OS Certificate of Authenticity.

A Note on WEEE (Waste Electrical and Electronic Equipment)

The Turing Trust accepts **only** donations of **working** equipment for re-use which are not therefore considered as Waste. Where organisations require a suitable Transfer Note (known as a WTN) we can provide that in a suitable format accepting a Duty of Care for the donated equipment a list of which needs to be provided electronically to us in advance by the donor organisation. Certain types of electronic item (e.g. CRT monitors) are classed as containing hazardous waste and are not accepted for donation. In case of doubt Donors should check with us first if an item of equipment is acceptable for donation.