FUJ00230908

From: Membery Bill
Sent: Thur 18/02/2010 11:27:47 AM (UTC)
To: Lillywhite Tom[GRO]
Subject: RE: Track II - list of questions
Attachment: Membery Bill.vcf

Hi Tom

Answers are:

8.
(a) What are the current security measures in place to prevent access to the Track II data?
[GIJ] Best for Tom to answer, but basically there is very limited access to the Audit Servers and presumably such access is itself audited.
(b) How easy or difficult could those measures be to breach (is there an objective measure/standard)?
[GIJ] Again one for Tom
(c) Could they be improved and if so, how?
[GIJ] Again one for Tom

a. This depends on which part of the system, the Live systems, the Test systems or the audit systems. Within the live estate defence in depth exists with ACLs, Firewalls, IDS, Obfuscation in Code, Clearances of staff, role management, etc.
b. Within Audit control is role based with limited access to audit servers and only limited key staff permitted to extract the data as part of the audit process, the severs are data centre based and the clients in a secure room with limited access
c. Support systems and Test systems is an area I am not certain about need to talk to Debbie Richardson Test and to Program, I believe JS ensured that development in India was not able to review, but not certain that Peak and TFS have controls in, needs an audit in this area
d. Currently there are no measures only tests are Pen Tests could do with a physical attempt to Breach by another Fujitsu Security Team member of staff.
e. Yes whole area could be improved use of ikey tokens, update of support systems and Test systems to specific test rigs for PCI.

Kind Regards
Bill

From: Lillywhite Tom
Sent: 18 February 2010 10:57
To: Membery Bill
Subject: FW: Track II - list of questions

Bill

See question 8 below…can you answer it?

From: Jenkins Gareth GI
Sent: 17 February 2010 09:54
To: Butts Geoff; Lillywhite Tom; Kirkham Suzie
Cc: D'Alvarez Alan; Welsh Graham; Clark Jason
Subject: RE: Track II - list of questions

FUJ00230908

Geoff / Suzie,

My suggested answers to most of the questions below prefixed ***[GIJ] in bold italics*** lower down in the email trail.

There's a few that I think Tom needs to answer, and others may want to correct some of the detail as I was not involved in the proposal that Jim and Jason have put together, though I understand what it is actually proposing and how it should work (I have some detailed comments on that, but that can be resolved if we really do progress with this).

Note that I'm now coming to the conclusion that we probably **can** technically put together a robust mechanism to remove the T2 Data. However it would be difficult to **prove** that it is robust and even harder to provide a simple explanation of it in a witness statement or in court, and so I would still recommend that we do **not** tamper with the audit trail.

Regards

Gareth

Gareth Jenkins
Distinguished Engineer
Applications Architect
Royal Mail Group Account

FUJITSU
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Tel: GRO Internal: GRO
(Note new external number -
old number will not work after 31/12/2009)
Mobile: GRO Internal: GRO
email: Gareth.Jenkins GRO
Web: http://uk.fujitsu.com

-----Original Message-----
From: Butts Geoff
Sent: 16 February 2010 18:40
To: Lillywhite Tom; Welsh Graham; Clark Jason; Jenkins Gareth GI
Cc: Kirkham Suzie; D'Alvarez Alan
Subject: FW: Track II - list of questions
Importance: High

All,

FYI - some detailed questions from Hugh Flemington following on from the discussion yesterday. I will be on leave on Thursday and Friday this week. Can you send Suzie any responses to the questions by close of play Thursday so that she can collate these and send to the respective legal teams. If the timescales are too tight, please let Suzie know so that expectations can be set with POL.

Thanks.

Regards,

FUJ00230908

Geoff

Geoff Butts,

Programme Manager, HNG-X Release 1,

Royal Mail Account

Practitioner, P&PM Academy

FUJITSU

Mob: GRO or Internally GRO
E-mail: geoff.butts GRO
Web: http://uk.fujitsu.com

Fujitsu Services Limited, Registered in England no 96056, Registered Office 22 Baker Street, London, W1U 3BW

-----Original Message-----
From: Kirkham Suzie
Sent: 16 February 2010 15:57
To: Butts Geoff
Subject: FW: Track II - list of questions
Importance: High

Geoff

PSB - please can you circulate to the team who will compile the response. They want a response by Friday

Kind regards

Suzie

Suzie Kirkham

Account Manager

Royal Mail Group

FUJITSU

Lovelace Road, Bracknell, Berks RG12 8SN

FUJ00230908

Tel: GRO Internal: GRO

Mob : GRO

Fax: GRO Internal: GRO

E-mail: suzie.kirkham GRO

Web: <http://uk.fujitsu.com>

-----Original Message-----
From: Prenovost Jean-Philippe
Sent: 16 February 2010 14:18
To: Kirkham Suzie
Subject: FW: Track II - list of questions

Hot off the press.

