android.nfc.tech.NfcA.transceive not working as expected

DESCRIPTION sh...@gmail.com created issue #1

Hi there,
I have a project for which the goal is to evaluate MifarePlus card features.
After personalization, MifarePlus is automatically brought to what they call SL1. At this stage MifarePlus behaves like a MifareClassic card except that it supports a few other NXP proprietary co
But tests run on an Nexus 5x/Android 8.1.0 suggests there is an issue with it. The response from the card to the initial proprietary command is 1 byte shorter than it should be.
Can't tell for sure whether this is in Android java code issue or in the underlying driver(NxpExtns), but to me it looks like something is intercepting the response from the card and processes it acc

My code snippet:

```
   public synchronized void retrieveTagInfo(Intent intent) {
      Tag tagFromIntent = intent.getParcelableExtra(NfcAdapter.EXTRA_TAG);

      Log.d(TAG, "tag: " + tagFromIntent);
      Log.d(TAG, "tag.getId() Arrays: " + Arrays.toString(tagFromIntent.getId()));
      Log.d(TAG, "tag.getTechList() Arrays: " + Arrays.toString(tagFromIntent.getTechList()));
      Log.d(TAG, "tag.toString(): " + tagFromIntent.toString());

      byte[] tagIdInBytes = tagFromIntent.getId();
      String tagId = bytesToHexString(tagIdInBytes);
      Log.d(TAG, "tag.getId() to hex " + tagId);

      NfcA nfcA = NfcA.get(tagFromIntent);;
      try {
         nfcA.connect();
         MifarePlus mifarePlus = new MifarePlus(nfcA);
         mifarePlus.authenticityCheck();
         tv.append("auth OK\n");
      } catch (Exception ex) {
         tv.append("auth error: " + ex.getMessage() + "\n");
      } finally {
         try {nfcA.close(); } catch (Exception x) {}
      }

public class MifarePlus {

   private String TAG = MifarePlus.class.getSimpleName();
   private NfcA nfcA;

   public MifarePlus(NfcA nfcA) {
      this.nfcA = nfcA;
   }

   private byte[] authenticateStep1(int keyNumber) throws Exception {

      byte[] apduBuffer = {0x76,0x00,0x00};
      apduBuffer[1] = (byte)(keyNumber & 0xff);
      apduBuffer[2] = (byte)((keyNumber>>8) & 0xff);

      Log.d(TAG, "CAPDU " + bytesToHexString(apduBuffer));
      byte[] apduResponse = nfcA.transceive(apduBuffer);
      Log.d(TAG, "RAPDU " + bytesToHexString(apduResponse) +" length: "+apduResponse.length);
.....


   public void authenticityCheck() throws Exception {

      int iRet;

      int keyNumber = 0x9004;
         byte[] ivBytes = new byte[16];
         for (int i = 0; i<16; i++) {ivBytes[i] = 0;}
         byte[] secret = {0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,
            0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f};


         byte[] ekNoB = authenticateStep1(keyNumber);
      Log.d(TAG, "AUTHENTICATE STEP 1 DONE");
.....
```

The logcat output indicates 1 byte missing (there should be 17 bytes coming back : 1 byte status(0x90=okay) + 16 bytes some encrypted random challenge

