IN THE INNER LONDON CROWN COURT

Serco Monitoring

v

Defendant X

PRELIMINARY EXPERT REPORT OF ROSS JOHN ANDERSON

I, Ross John Anderson, say as follows.

1. I am Professor of Security Engineering at Cambridge University. I am a Fellow of the Royal Society, the Royal Academy of Engineering, the Instisute of Physics, the Institution of Engineering and Technology and of the Institute of Mathematics and its Applications. I hold the BA, MA and PhD degrees from the University of Cambridge.

2. My research focusses on security engineering – the art and science of building systems that remain dependable in the face of malice, error and mischance. I am the author of the textbook 'Security Engineering – A Guide to Building Dependable Distributed Systems' (Wiley, 2001 and 2008) of which Chapter 14 is a standard reference on security printing and seals. Both editions of the book are available free online from my website. I have also published over a hundred research papers on the topic of security engineering. I am also responsible for teaching many of the practical aspects of computer science at Cambridge University, including courses on software engineering and security, and organising group projects.

3. Prior to becoming an academic in 1992, I worked for many years in in-

dustry, where I was involved in designing equipment, writing software and consulting on security and cryptography; I also worked for a number of banks, most recently Standard Chartered Bank in 1989 where I was responsible for designing the security architecture for all the bank's retail operations in Asia. I also consulted for many firms that sell information security products to banks, including PIN entry devices and the cryptographic processors that are used to secure ATM transactions. Phyiscal tamper resistance is an essential attribute of cryptographic processors and I was responsible for the design and evaluation of this among other things.

4. Since moving to academia in 1992, the security of tamper-resistant cryptographic and transaction processing systems has remained a research interest. I am an author of many of the most widely-cited publications on the security of cryptographic and tamper-resistant systems, including

   (a) "Why Cryptosystems Fail" in *Communications of the ACM* vol 37 no 11 (November 1994) pp 32–40

   (b) "Liability and Computer Security – Nine Principles", in *Computer Security – ESORICS 94*, Springer LNCS vol 875 pp 231–245

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

   (d) "Why Information Security is Hard – An Economic Perspective", in *Proceedings of the Seventeenth Computer Security Applications Conference* IEEE Computer Society Press (2001), pp 358–365

   (e) "Cryptographic Processors – A Survey" (with Mike Bond, Jolyon Clulow and Sergei Skorobogatov), *Proc. IEEE* v 94 no 2 (Feb 2006) pp 357–369

(f) "Thinking inside the box: system-level failures of tamper proofing" (with Saar Drimer and Steven Murdoch), 2008 IEEE Symposium on Security and Privacy, pp 281–295; outstanding paper award

(g) "Chip and Pin is Broken" (with Steven Murdoch, Saar Drimer and Mike Bond), at *IEEE Symposium on Security and Privacy* (2010) pp 433–444; outstanding paper award

(h) "Measuring the Cost of Cybercrime" (with Chris Barton, Rainer Böhme. Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage), at the *Workshop on the Economics of Information Security* 2012

(i) "Chip and Skim: cloning EMV cards with the pre-play attack" (with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov), arXiv 0547955, Sep 2012

These papers, and other papers of mine on information security, may be downloaded from my web site, `http://www.ross-anderson.com`.

5. I have acted as an expert witness in a large number of cases involving disputed electronic banking transactions, both in the UK and abroad, including both civil and criminal matters. In criminal matters I have acted for both the prosecution and the defence. I have also been asked on many occasions to assist parliamentary committees on matters of information security, with two recent examples being the House of Lords Science and Technology Committee's inquiry into Personal Internet Security (at which I testified) and the Health Select Committee's inquiry into the Electronic Patient Record (at which I was a Special Adviser). I also chair the Foundation for Information Policy Research.

6. I have also acted as an expert adviser on other tamper-resistant systems,

notably to the Electricity Supply Commission of South Africa in a project in 1992–4 to introduce prepayment meters on a large scale, which enabled the electrification of over 2 million households during Nelson Mandela's presidency; and to the Department of Transport in the late 1990s during negotiations in the European Council that led to the EU's adoption of standards for digital tachographs. These projects are described in my book.

7. My source of instructions is the defendant's solicitor Alex Whitmore of Dalton Holmes Gray. I have been supplied with (a) a Serco document bundle dated August 1st containing witness statements of Witness 1, Witness 2 and Witness 3, plus supplementary material; (b) a DTMATMR21 'Subject all events considered' call-centre log from 12/5/13 to 23/7/13; (c) an expert witness statement from Witness 4 dated 5th August on the examination of PID 51820; and (d) the initial breach notice served by Serco at court. I was also briefed on what happened at the initial hearing on 12th July.

