FUJ00170288

From: Keating, Lewis (UK - Leeds) GRO

Sent: Thur 11/05/2017 7:46:17 AM (UTC)

To: Norman, Russell[GRO]; Godeseth, Torstein[GRO]; Newsome, Pete[GRO]; Westbrook, Mark (UK - Manchester)[GRO]; 'jonathan.gribben[GRO]

Subject: RE: Further Project Bramble discussion - Riposte

Hello all

Please find below a list of questions, as previously discussed, for the call @ 1pm.

Thanks
Lewis

Walkthrough of the Cryptographic Process
Step through the cryptographic process between Counter and BRDB onwards to Audit Store to refresh understanding with a view to obtaining a view on the following specific questions:

Horizon Online

1. Is the segregation of duties breach between database administration and the key management server, the only way in which a weakness could be exploited to overwrite transactional information in a way where it cannot be traced and looks legitimate to the system?
2. Is 1am the following day stipulated as the date and time by which overwrite would need to be achieved by due solely to the audit store, and if so are there not other more timely data feeds which would highlight a discrepancy between actual 'transactional reality' and what is recorded in the Audit Store or the BRDB?
3. For step 6 of the replacement routine, can you remind us the technical reasons for requiring access to the BAL Private Key?
4. On step 9 on the super user audit log – how long can this log be edited by the super user? Same 1am window before transmission to the Audit Store? Also a reminder that it is the hardware protection rather then the digital seal which is important on the Audit Store due to the usage of the cracked MD5 algorithm for sealing?
5. On the point on editing the log, if I'm reading correctly it would always be possible to see the last action by the superuser, even if they deleted all else?
   Can we provided further detail on how the attached would work – 'In order to make the changes to the Message Log described in section 2.2, the Super User would need Read access to the Key Store database which runs on the NPS and Read / Write access to the BRDB. Note that should the rogue application run on the BAL, then this isn't necessary as the BAL's have access to the Key store based on the IP address.'
   5a. Could a superuser (theoretically) cover their tracks completely by removing log on / log off activity from the audit log without leaving a trace? If not how feasibly is a comparison between all log on/ log off activities of super-users' and MSCs in order to detect un-authorised access?
6. 'Although the Database Audit tables are not regularly examined they were recently checked as part of an external Audit of Horizon Online.' – Could you provide further context on this audit? What was checked and why?
7. How often would the individuals who contravene access SoD between the NPS and BRDB tend to logon to the NPS? Also does the point raised on not needing to logon with access to the BAL broaden this concern?
8. For step 2, how big is the average message log associated with any log on session. (i.e. is a log on session generally all day and therefore the message log will hold thousands of transactions?)
9. For step 4, are there any barriers to uploading this application onto Fujitsu systems (if this would be required). Presumably this would be required due to the volume of work required?
10. For step 5, what is meant by 'similar'?
11. On step 8, is there a formal control operated by Fujitsu which can be referenced which would provide evidence for 'any instance of slow running on the system would be investigated by the support teams'. If

FUJ00170288

not can we articulate how obvious this would be to evidence it would be picked up in BAU activity?

12. For step 9, can we expand on the relationships between data held in the message log and in branch accounts (or database tables which feed counter reporting). We would like to be able to articulate the degree of difficulty amending both sources concurrently would require. And we would like to state this in terms of:

a. Timing issues
b. Complexity (would more programmes be needed)
c. If this was not done perfectly then would mis-matches be identified / flagged?

Riposte

1. 'The Riposte product managed the Message Store and it did not allow any message to be updated or deleted. ' – Is there any further information available on this control?
   'Each message also had an associated CRC, this was basically a checksum that was included to ensure that the message had not become accidently corrupted. Note that this was not a cryptographically secure seal and it would be possible for a sufficiently technically skilled person to alter a message and recalculate the CRC if they had access to the message outside the message store.' – i.e. the level of protection on Riposte was lower?
2. The Digital Seal for the Riposte Audit Store remained the same as for Horizon Online – i.e MD5? And the hardware protection was applied the same as well?
3. 'Due to the size of the Post Office Network, Branches were split into 4 separate Clusters. Each Cluster included 4 Correspondence Servers (2 in each Data Centre), thus ensuring that there were normally 4 copies of the data held in the Data Centres.' – Does this mean you would need to duplicate corrupted data across 4 servers?
4. In 'Detecting Changes to the Audit Trail' the following is stated, 'However, if such data were injected at the Correspondence Server, it would be clear that this had occurred since the Node Id associated with the message would be that of the Correspondence Server at which the message had been injected and not a normal Counter Node Id. This would be clearly visible in any audit extract.' Could this not be spoofed?

Consideration on the Implications for Fundamental Question Set Posed by POL being:

1.1 The key question is whether Horizon accurately and only records the transactions input or approved by branch staff in a manner that either:-

1.1.1 cannot be added to, deleted or altered; or,

1.1.2 if they can be added to, deleted or altered, such changes will, in all circumstances, be either:

(a) visible to postmasters; or at least

(b) logged and identifiable by Post Office / Fujitsu / a third party expert.

1.2 Assuming the above is correct, it should be possible to either:-

1.2.1 prove that no such changes occurred in a particular branch; or

1.2.2 where changes have occurred, identify such changes and show what changed.

1.3 The specific outstanding questions are:-

1.3.1 What exact information is logged by the Super-User Audit Logs?

1.3.2 Would this logged information show that:-

(a) a Super-User had done something that could change a branch's accounts in the real-world (e.g. that the Super-User had amended or deleted a transaction in the Branch Database); and

(b) what that Super-User had done (i.e. does it show the change in such a way that it could be identified and either isolated or reversed out)?

1.3.3 If the Super-User Audit Logs would not reveal all actions by Super-Users that could affect branch accounts, please provide a full description of ways in which a Super-User could amend a branch's accounts in a way that could would not leave behind a footprint of their activity is required.

-----Original Appointment-----
From: Russell.Norman [GRO]
Sent: 09 May 2017 16:49
To: Russell.Norman [GRO]; Torstein.O.Godeseth [GRO]; pete.newsome [GRO]; Keating, Lewis (UK - Leeds); Westbrook, Mark (UK - Manchester)

FUJ00170288

Subject: Further Project Bramble discussion - Riposte
When: 11 May 2017 13:00-14:00 (UTC+00:00) Dublin, Edinburgh, Lisbon, London.
Where: Skype Meeting

This meeting can move between 12-2 if necessary and will centre around riposte. I will not be attending the call but will arrange it so please let me know if you would like to change the time.

Fujitsu are aiming to source Gareth Jenkins for this call.

Thanks,

Russell

.....

Join Skype Meeting

Trouble Joining? Try Skype Web App

Join by phone

GRO English (United Kingdom)

English (United Kingdom)

GRO (UK External) (UK&I) English (United Kingdom)

Find a local number

Conference ID: GRO

Forgot your dial-in PIN? | Help

For the optimal Skype for Business experience, logon to conferences with your PC and use some USB headphones. If you do not have a set of USB headphones, please order some using the standard process.

.....

FUJ00170288