logcat:

```
02-14 15:39:13.759 563-723/? D/audio_hw_primary: disable_audio_route: usecase(1) reset and update mixer path: low-latency-playback
02-14 15:39:13.774 563-723/? D/audio_hw_primary: disable_snd_device: snd_device(95: vi-feedback)
02-14 15:39:13.774 563-723/? D/audio_hw_primary: disable_audio_route: usecase(24) reset and update mixer path: spkr-vi-record
02-14 15:39:14.630 3140-9960/? I/GeofencerStateMachine: removeGeofences: removeRequest=RemoveGeofencingRequest[REMOVE_BY_IDS Ids=[atn_geofence_request_id], packageName=com
02-14 15:39:15.135 2374-2577/? D/Event: No subscribers registered for event class com.google.commerce.tapandpay.android.valuable.datastore.HasValuablesEvent
02-14 15:39:15.136 2374-2577/? D/Event: No subscribers registered for event class de.greenrobot.event.NoSubscriberEvent
02-14 15:39:15.137 2374-2577/? D/Event: No subscribers registered for event class com.google.commerce.tapandpay.android.valuable.datastore.HasGiftCardsEvent
02-14 15:39:15.137 2374-2577/? D/Event: No subscribers registered for event class de.greenrobot.event.NoSubscriberEvent
02-14 15:39:15.141 2374-2577/? D/Event: No subscribers registered for event class com.google.commerce.tapandpay.android.valuable.datastore.ValuablesListEvent
02-14 15:39:15.142 2374-2577/? D/Event: No subscribers registered for event class de.greenrobot.event.NoSubscriberEvent
02-14 15:39:15.326 767-776/? I/zygote64: Background concurrent copying GC freed 62501(4MB) AllocSpace objects, 4(208KB) LOS objects, 42% free, 23MB/41MB, paused 129us total 134.383n
02-14 15:39:15.694 3140-3794/? W/Conscrypt: Could not set socket write timeout:
02-14 15:39:15.694 3140-3794/? W/Conscrypt:    java.lang.reflect.Method.invoke(Native Method)
02-14 15:39:15.694 3140-3794/? W/Conscrypt:    com.google.android.gms.org.conscrypt.Platform.setSocketWriteTimeout(:com.google.android.gms@11975440:13)
02-14 15:39:16.834 767-5236/? D/WificondControl: Scan result ready event
02-14 15:39:16.854 3195-3195/? D/NativeNfcTag: Connect to a tech with a different handle
02-14 15:39:16.871 3195-3195/? E/NxpExtns: Mifare : phLibNfc_GetKeyNumberMFC Key found
02-14 15:39:16.872 3195-3195/? E/NxpExtns: Mifare : phLibNfc_GetKeyNumberMFC returning = 0x0 Key = 0x0
02-14 15:39:16.874 3195-3383/? E/NxpExtns: Error Sending msg to Extension Thread
02-14 15:39:16.882 3195-3195/? D/NativeNfcTag: Check NDEF Failed - status = 3
02-14 15:39:16.890 3195-3195/? E/NxpExtns: Mifare : phLibNfc_GetKeyNumberMFC Key found
02-14 15:39:16.890 3195-3195/? E/NxpExtns: Mifare : phLibNfc_GetKeyNumberMFC returning = 0x0 Key = 0x0
02-14 15:39:16.892 3195-3383/? E/NxpExtns: Error Sending msg to Extension Thread
02-14 15:39:16.901 3195-3195/? D/NativeNfcTag: Check NDEF Failed - status = 3
02-14 15:39:16.914 3195-2702/? D/NativeNfcTag: Starting background presence check
02-14 15:39:16.923 767-12896/? I/ActivityManager: START u0 {act=android.nfc.action.TAG_DISCOVERED flg=0x20000000 cmp=com.youtap.epursetest/com.youtap.horseshoe.MainActivity (has
02-14 15:39:16.923 767-12896/? W/ActivityManager: startActivity called from non-Activity context; forcing Intent.FLAG_ACTIVITY_NEW_TASK for: Intent { act=android.nfc.action.TAG_DISCOVER
02-14 15:39:16.926 2584-2584/? D/MainActivity: onNewIntent() getAction android.nfc.action.TAG_DISCOVERED
02-14 15:39:16.926 2584-2584/? D/MainActivity: onNewIntent() toString Intent { act=android.nfc.action.TAG_DISCOVERED flg=0x30000000 cmp=com.youtap.epursetest/com.youtap.horseshoe.
02-14 15:39:16.928 2584-2584/? D/MainActivity: tag: TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFormatable]
02-14 15:39:16.929 2584-2584/? D/MainActivity: tag.getId() Arrays: [4, 97, 5, 42, -13, 90, -128]
02-14 15:39:16.929 2584-2584/? D/MainActivity: tag.getTechList() Arrays: [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFormatable]
02-14 15:39:16.929 2584-2584/? D/MainActivity: tag.toString(): TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFormatable]
02-14 15:39:16.929 2584-2584/? D/MainActivity: tag.getId() to hex 0461052af35a80
02-14 15:39:16.937 3195-3195/? W/AudioTrack: AUDIO_OUTPUT_FLAG_FAST denied, rates do not match 16000 Hz, require 48000 Hz
02-14 15:39:16.942 417-417/? W//system/bin/hw/android.hidl.allocator@1.0-service: ashmem_create_region(3840) returning hidl_memory(0x7c1042b310, 3840)
02-14 15:39:16.944 417-417/? W//system/bin/hw/android.hidl.allocator@1.0-service: ashmem_create_region(3840) returning hidl_memory(0x7c1042b310, 3840)
02-14 15:39:16.947 563-723/? E/volume_listener: check_and_set_gain_dep_cal: Failed to set gain dep cal level
02-14 15:39:16.947 2584-2584/? D/MifarePlus: CAPDU 760490
02-14 15:39:16.948 563-8226/? D/audio_route: Apply path: speaker-protected
02-14 15:39:16.953 563-8226/? D/audio_hw_primary: enable_snd_device: snd_device(95: vi-feedback)
02-14 15:39:16.953 563-8226/? D/audio_route: Apply path: vi-feedback
02-14 15:39:16.953 563-8226/? D/audio_hw_primary: enable_audio_route: usecase(24) apply and update mixer path: spkr-vi-record
02-14 15:39:16.953 563-8226/? D/audio_route: Apply path: spkr-vi-record
02-14 15:39:16.955 2584-2584/? D/MifarePlus: RAPDU 9005b89eed9873d28637997b185bc6ed length: 16
02-14 15:39:16.955 2584-2584/? D/MifarePlus: AUTHENTICATE STEP 1 DONE
```