Let's discuss once you have had a chance to review.

Kind regards

JP

-----Original Message-----
From: hugh.flemington GRO
Sent: Monday, February 15, 2010 5:48 PM
To: Prenovost, Jean-Philippe
Subject: Re: Track II - list of questions

Hi JP.

Below is the magic list of questions compiled from a few people today since our call this morning. Would Fujitsu be able to get us reponses by close of play on Friday plse?

It looks like a long list, but we want to get as full a picture as possible before any decision about deletion is taken within Pol about whether to press for a compromise from the PCI or go for simple deletion of T2 data. Pol need to understand what Fujistu would be able to say if necessary in a witness statement that could be used in evidence in criminal or civil litigation. Your responses will also help build any submission to PCI (can you tell which way I think Pol will go!). To that end it would be helpful if Fujitsu could indicate the certainty of your answer in each case. If it is not possible to answer any of the questions, please say so too.

Questions:

FUJ00230908

1. Before Track II data is deleted, would Fujitsu be able to say precisely what impact the deletion would have eg what additional data would also be deleted or amended and if so, how it would be amended.
[GIJ] The intention is that Track 2 data would be obfuscated as would any corresponding Digital signatures and Checksums since they would no longer be relevant. Also the PAN would be obfuscated by replacing it with a "hashed" PAN (as is done in HNG-X). We would also add in an Encrypted version of the PAN so that if necessary the original PAN could be recovered (again this is similar to what is done on HNG-X). Although not included in the current study report, I would also recommend that any ICC Data (ie data generated by the Chip on the Card) is also obfuscated. The result of this is that the Audit of the original message would be changed and it would no longer be possible to assert it has not been changed since originally recorded. Also the revised audit file would need to be re-sealed again indicating that it has not be tampered with since the time of the "official" change.

2. We are trying to understand how quick and easy it would be to assess the impact of the deletion. After the deletion:

(a) would Fujitsu be able to say precisely what additional data had in fact been deleted or amended, how it had be amended and precisely what affect this has on the Horizon system?
[GIJ] We would be able to say what sort of data has been deleted / amended, but clearly would not be able to say what the original data was!

(b) to accurately answer 2(a) would it be necessary for Fujitsu to consider the impact of the deletion on the data submitted by each Post Office branch, or would the answer be apparent at a macro level?
[GIJ] This would be apparent at a Macro level

(c) Would the amendment or corruption of other data be reversible?
[GIJ] Not clear what is meant by "other data". The intention is to only amend Track 2 data and related signatures / checksums (and possibly ICC Data). Non Track 2 data would not be changed. However the integrity controls that are normally checked when generating evidence would no longer be valid. It is intended that the changed data would be signed at the time it is changed to enable it to be asserted that it has not been corrupted after the removal of the Track 2 data.

(d) Would any amendment or corruption non Track II data other data be a one off event ie due to Track II data, or is there a risk that the deletion sets in motion a chain reaction leading to further amendments or corruption in the future?
[GIJ] For any audit file, it would be a one off event. However there are many audit files generated each day on Horizon and it is likely that a considerable period of time would be required to alter all the necessary Audit files so different files would be amended / corrupted at different times. I would not expect any chain reaction for a specific file though.

(e) How long would it take and how much would it cost to assess the full impact of deletion?
[GIJ] I've not seen any costs. Can someone else answer this. However I would not expect this to be Cheap!

(f) Would it be possible to illustrate to, for example, a court, what precisely has been done to establish continuity?
[GIJ] It might be possible. However it is normally a non-technical person that provides evidence in court and it would be difficulty to provide a simple description of what has been done that can be easily understood and would not cause a distraction from the main evidence.

3. After the deletion, what would Fujitsu be prepared to say generically about the integrity and accuracy of the remaining data on the Horizon system? How certain could Fujitsu be of that integrity and accuracy, please?

FUJ00230908

[GIJ] We could describe the process and indicate that the data was correct from the time it was generated until the T2 data was removed and also that it had not been corrupted since that time. What would be hard would be to show that the tools used to remove the T2 data had not inadvertently corrupted other data as a side effect since it is all in the same basic message.