8. Two allegations of breach were made initially:

   (a) 25th April 2013: tampering with the tag

   (b) 1st June 2013: being two and a half hours late back

9. It turned out that the 1st June had been the occasion of the defendant's mother's birthday; there had been prior solicitor's correspondence about this between the defendant and Serco; the defendant had a handwritten note recording a phone call from Serco on May 20th granting a late date on June 1st; and this was confirmed in the Serco DTMATMR21 document (b). Serco accordingly withdrew the second charge leaving the issue of alleged tampering on 25/4/13.

10. I am asked by my instructing solicitor whether there may be reasonable doubt about the allegation that the defendant failed 'to allow the order to be electronically monitored in that on or about the following date(s) and time(s) you did cause, or allow to be caused, the integrity of the Personal Identification Device, part of the electronic monitoring equipment, to be compromised. (Damage to the "tag".) PID tamper 25/4/13 08:23:40'

11. According to the court documents (d), after a tamper alarm was reported by the monitoring system, the defendant was visited by Witness 1 who reported 'no visible signs of a tamper' and replaced the PID (though she 'had to try three PIDs before I found one that worked'). Four days later a further tampering event was reported; the defendant was visited by ZZZZZ who reported 'No marks or any signs of tampering. FMO didn't secure the clips properly. The clips had a gap between the strap and the pid. FULL RECALL DONE AND new pid 2 fitted. Ranges 30/40. MU moved to a table nearer the door.' The PID was replaced yet again by Witness 1 on June 16th following 'multiple short absence', apparently due to the PID not communicating properly with the site monitoring unit (SMU) – the base station installed in the defendant's home that communicates with both the PID and Serco's central computer system.

12. There is correspondence in the court papers regarding a previous warning for 'absences' and saying 'further investigations have since been made and the warning has now been cancelled' (dated April 30th). I must presume this related to earlier presumed tampering events than the event on April 25th for which the defendant is now being prosecuted. The call-centre logs only go back as far as May 12th, so I do not have the history for February, March and April (though there is a handwritten note from the defendant recording equipment alarms or failures on Feb 19, 20 and 25;

Mar 16; April 5, 16. 25, 29 and 30; and May 3, 5, 13 and 14. A subsequent letter (16/05) blames a 'weak signal' and refers to a further PID change on May 15th. Here too there was prior solicitor's correspondence. The DTMATMR21 document records further service outages including a power cut on May 20th and two 'change in code sequence too large' events which may perhaps indicate an equipment malfunction or reset, whether in the PID or the SMU. One of these was on April 25th, the day of the alleged offence. Yet when I look at exhibit ADM/1 (the first page of appendices to the statement of Witness 3) I find two such alarms in the raw events log.

13. On the day of the alleged offence there are the following records in the DTMATMR21 document

    (a) 01:03:08 a call appears to have made and answered by another person (not the subject)

    (b) 01:33:32 the system appears to have created in error, and cancelled, a 'First of Two visit required between 25/05/2013 01:33:32 (BST) and 25/05/2013 05:33:32 (BST)'

    (c) 04:03:32 the system again appears to have created in error, and cancelled, a 'First of Two visit required between 25/05/2013 04:03:32 (BST) and 25/05/2013 08:00:00 (BST)'

    (d) 07:07:38 'change in code sequence too large'

    (e) 20:00:00 'Lost Contact Investigation Visit required between 25/05/2013 20:00:00 (BST) and 25/05/2013 23:59:59 (BST)'

    (f) 20:00:00 the system again appears to have created in error, and cancelled, a 'First of Two visit required between 25/05/2013 20:00:00 (BST) and 25/05/2013 23:59:59 (BST)'

(g) 22:30:00 the system again appears to have created in error, and cancelled, a 'Second of Two visit required between 25/05/2013 22:30:00 (BST) and 26/05/2013 08:00:00 (BST)'

14. The overall impression from the factual documentation is of a shambolic system with a high false alarm rate. There is a substantial security engineering literature on such systems going back to the problems of radar operators in World War 2, and extending through the Cold War to modern problems such as security screening in airports and certificate alerts in web browsers. Where most alarms are false alarms, it is difficult to maintain watchers in a state where they are alert but also capable of discriminating. Human cognitive heuristics and biases lead watchers to jump to conclusions and see patterns that are not there. It is important for such systems to be complemented by well-designed procedures, regular testing and automated tool support where possible.