The expected behaviour for NfcA.transceive would be to transparently pass back and forth data from the application/card and let those entities handle the aspects of the application protocol

Thank you

✓ Links (4)

"The code will initiate the authentication sending 6000 command (see https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf)"
" https://android-review.googlesource.com/c/platform/packages/app… "
" …s. In principle Android should not even try to recognize this is a mifare auth command. Consequently should not try to match the key internally. Let the application deal with the card response and l
"https://support.google.com/nexus/answer/4457705?hl=en"

COMMENTS

dn...@google.com <dn...@google.com> #2

Assigned to dn...@google.com.

Thanks for reporting this issue.
Can you provide the below requested information to better understand the issue:

Android build
Which Android build are you using? (e.g. KVT49L)

Device used
Which device did you use to reproduce this issue?

Steps to reproduce
What steps do others need to take in order to reproduce the issue themselves?
Please provide sample project or apk to reproduce the issue. Also mention the steps to be followed for reproducing the issue with the given sample project or apk.

Frequency
How frequently does this issue occur? (e.g 100% of the time, 10% of the time)

Expected output
What do you expect to occur?

Current output
What do you see instead?

Android bug report
After reproducing the issue, press the volume up, volume down, and power button simultaneously. This will capture a bug report on your device in the “bug reports” directory. Attach the bug r

Alternate method:
After reproducing the issue, navigate to developer settings, ensure ‘USB debugging’ is enabled, then enable ‘Bug report shortcut’. To take bug report, hold the power button and select the ‘Tak

sh...@gmail.com <sh...@gmail.com> #3

BuildNumber: OPM3.171019.014
AndroidVersion: 8.1.0
DeviceUsed: Nexus 5x

Attached is apk and project zip. To prove my point and make it easier to reproduce, I have changed the code so that it sends a MifareClassic command via NfcA class which should work on a

Steps to reproduce:
Run the apk and present a MifareClassic card.
The code will initiate the authentication sending 6000 command (see https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf)