4.

(a) Precisely how would the deletion of the Track II data change transaction and events logs?
[GIJ] There is a single log produced by Horizon which includes both Transaction details and Event information (and a whole load of other information which is not usually used in evidence). All messages in this log that include Track 2 data would be altered by the tools. This would affect some Transactions (and in particular any that relate to Banking, Credit / Debit card and perhaps E-Top Ups (depending on detailed design). The tool is unlikely to alter and messages relating to Events since they don't include Sensitive data. However the audit file that contains the events would have been altered.

(b) would its deletion only corrupt rows on those logs which relate to credit card transactions, or would it affect other rows too and if so, how?
[GIJ] It would also affect rows containing Debit card and banking Transactions and perhaps E Top-Ups as well. Other rows are unlikely to be affected (but it may be difficult to prove that).

(c) how would credit card transactions after the Track II deletion appear in events and transaction logs?
[GIJ] Where data has been altered, then it is expected that the original data would be replaced by a standard character (probably an asterisk). However PANs would be replaced by Hashed PANs and each message would be extended to include details of the Encrypted PAN to allow the original PAN to be retrieved.

(d) After the deletion, would POL be able to definitively prove the amount of each credit card transaction, whether it took place and when it took place and if so, how would it prove this?
[GIJ] This is the key issue. The tool would be designed such that financial amounts would not be changed. However being able to prove that this had not happened inadvertently would be difficult.

(e) Would we still be able to trace a transaction?
[GIJ] Yes.

5. What is the probability that the deletion would affect the data contained in the following? (Especially its reliability and accuracy). If it would affect such data, please describe the potential and likely affects:

(a) branch trading statements;
[GIJ] Not applicable. We do not provide BTS as part of the formal audit evidence. (We have been able to do so in some cases from Horizon, but it is not part of the contractual service we provide.)
(b) Transaction correction notices (formerly called error notices ie charge or credit errors);
[GIJ] Such transactions are unlikely to contain data that would result in them being altered. However it might be difficult to prove that.
(c) Data relating to cash and stock remittances to a branch;
[GIJ] Such transactions are unlikely to contain data that would result in them being altered. However it might be difficult to prove that.
(d) Data relating to cash receipts from a branch;
[GIJ] Such transactions are unlikely to contain data that would result in them being altered. However it might be difficult to prove that.
(e) Data relating to transactions (eg sales) performed at a branch;
[GIJ] These may be affected if they are card related.
(f) Cash declarations;

FUJ00230908

[GIJ] Not applicable. We do not provide Cash Declarations as part of the formal audit evidence. (We have been able to do so in some cases from Horizon, but it is not part of the contractual service we provide.)
(g) Balance snapshots;
[GIJ] Not applicable. We do not provide Balance Snapshots as part of the formal audit evidence. (We have been able to do so in some cases from Horizon, but it is not part of the contractual service we provide.)
(h) NBSC or HSH telephone call logs; and
[GIJ] These are held in separate logs and aren't affected. (I'm not familiar with what is and is not held, but such logs are unchanged.)
(i) Data relating to any IT problems experienced at a branch.
[GIJ] I assume that this relates to event logs etc, so again these are held is separate logs which are unaffected.

If the deletion would not affect the above data, how certain could Fujitsu be of that, please?

6. In your own words, please can you describe the full effect that the deletion of the Track II data is likely to have on the Horizon system and how certain you can be of that.
[GIJ] Not sure what else to add to the detailed answers above.

7.
(a) Would the encryption of the PAN cause any issues?
[GIJ] This requires the original message to be increased in size and so we would be unable to assert that nothing had been added to the original audit data.
(b) And what about it's subsequent de-encryption to produce as evidence in any cases? Will we still be able to access it?
[GIJ] My understanding of the proposed solution is that this would be possible. Note that the way in which it is encrypted would be different from "normal" encrypted PANs so new tools would be required to decrypt the data.

Finally
8.
(a) What are the current security measures in place to prevent access to the Track II data?
[GIJ] Best for Tom to answer, but basically there is very limited access to the Audit Servers and presumably such access is itself audited.
(b) How easy or difficult could those measures be to breach (is there an objective measure/standard)?
[GIJ] Again one for Tom
(c) Could they be improved and if so, how?
[GIJ] Again one for Tom

Kind regards,
hugh

FUJ00230908