Laser-printed PIN Mailer Vulnerability Report

Mike Bond, Steven J. Murdoch, and Jolyon Clulow

Computer Laboratory, University of Cambridge,
JJ Thomson Av., CB3 0FD, UK
{Mike.Bond, Steven.Murdoch, Jolyon.Clulow}@cl.cam.ac.uk

Abstract. Tamper-evident laser-printed PIN mailers are used by many institutions to issue PINs and other secrets to individuals in a secure manner. Such mailers are created by printing the PIN using a normal laser, but on to special stationery and using a special font. The background of the stationery disguises the PIN so that it cannot be read with the naked eye without tampering. We show that currently deployed PIN mailer technology (used by the major UK banks) is vulnerable to trivial attacks that reveal the PIN without tampering. We describe *image processing attacks*, where a colour difference between the toner and the stationary "masking pattern" is exploited. We also describe *angled light* attacks, where the reflective properties of the toner and stationery are exploited to allow the naked eye to separate the PIN from the backing pattern. All laser-printed mailers examined so far have been shown insecure.

1 Laser-printed PIN Mailers

Laser-printed PIN mailers are used to issue PINs to customers of banks , and in many other roles, including secure issue of login secrets for internet services, and in delivery of sensitive material such as pay advice slips. They are now a popular alternative to old-fashioned impact printed PIN mailers, and pressure-sealed mailers.

The three major laser-printed PIN mailer technologies we examined are Documotion's *Hydalam* [1], Bastione's *PINTAB* [2] and Paragon's *Scratch Code* [3]. All the technologies are designed to work with a conventional laser printer. The special mailer stock has a plastic region which is toner receptive, and has a masking pattern printed underneath which when combined with the PIN (printed using a special dithered font) makes it very difficult to read. To tamper the mailer, the masking pattern is removed in one of a number of ways: it is peeled off from behind as a removable tab, it is scratched away using a coin or fingernail from the reverse of the plastic, or the entire plastic is peeled away from the surface of the mailer. The stationery is designed so that attempts to reattach tabs, or recreate the masking pattern are difficult. An instruction box on the back of a PIN mailer typically advises customers how to detect tampering of their mailer.

The laser printer renders the PIN onto the plastic region, using a special font with dithered background and foreground, resulting in a series of fine dots of

toner. For example figure 1 shows an example the plastic regions of untampered and tampered Hydalam brand mailers.

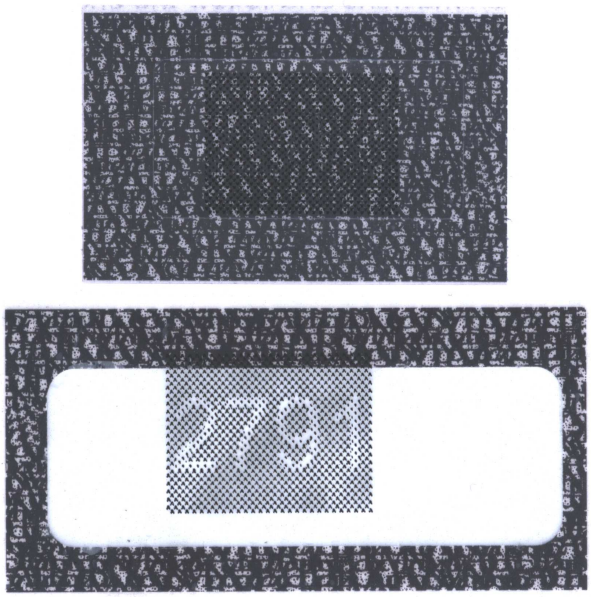

Fig. 1. Untampered and tampered Hydalam mailers from Halifax plc, Nov 2004

2 Direct Inspection Attack

If the dither pattern is coarse, the PIN can be read by careful, direct visual inspection, with the eye at a perpendicular angle to the mailer. Digits rendered with a fine pattern can often be read by individuals with good eyesight. We experimented with this on a number of samples: some individuals were able to make entirely correct predictions by direct inspection, others gave close matches, and some were unable. Accuracy of digit recognition is significantly improved by knowledge of the font used to render the PIN. For example, observation that a `0` digit is visibly narrower than an `8` or `9` digit can resolve the ambiguity between these digits (see figure 2 in the final section of the paper for an example of the font in question).

3 Image Processing Attack

When the dither pattern is too fine to read the digits with accuracy by direct inspection, and the angled light attack countermeasure is used, simple image processing tools can aid a human to make PIN identification viable.