The NfcA.tranceive fails according to this trace:

```
02-16 15:05:35.921 771-3522/? W/ActivityManager: startActivity called from non-Activity context; forcing Intent.FLAG_ACTIVITY_NEW_TASK for: Intent { act=android.nfc.action.TAG_DISCOV
02-16 15:05:35.926 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: onNewIntent() getAction android.nfc.action.TAG_DISCOVERED
02-16 15:05:35.927 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: onNewIntent() toString Intent { act=android.nfc.action.TAG_DISCOVERED flg=0x30000000 cmp=
02-16 15:05:35.929 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: tag: TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tech.NdefFor
02-16 15:05:35.929 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: tag.getId() Arrays: [-16, 15, 55, 30]
02-16 15:05:35.929 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: tag.getTechList() Arrays: [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tec
02-16 15:05:35.929 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: tag.toString(): TAG: Tech [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, android.nfc.tec
02-16 15:05:35.930 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: tag.getId() to hex f00f371e
02-16 15:05:35.930 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity:  nfcA.getTag().getTechList() Arrays: [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, and
02-16 15:05:35.930 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity:  prior to connect: nfcA.isConnected(): false
02-16 15:05:35.934 418-418/? W//system/bin/hw/android.hidl.allocator@1.0-service: ashmem_create_region(3840) returning hidl_memory(0x7a0662b310, 3840)
02-16 15:05:35.936 418-418/? W//system/bin/hw/android.hidl.allocator@1.0-service: ashmem_create_region(3840) returning hidl_memory(0x7a0662b310, 3840)
02-16 15:05:35.938 566-725/? E/volume_listener: check_and_set_gain_dep_cal: Failed to set gain dep cal level
02-16 15:05:35.939 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity:  after connect: nfcA.isConnected(): true
02-16 15:05:35.939 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity:  nfcA.getTag().getTechList() Arrays: [android.nfc.tech.NfcA, android.nfc.tech.MifareClassic, and
02-16 15:05:35.941 566-5010/? D/audio_route: Apply path: speaker-protected
02-16 15:05:35.941 32342-32342/com.example.mihaitarabuta.myapplication D/MifarePlus: CAPDU 6000
02-16 15:05:35.942 3415-3431/? E/NxpExtns: Mifare : phLibNfc_GetKeyNumberMFC returning = 0x1 Key = 0x0
02-16 15:05:35.946 566-5010/? D/audio_hw_primary: enable_snd_device: snd_device(95: vi-feedback)
02-16 15:05:35.946 566-5010/? D/audio_route: Apply path: vi-feedback
02-16 15:05:35.946 566-5010/? D/audio_hw_primary: enable_audio_route: usecase(24) apply and update mixer path: spkr-vi-record
02-16 15:05:35.946 566-5010/? D/audio_route: Apply path: spkr-vi-record
02-16 15:05:35.956 32342-32342/com.example.mihaitarabuta.myapplication D/MainActivity: java.io.IOException: Transceive failed
                                                                                        at android.nfc.TransceiveResult.getResponseOrThrow(TransceiveResult.java:52)
                                                                                        at android.nfc.tech.BasicTagTechnology.transceive(BasicTagTechnology.java:151)
                                                                                        at android.nfc.tech.NfcA.transceive(NfcA.java:120)
                                                                                        at com.example.mihaitarabuta.myapplication.MifarePlus.classicAuthKeyAStep1(MifarePlus.java:181)
                                                                                        at com.example.mihaitarabuta.myapplication.MainActivity.retrieveTagInfo(MainActivity.java:110)
                                                                                        at com.example.mihaitarabuta.myapplication.MainActivity.onNewIntent(MainActivity.java:76)
                                                                                        at android.app.Activity.performNewIntent(Activity.java:7011)
                                                                                        at android.app.Instrumentation.callActivityOnNewIntent(Instrumentation.java:1309)
                                                                                        at android.app.Instrumentation.callActivityOnNewIntent(Instrumentation.java:1321)
                                                                                        at android.app.ActivityThread.deliverNewIntents(ActivityThread.java:2932)
                                                                                        at android.app.ActivityThread.performNewIntents(ActivityThread.java:2948)
                                                                                        at android.app.ActivityThread.handleNewIntent(ActivityThread.java:2964)
                                                                                        at android.app.ActivityThread.-wrap14(Unknown Source:0)
                                                                                        at android.app.ActivityThread$H.handleMessage(ActivityThread.java:1667)
                                                                                        at android.os.Handler.dispatchMessage(Handler.java:106)
                                                                                        at android.os.Looper.loop(Looper.java:164)
                                                                                        at android.app.ActivityThread.main(ActivityThread.java:6494)
                                                                                        at java.lang.reflect.Method.invoke(Native Method)
                                                                                        at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:438)
                                                                                        at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:807)
```