15. Yet Serco appears to operate unreliable back-end systems, as we see from the visit schedules created in error and then cancelled.

16. I note also a later entry (June 4th) which records that the prosecution was raised as a result of the 1st June violation and served on June 7th. This was an error and was withdrawn. There is no record of a decision to prosecute opposite the alleged violation on 25th April, for which the defendant now faces trial. This charge appears to have been an afterthought to the now-withdrawn charge.

17. This raises doubt about the robustness of Serco's manual procedures.

18. The record also raises questions about the testimony of Witness 3 to the effect that the PID 'was securely fitted to the curfewee for at least 91 days without incident or failure' (section 26).

19. In his testimony at section 28, he says that 'In the rare event of an FMO fitting a clip insecurely I would expect to see multiple PID strap check failures being recorded while the curfewee inevitably fidgets when for example playing on a computer game, or moving the strap and/or PID while changing socks, changing in and out of trousers, drying with towel (sic), normal day to day activities etc. I could find no such recordings on the raw events.' And yet the FMO ZZZZZ reported that the FMO Witness 1 'didn't secure the clips properly. The clips had a gap between the strap and the pid.'

20. It appears that much of the data presented to the court has been filtered. For example, two 'PID PR code too large' events in exhibit ADM/1 for 25/4 become a single 'change in code sequence too large' event in the DTMATMR21 document.

21. The internal logic of the system is also not clear from the supplied documents. For example, we see on 25/4 'PID strap check failed' at 08:23:40, 'PID tamper has occurred' at the same time, and 'PID strap check passed' at 08:23:55. Yet later that day we find 'PID strap check failed' at 17:59:44 followed by 'PID strap check passed' at 17:59:47, yet without a 'PID tamper has occurred' alert between them. It is not clear why a tamper alert was raised the first time but not the second time. It is not clear what may have caused the 'PID PR code too large' and whether this might have had any bearing on the tampering alarm.

22. I now turn to the expert report prepared by Witness 4 of [Company]. He reports a lack of contact marks on the PID case or strap and concludes 'This means that a soft or rounded object, like the soft tissues of the fingers, to generate the tamper message to the control centre' (sic). Yet the strap shows no evidence of having been subjected to the 35kg loading

that according to Witness 3 must be applied to break the strap; we gather than angled loading would have resulted in striations while linear loading would have deformed the punched holes.

23. However the strap has stretched by 1.3mm or 0.7% of the original length and it is slightly kinked. The amount of stretch is consistent with wear and tear but Witness 4 is of the view that the kink is consistent with attempted tampering:

> There is a small kink in the natural curvature of the strap suggesting that a large load has been applied to the strap away from the wrist when installed. This could be as a result of the subject trying to stretch the strap off the wrist.

24. There are prising marks between the clip and the case indicative of a tampering attempt that was unsuccessful but might have increased the likelihood of subsequent false alarms. This is stated in 4e and reiterated at 11: 'there is prising marks on the clip, which will have effected the load at which a tamper message would have been generated' (sic). There are also tamper marks on the PID case but these are of no significance as cases are reused between curfewees.

25. The fibre optic cable is recessed inside the strap, with the result that the force required to generate a tampering alarm would be lower. Here (section 7) Witness 4 seems to assume that the PID was installed on the defendant's wrist, rather than her ankle, because of a swollen ankle; but he is aware that it's round her wrist at sections 5 and 10. He notes at 7 though 'This phenomenon would have a greater effect, the smaller the size of the strap'.

26. So Witness 4's substantive conclusions are that the PID would have been

more sensitive than usual (and thus more likely to register a false alarm) for three reasons: the fibre optic cable is recessed; the prising marks indicative of an earlier unsuccessful tamper; and the shortness of the strap. In the other pan of the scales is the observation that the small kink in the strap 'could be as a result of the subject trying to stretch the strap off the wrist.'

27. I am surprised that Witness 4 does not report making any experiments to substantiate this claim. This case does not turn on a unique incident such as a car crash but an easily repeatable action, namely pulling on a PID strap. Standard forensics procedure would be to fix PIDs on volunteer subjects' wrists and ankles, pull them off, and get several observers to measure the resulting kinks at a series of tensions below and above the threshold at which the PID registers a tamper alarm. If the amount of kink is dependably measured by different observers and is found to be correlated to tamper events by appropriate statistical tests, then such an inference might reasonably be relied on by a court. As it is, Witness 4's methodology is defective.