The Hydalam mailer we attacked had the PIN printed using a fine dither pattern, and the finer dithering in the font made basic angled light attack difficult. We thus scanned the mailer at 1200dpi in colour and greyscale using a flatbed scanner, illuminated from the front by the scanning mechanism, and from behind using a desk lamp. We also repeated the experiment substituting a digital camera in macro mode for the scanner.

We analysed the images using the freely available image manipulation tool "GIMP" [4]. We also experimented with Adobe Photoshop and Paintshop Pro. We applied a colour intensity threshold function, adjusting the threshold manually, whilst standing one to two metres away from the screen. When the threshold is set between the intense black of the toner and the dark grey of the masking pattern, the PIN becomes visible. Once we had chosen the optimal threshold, we applied a gaussian blurring filter to assist our eyes with recognition of the digits.

The top image in figure 2 shows a PIN revealed from Hydalam stock using a coarse dither. The lower image shows a PIN printed in a higher resolution font, and revealed using an optimised method, though still working within the confines of standard functionality of image-editing packages. In these more difficult cases, or when the font is unknown, there can be ambiguity about some digits. However, if the PIN is used in an ATM system, for example, this ambiguity can be resolved within the typical retry limit of three attempts. The images in figure 3 show further examples of this attack

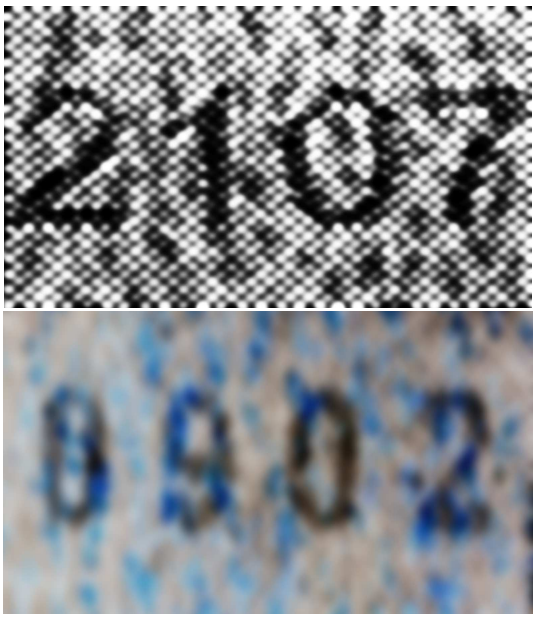

Fig. 2. Image Processing Attacks on Hydalam (Halifax Plc, Smile, Nov 2004)

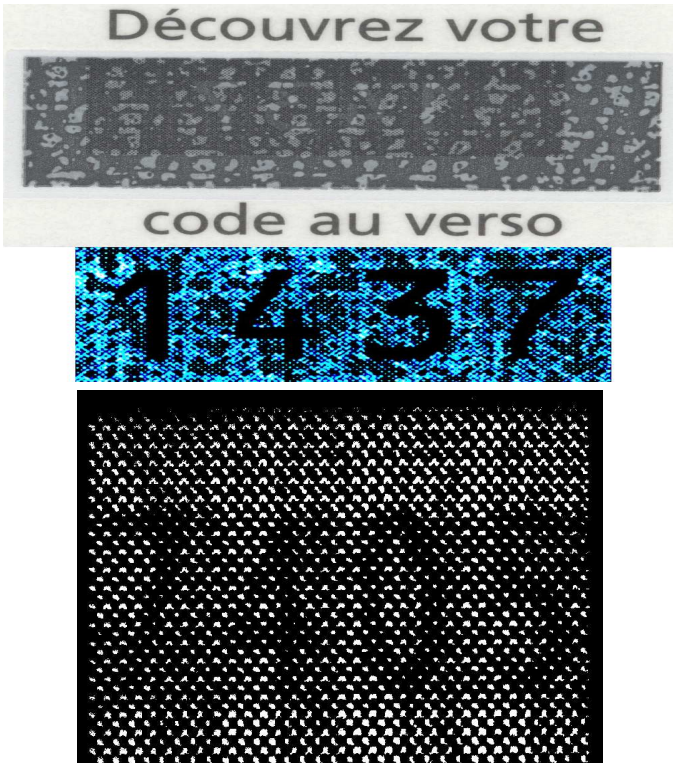

Fig. 3. Image Processing Attacks on Scratch Code (Paragon, Barclays, Dec 2004)

We believe the basic technique of image capture, followed by threshold, then blur, can be optimised and automated to recover PINs from a wide number of variants of laser-printed PIN mailers. Indeed, we have found the image processing attack effective against all *deployed* stock analysed so far, regardless of manufacturer.