Expected result:
transceive should return 4 bytes representing the TokenRB as per specs and inline with its contract/documentation

Personally, I think this issue is not within the javacode but rather in the jni code. Is there any way I can enable tracing for that?
There must be some handlers/callback functions that aren't right/used right. Perhaps some assumptions are made so that when a MifareClassic is detected, one must use only the MifareCla

Thank you

deleted
0 B

deleted
0 B

dn...@google.com <dn...@google.com> #4

As requested in comment #2, please share bugreport for further analysis.

sh...@gmail.com <sh...@gmail.com>

deleted
0 B

dn...@google.com <dn...@google.com> #5

We have passed this to the development team and will update this issue with more information as it becomes available.

sh...@gmail.com <sh...@gmail.com> #6

Hi there,
Any news from the dev team? I see it is blocked by some issue for which I do not have the relevant access permissions.
Would like to come to a resolution for my project and if you can give me some indication as to when/if will be addressed - that would be helpful for me.

Thanks

ji...@nxp.corp-partner.google.com <ji...@nxp.corp-partner.google.com> #7

first, if you send 6000, Android did recognize this command is a Mifare Auth command.
But before send 6000, you need to know which key the tag sector 00 is using. For your case, the default key used in Android didn't match, so an error returned.
Please use the authenticate() API defined in MifareClassic.java with right key for auth.

second, there is a fix I just post on AOSP, it will return the error code to application instead of throw an IOExeption.
https://android-review.googlesource.com/c/platform/packages/apps/Nfc/+/645208

sh...@gmail.com <sh...@gmail.com> #8

Hi there,
Thank you for looking into it. Really appreciate it. Unfortunately I don't know if this helps me a lot. Let me explain why.
On your comments:
"first, if you send 6000, Android did recognize this command is a Mifare Auth command".
"But before send 6000, you need to know which key the tag sector 00 is using. For your case, the default key used in Android didn't match, so an error returned. "

>>Actually I'm using the NfcA class. In principle Android should not even try to recognize this is a mifare auth command. Consequently should not try to match the key internally. Let the appli

"Please use the authenticate() API defined in MifareClassic.java with right key for auth."

>>If I use the MifareClassic class - it works on latest android - I have almost no issue with that. My problem is when I'm using the MifareClassicPlus type of cards. These cards support the M
and use transceive. But when I do that, some part of the android code is striping a byte from the card response.
According to my initial log that prompted me to open this ticket:
Using NfcA.transceive I'm sending this proprietary command:
02-14 15:39:16.947 2584-2584/? D/MifarePlus: CAPDU 760490
and getting back:
02-14 15:39:16.955 2584-2584/? D/MifarePlus: RAPDU 9005b89eed9873d28637997b185bc6ed length: 16
The problem with the response is that it is 1 byte short. I strongly suspect that the jni code is not solid enough to be able to really implement a transparent "transceive" when the MifareClassi

Is the fix you did addressing this issue ?
If so, can I get an android build for my Nexus 5x to test ?

Many thanks.

dn...@google.com <dn...@google.com> #9

Marked as fixed.

The development team has fixed the issue that you have reported and it will be available in a future build.

sh...@gmail.com <sh...@gmail.com> #10

Will this build be made available for nexus 5x? If not, what phone model do you recommend for me to test the fix?

According to this link updates may no longer come for nexus 5x...
https://support.google.com/nexus/answer/4457705?hl=en

Thanks