SEPolicychanegsinW

1.Revert "Add service wait override property for audioserver clients"

commit 6de5d5062f9265ab97a599fabe2d71307f74c9e2
Author: Priyanka Advani (xWF) <padvani@google.com>
Date: Fri Nov 15 18:18:47 2024 +0000

Revert "Add service wait override property for audioserver clients"

This reverts commit b95542e37de5c0b741b120b38c469990524dd06e.

Reason for revert: Droidmonitor created revert due to b/379306629. Will be verifying through ABTD before submission.

```
diff --git a/private/property_contexts b/private/property_contexts
index 3da6d7b73..58a18582a 100644
--- a/private/property_contexts
+++ b/private/property_contexts
@@ -426,9 +426,6 @@ audio.timecheck.disabled                u:object_r:audio_config_prop:s0
exact
 audio.timecheck.timeout_duration_ms       u:object_r:audio_config_prop:s0 exact int
 audio.timecheck.second_chance_duration_ms u:object_r:audio_config_prop:s0 exact int

-# Client wait timeout for audioserver before returning error (usually between 3000 to 10000).
-audio.service.client_wait_ms              u:object_r:audio_config_prop:s0 exact int
-
 # spatializer tuning
 audio.spatializer.priority              u:object_r:audio_config_prop:s0 exact int
 audio.spatializer.effect.affinity       u:object_r:audio_config_prop:s0 exact int
```

2.microdroid_manager: allow tcdain

commit 2ea821d5cca5d3dcf3b3f2f7c9a3b398264f73dc
Author: Frederick Mayle <fmayle@google.com>
Date: Thu Nov 14 18:01:44 2024 -0800

    Bug: 220071963
    Test: packages/modules/Virtualization/android/vm/vm_shell.sh start-microdroid

```
diff --git a/microdroid/system/private/microdroid_manager.te b/microdroid/system/private/microdroid_manager.
te
index 75c89bebc..96a05f774 100644
--- a/microdroid/system/private/microdroid_manager.te
+++ b/microdroid/system/private/microdroid_manager.te
@@ -129,7 +129,8 @@ allow microdroid_manager sysfs_zram:file rw_file_perms;
 allow microdroid_manager ram_device:blk_file rw_file_perms;

 # Allow microdroid_manager to read/write failure serial device
-allow microdroid_manager serial_device:chr_file w_file_perms;
+# tcdrain requires ioctl.
+allow microdroid_manager serial_device:chr_file { w_file_perms ioctl };

 # Allow microdroid_manager to handle extra_apks
 allow microdroid_manager extra_apk_file:dir create_dir_perms;
```

3.Renaming adaptive authentication selinux entries

commit 6f991b010170085b765e07a9a89913c5c91b3cd3
Author: Grace Cheng <graciecheng@google.com>
Date: Fri Nov 8 03:14:45 2024 +0000

```
    Renaming adaptive authentication selinux entries

    Renaming adaptive authentication selinux entries to
authentication
    policy due to renaming of service in ag/3040682

    Test: m -j
```

4.Allow rkp_cert_processor to call system_server and package_native.

commit 1454b4ccce693ee419525a90ccae8691dd4f6624
Author: Vikram Gaur <vikramgaur@google.com>
Date: Thu Nov 14 11:08:15 2024 +0000

Allow rkp_cert_processor to call system_server and package_native.

These services are necessary to check the presence of packages which may be required for RKP certificate post processing.

Bug: 361877215
Test: tested locally

```
diff --git a/private/rkp_cert_processor.te b/private/rkp_cert_processor.te
index 578bd4cb4..e5c9d0748 100644
--- a/private/rkp_cert_processor.te
+++ b/private/rkp_cert_processor.te
@@ -6,7 +6,10 @@ init_daemon_domain(rkp_cert_processor)
 net_domain(rkp_cert_processor)

 binder_use(rkp_cert_processor)
+binder_call(rkp_cert_processor, system_server)

 add_service(rkp_cert_processor, rkp_cert_processor_service)

 use_bootstrap_libs(rkp_cert_processor)
+
+allow rkp_cert_processor package_native_service:service_manager find;
```

