APACS RESPONSE TO CLARIFICATION QUESTIONS RAISED BY STEPHEN MURDOCH OF CAMBRIDGE UNIVERSITY

Q - Which testing laboratories evaluated the two PEDs we discuss, under the Visa PED specification and APACS Common Criteria standard?

A We are not at liberty to disclose the names of the laboratories in question or other details that may impact their business. The choice of which approved laboratory a PED developer might choose is up to them. It is a contractual relationship between the laboratory and the developer. We can confirm that laboratories approved by the respective payment schemes evaluated both devices.

Q - Were the vulnerabilities we identified recognized during the evaluation?

A. During any security evaluation it is expected that the laboratory will identify areas where a potential attack could be carried out. Once they have identified these areas, they consider if the current security measure provided by the terminal are sufficient to meet the current level of the security requirement or if improvements are required. In this case the evaluation reports conducted against the devices evaluated under the common criteria did not identify any specific vulnerabilities in the devices that required additional mitigation.

Q - If so, how were they dealt with? If not, where do you think the evaluation process failed?

A The evaluation process did not fail. The devices passed at the level of protection identified in the criteria and against the stated attack potential.

Q - Can we have the evaluation report?

A No, as APACS has no remit to share testing reports – they are commercially-sensitive information and as a result there are stringent Non Disclosure Agreements in place to preserve confidentiality. The evaluation report from any evaluation process is a confidential document between the laboratory conducting the evaluation, the developer of the device and, where necessary, the certifier of the evaluation.

Q - Can you explain why certification reports are not public when they are of public interest and their results affect customers?

A We have no evidence to believe that their results impact our customers and we do not believe that making these highly technical reports publicly available is in the public interest. The evaluation reports contain detailed information as to how the security features of a terminal work. Releasing the document into the public would reduce the effectiveness of these controls, and therefore defeat the object of performing the security evaluation. However, we continue to welcome any insights to potential vulnerabilities and

threats so we can inform the evaluation laboratories in order to reinforce the strength of the evaluation process.

We would also wish to note that we are not aware of any widely recognised and credible evaluation methodology process, in security or otherwise, which makes evaluation reports publicly available.

Q - Is the certification of the PEDs we studied to be withdrawn?

A No.

Q - Are the affected PEDs to be withdrawn from use, and if so, when?

A They are not being withdrawn from use as after careful consideration by the industry we do not agree with your risk assessment.

However, both devices are “end-of-life” products and are no longer available for new deployments. Over time new models will replace them.

Q - If we find further vulnerabilities in other PEDs, will those be promptly withdrawn from the market?

A Every vulnerability is looked at on a case-by-case basis and so it would entirely depend upon the specifics; the level of exposure and exploitability of that vulnerability; the nature of the assets it exposes; and the skills and capabilities needed by the adversary to develop and exploit the vulnerability.

Q - Are you aware of other PEDs with the same issues?

A No.

Q - If so, will their certification be withdrawn?

A N/A

Q - Are the testing labs that performed the evaluations to have their accreditation revoked?

A The only body that can revoke an evaluation laboratories evaluation accreditation is the evaluation scheme management body. In the case of the Common Criteria that is CESG for UK labs, the National Technical Authority for Information security. We remain totally confident in the current processes used to maintain the evaluation quality of the evaluation laboratories. CESG has been made aware of your findings you may however wish to approach them to determine if they are planning to revoke any accreditation.

Q - What changes, if any, will be made to the certification processes in order to prevent such failures in the future?

A We do not consider this to be a failure. We do, of course, continue to welcome any insights to potential vulnerabilities and threats so we can inform the evaluation laboratories in order to reinforce the strength of the evaluation process. In this case it is important to recognise that the requirements against which evaluations are conducted have increased significantly. These requirements increased well before you made you carried out your study and made the findings available to us.

Q - Will encrypted PIN verification and/or iCVV be deployed to reduce the risk of smartcard interception, and if so, when?

A Encrypyted PIN capabilities will only become available once the industry starts to roll-out DDA capable cards. In the meantime the industry is now under a mandate from the global card schemes that any new card issued after 1 Jan 2008 must implement iCVV.

Q - What measures are in place or being put into place to mitigate the vulnerabilities we discuss?

A One of the measures against terminal tampering is to give effective and proactive guidance to the merchants deploying the terminals, complemented by industry fraud monitoring capabilities. This guidance was made available to merchants several months ago and prior to us being aware of your paper.

Q - Were these vulnerabilities recognized during the PED development process?

A All developers are aware of the need to protect the key data assets being stored and processed in their devices, and they all take steps to mitigate vulnerabilities that might expose these assets, in line with the threat attack potential they are being evaluated against.

Q - What changes in the PED development process are to be taken to prevent further vulnerabilities?

A This will be for individual developers to consider. However, improvements and changes in the security evaluation requirements have and will continue to drive improvements in the development of the PEDs in order for them to attain approved status. This is a continually evolving process in response to new threats and new vulneabilities..

Q - Are you aware of any cases where PED tampering was used for fraud? If so, can you provide details? If no details can be provided, can you at least provide the number of cases seen and the sums involved?

A There have been some instances of PED tampering being used to commit fraud in the UK but not the type of attack detailed in your report. The numbers of PED compromise

that have taken place in the UK are minimal, however, and the banking industry's standard fraud prevention measures have meant that these frauds and their location were detected quickly. It is not within our remit to provide specific details, number of case or losses.

Q - Can you assess the risk to customers from these vulnerabilities based on your (yet, non-public) knowledge of the types of fraud committed by criminals?

A We believe that the risk remains very low from these types of hardware based attacks. For the following reasons:

- This type of attack requires far greater effort and engineering to execute than you currently estimate, is significantly difficult to industrialise to the numbers of devices that would gain criminals the return they would expect and, therefore, not economically viable to criminals.
- Hardware tampering is relatively easy to detect through fraud monitoring and physical inspection of the devices, this is because devices have to be left in situ for so long that they are increasingly vulnerable to detection.
- Unfortunately there continue to be simpler attack strategies that the criminals can follow which are much more in line with their current capabilities.

Q - Will any other action be taken as a response to our paper?

A We have shared the results of your paper across the industry and with laboratories and going forward of course we continue to welcome any insights you can provide to potential vulnerabilities and threats. We aim to provide the most current information to the evaluation laboratories in order to reinforce the strength of the evaluation process.

Q - Will you provide us newly approved PEDs for evaluation?

A No. We do not believe that it would be appropriate for the industry or the developers to offer new PEDs for you to evaluate. Whilst we recognise that you are competent engineers and researchers, you are neither trained evaluators against the approved methodologies, nor are you an accredited evaluation laboratory - capable of conducting evaluations on a commercial basis - respecting clients' expectations of commercial confidentiality.

Q - Do you have any further comments to add?

A Yes. We found the report raise some interesting issues and, as mentioned, we welcome any insights to potential vulnerabilities and threats in order to provide the most current information to the evaluation laboratories in order to reinforce the strength of the evaluation process.

However, there was degree of ambiguity in your report in two particular cases where we would welcome clarification. Firstly, it is not clear how the tamper-proofing failed or was defeated that lead to your ability to tap into the data lines. In fact your description seems

to describe a method that doesn't require the tampering to be defeated. Secondly, it is not clear what data paths and data you are specifically accessing. We would therefore appreciate being sent the technical details of the research work performed including specific information relating to what data was obtained and how long it took to be able to obtain the data.

-oooOooo-