4 Angled Light Attack

The plastic surface and toner have different reflective properties. Holding the mailer with the eye at about 10 degrees from parallel, with a light source at the same angle opposite causes the plastic to become highly reflective. The difference between the toner and plastic becomes obvious, and the PIN is easily read even by individuals with poorer eyesight. Figures 4 and 5 were taken substituting a digital camera for the human eye, and clearly show the effect.

The effectiveness of the angled light attack appears to be governed by a number of factors: the design of the font, the resolution of the font, the density of toner laid down, and the properties of the plastic patch itself.

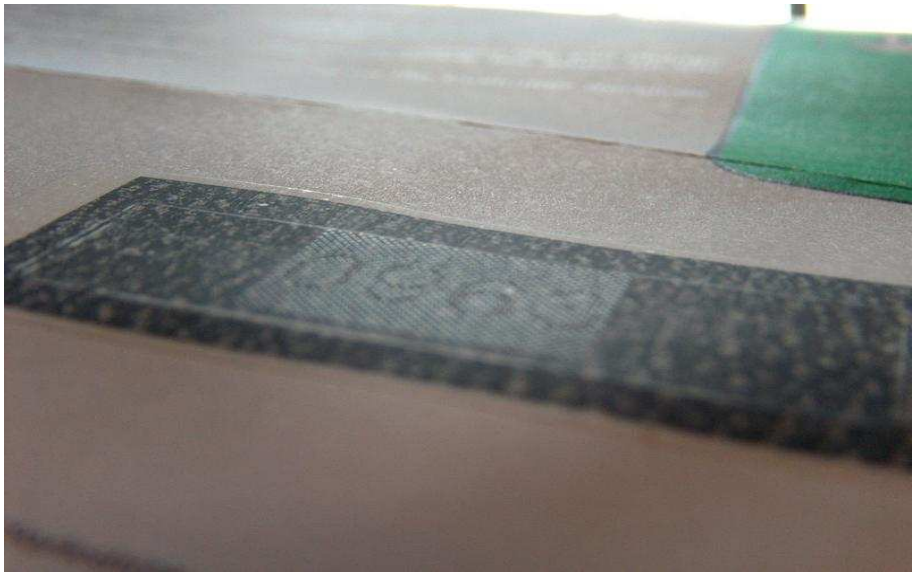

Fig. 4. Angled Light Attack on Hydalam Mailer (Halifax Plc Nov 2004)

Fig. 5. Angled Light Attack on PINTAB Mailer (Nominet UK, Jun 2005), brown envelope mask used to reduce glare for purposes of photography

5 Conclusions

The combination of PIN mailer technology and printing techniques used by most major UK banks and a number of other institutions does not currently achieve the tamper-evidence one would expect. All deployed laser-printed mailers from all manufacturers examined so far can be defeated. Trivial human inspection is possible if the dither pattern is too coarse, or if too much toner is used, and straightforward computer-aided image manipulation attacks work wherever there is a colour difference between toner and masking pattern. Angled-light attacks are also extremely effective, even when there is minimal colour difference between toner and masking pattern, as the differences in reflective properties of the materials is much greater.

It should also be noted that the full catalogue of possible attacks on laser-printed PIN mailers extends past those detailed here to consider magnified inspection attacks, augemented angled light attacks and chemical attacks. Whilst these are beyond the scope of this report they need to be fully investigated and counteracted by the manufacturers at the earliest opportunity; they will be the subject of forthcoming publications in this area.

In the short term, careful tuning of the fonts used could yield significant improvement. In the mid-term, the technology could clearly be improved, and we have been working closely with technology manufacturers, UK banks and APACS toward developing the next generation of PIN mailer technology. We delayed the release of this report by 9 months to allow for this work to be undertaken. Finally, in the long-term, we imagine a rethinking of PIN issue strategy will provide a secure and cost-effective way to make the best use of the available physical and logical security mechanisms.

Finally the authors would like to make it clear that this document is an updated version of a report on the vulnerability originally circulated to manufacturers and UK banks in Nov 2004. The original document is also available [5].

References

1. Hydalam Mailer Technology `http://www.versari.com/Hydalam.asp`
2. Bastione Ltd, The Tallet, North Road, Timsbury, Bath BA2 0JJ, UK
3. `http://www.paragon-europe.com`
4. The GNU Image Manipulation Program, `http://www.gimp.org`
5. `http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer-Old.pdf`