28. I am further surprised to see that Witness 4 not only claims in his 'Opinion and conclusion' section that 'In my opinion [defendant] has attempted to manipulate the tag around the wrist in order to be freed from the curfew order'. The charge relates to whether the defendant caused, or allowed to be caused, the integrity of the PID to be compromised; there is no evidence of who pulled the strap (if indeed anyone pulled it hard enough for there to be a material breach), and of course only a court could free the defendant from the order. But even if Witness 4 had written this sentence more carefully, what he probably meant is not really supported by his observations.

29. Witness 4 goes on to say 'In my opinion the subject has also used a

tool to try to lever the plastic clip away from the PID to separate two plastic components and loosen the strap from the currect position. This has stretched the strap, kinked the natural parabolic curvature and left behjind evidence of a tamper on the surfance texture of the plastic.' This is not consistent with his earlier explanation that the kink must be due to the strap being pulled with the fingers. Putting a screwdriver between the PID and a clip, and pulling the strap, are quite different operations.

30. Witness 4 appears to be quite unaware of the other indications of system fragility in this case, such as the 'change in code sequence too large' and the message visit messages created in error and then cancelled.

31. There is one further aspect of this case that the court might care to notice, namely the common purpose between most of the players in this drama except for the defendant. The monitoring system is operated by Serco; the PIDs are manufactured by Serco Geografix, presumably a subsidiary; the prosecution if brought by Serco; and presumably Witness 4's company is under contract to them too. Such cosy arrangements are not always conducive to independent thinking, or to employees or contractors being willing to discuss failings frankly. There have been other such cases, such as the notorious Shirley McKie miscarriage that brought fingerprint evidence into question, and stemmed from the fact that all UK fingerprint examiners were at the time employed by police forces or prosecutors; there have been other interesting cases in the payments industry, where suppliers are reluctant to break ranks.

32. Given that the monitoring system appears to be flaky, with a high rate of false alarms, buggy back-end systems and chaotic supporting procedures, and that the forensic report produced by the prosecution has clear errors in logic and defects in methodology, I recomend that the court enable

me to conduct a proper independent forensic examination. For this I will require access to the system.

33. I therefore request the court to order Serco to provide me with:

    (a) the PID in this case;

    (b) six PIDs and a site monitoring unit (SMU) with which to experiment;

    (c) 50 sets of straps and clips for destructive forensic testing;

    (d) a field management unit (FMU) with which to configure PIDs and the SMU;

    (e) the specification of the central computer system (CCS);

    (f) the Ministry of Justice specifications for the PID, the SMU and the FMU;

    (g) details of the training given to field management operatives;

    (h) details of the training given to supervisory staff and/or forensic experts whose duties include examining PIDs for signs of tampering;

    (i) such data as Serco have on the rate of false alarms and missed alarms from the PID, SMU, CCS and from administrative procedures;

    (j) reports of testing done on the tamper-resistance or tamper-evidentness of PIDs, straps and clips, whether internally by Serco or by external parties such as the Ministry of Justice;

    (k) copies of other reports on the security of the system prepared by Serco's auditors, Ministery of Justice inspectors, CESG and any other party to have professionally assessed the dependability of the system.

34. Without access to the system's documentation, and to samples of PIDs, straps and clips for testing, I doubt it will be possible to perform a thorough independent evaluation of the claims made in respect of the alleged tampering incident.

35. In the absence of access to technical documentation and actual testing, all I can advise the court is that the factual and expert evidence on which this prosecution rests have sufficient inconsistencies to raise reasonable doubt about the claim that the defendant must have made a tampering attempt, or caused such an atempted to be made by soemone else, on April 25th 2013. It may be that the alarm was caused by a technical fault, as these certainly happened; or the alarm may have resulted from the PID having become overly sensitive, perhaps through wear and tear, so that it did not require 35kg of force to register a tamper but merely some innocuous activity.

36. I understand that it is my duty to help the court on the matters within my expertise and that this duty overrides any obligation to the person from whom I have received instructions. I have complied with that duty. I have done my best to be accurate and complete.

37. I believe that the matters of fact stated in my report are true, and the opinions I have expressed represent my true and complete professional opinion.

Signed

Ross Anderson

August 15th 2013