5. Allow the payload to print logs

commit 256f21f700cfb27a3f46b55115b99798289753bf
Author: Sebastian Ene <sebastianene@google.com>
Date: Wed Nov 13 16:49:54 2024 +0000

```
    Allow the payload to print logs

    This fixes the SELinux denials when the payload tries to print a message
    on the console.

    Test: Start the EmptyPayload and make sure that we see the Hello
    Microdroid log.
    APP_EMPTY_PATH=$(adb shell "pm path
    com.google.android.microdroid.empty_payload | cut -d ':' -f 2")
    TEST_ROOT=/data/local/tmp/virt
    adb shell mkdir -p $TEST_ROOT
    adb shell /apex/com.android.virt/bin/vm run-app --debug full --log
    $TEST_ROOT/log.txt --console $TEST_ROOT/console.txt
${APP_EMPTY_PATH}
    $TEST_ROOT/EmptyPayloadApp.apk.idsig $TEST_ROOT/instance.img
    --payload-binary-name MicrodroidEmptyPayloadJniLib.so --instance-id-file
    $TEST_ROOT/instance_id
    Bug: 378479069
```

6.Add service wait override property for audioserver clients

commit b95542e37de5c0b741b120b38c469990524dd06e
Author: Andy Hung <hunga@google.com>
Date: Tue Nov 12 16:57:15 2024 -0800

```
    Add service wait override property for audioserver clients

    Flag: EXEMPT bugfix
    Test: compiles
    Bug: 375691003
```

7.Add test_pkvm_tee_service example tee service

commit 477e8f7ff07a6b811a0b183175ec897438697fce
Author: Nikita Ioffe <ioffe@google.com>
Date: Thu Oct 24 12:46:00 2024 +0000

> **Add test_pkvm_tee_service example tee service**
>
> **It can be used to test that custom smcs filtering is correctly integrated on devices with pkvm hypervisor.**
>
> **Bug: 360102915**
> **Test: vm run-microdrodid --tee_services test_pkvm_tee_service**
> **Test: builds**

8.Add plumbing for new tee_service_contexts

commit 48966b6105be61ea89f42310532582a2059f2b89
Author: Nikita Ioffe <ioffe@google.com>
Date: Tue Oct 22 14:01:17 2024 +0000

> **Add plumbing for new tee_service_contexts**
>
> **This will be used to enable some VMs to issue custom vendor-defined SMCs. On the Android host side, the allow list of what VMs can access what SMC services via selinux. In short the implementation will look like these:**
>
> *** new tee_service_contexts defines all SMC services available to VMs and their mapping to selinux labels**
> *** sepolicy defines what VMs can access what SMC services. The access control is defined at the "VM owner process" (i.e. process using AVF APIs to start a VM).**
> *** virtmngr will enforce the access control by reading the mapping from /system/ect/selinux_tee_service_contexts and the using selinux_check_access function from libselinux to check if the VM owner is allowed to access requested SMC services.**
>
> **Since SMC is an arm concept, we use a more generic "tee_service" name to define it.**
>
> **More information available at go/pkvm-pvm-allow-vendor-tz-services-access**
>
> **Follow up patch will define an example tee_service that can be used to test these feature end-to-end.**
>
> **Bug: 360102915**
> **Test: build & flasg**
> **Test: adb shell ls -alZ /system/etc/selinux/tee_service_contexts**

9.Add an adb_tradeinmode type for restricted adbd.

commit c5e4033d8039d0b4ed936c7fea0ead2b1adbaf74
Author: David Anderson <dvander@google.com>
Date: Fri Oct 11 08:58:23 2024 -0700

> **Add an adb_tradeinmode type for restricted adbd.**
>
> **This adds sepolicy for a super restricted adbd mode. Currently, this mode has just enough permissions to handle adb connection.**
>
> **It also adds a new property, persist.adb.tradeinmode, which can be used to enter this restricted version of adbd.**
>
> **Test: manual test**
> **Bug: 307713521**
> **Bug: 375954854**
> **(cherry picked from https://android-review.googlesource.com/q/commit:3fce5ad00269b135ddcb8fc20e3641a681d46028)**

10. Add com.android.nfcservices-file_contexts to Android.bp

commit 6854dd7187d34259db0f25fdf1346e11acaa2f5e
Author: Roshan Pius <rpius@google.com>
Date: Mon Nov 11 18:01:12 2024 +0000

```
    Add com.android.nfcservices-file_contexts to Android.bp

    Bug: 355312096
    Change-Id:
Ifc97894e89825d4d3fceb4172601410441f0ab45
    Test: Compiles

diff --git a/apex/Android.bp b/apex/Android.bp
index 304eb85c4..0374b6285 100644
--- a/apex/Android.bp
+++ b/apex/Android.bp
@@ -155,6 +155,13 @@ filegroup {
     ],
 }

+filegroup {
+    name: "com.android.nfcservices-file_contexts",
+    srcs: [
+        "com.android.nfcservices-file_contexts",
+    ],
+}
```