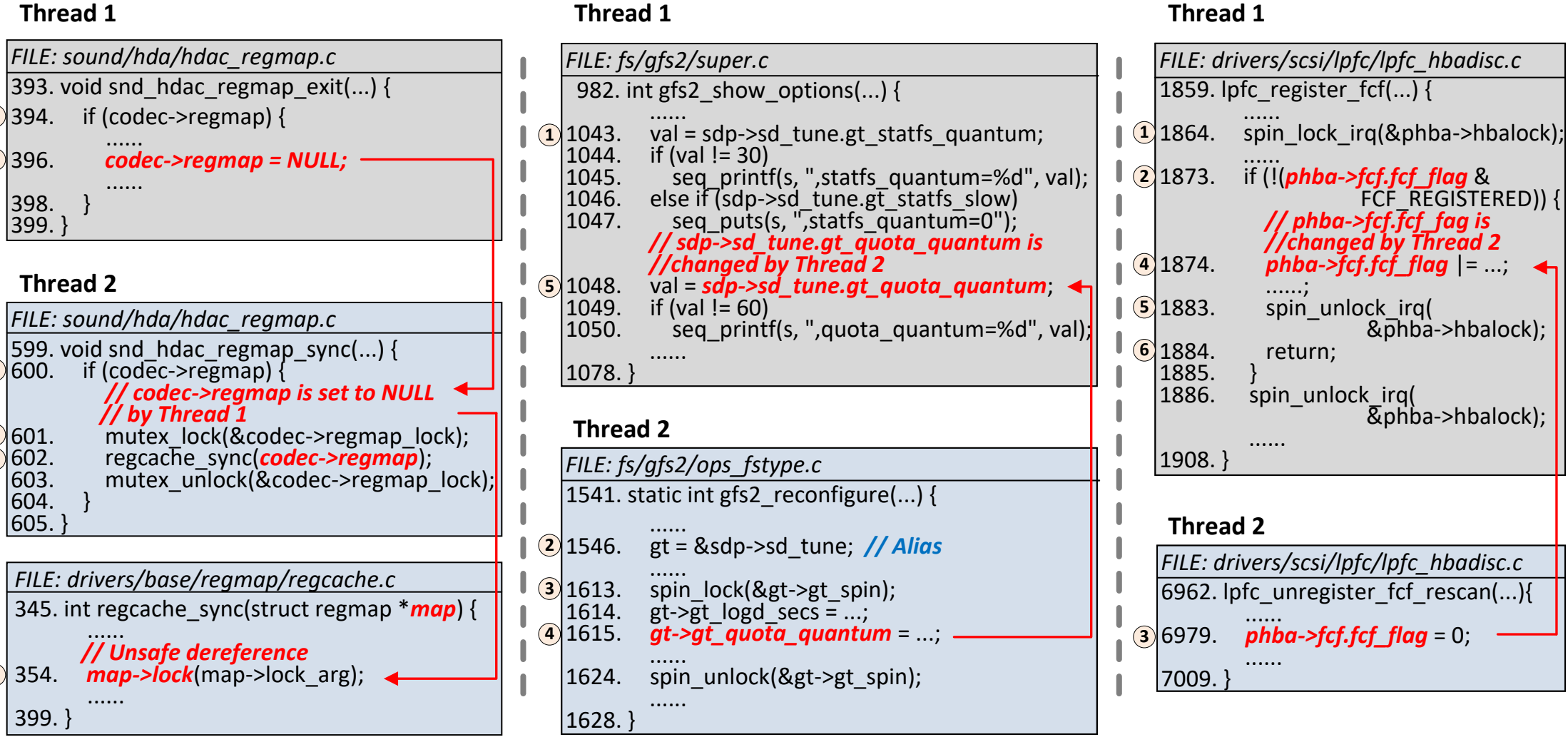
Thread 1
FILE: sound/hda/hdac_regmap.c
393. void snd_hdac_regmap_exit(...) {
2 394. if (codec->regmap) {
.....
3 396. codec->regmap = NULL;
.....
398. }
399. }
Thread 2
FILE: sound/hda/hdac_regmap.c
599. void snd_hdac_regmap_sync(...) {
1 600. if (codec->regmap) {
// codec->regmap is set to NULL
// by Thread 1
4 601. mutex_lock(&codec->regmap_lock);
5 602. regcache_sync(codec->regmap);
603. mutex_unlock(&codec->regmap_lock);
604. }
605. }
FILE: drivers/base/regmap/regcache.c
345. int regcache_sync(struct regmap *map) {
.....
// Unsafe dereference
6 354. map->lock(map->lock_arg);
.....
399. }
(a) Null-pointer dereference in the HDA driver
Thread 1
FILE: fs/gfs2/super.c
982. int gfs2_show_options(...) {
.....
1 1043. val = sdp->sd_tune.gt_statfs_quantum;
1044. if (val != 30)
1045. seq_printf(s, ",statfs_quantum=%d", val);
1046. else if (sdp->sd_tune.gt_statfs_slow)
1047. seq_puts(s, ",statfs_quantum=0");
// sdp->sd_tune.gt_quota_quantum is
//changed by Thread 2
5 1048. val = sdp->sd_tune.gt_quota_quantum;
1049. if (val != 60)
1050. seq_printf(s, ",quota_quantum=%d", val);
.....
1078. }
Thread 2
FILE: fs/gfs2/ops_fstype.c
1541. static int gfs2_reconfigure(...) {
.....
2 1546. gt = &sdp->sd_tune; // Alias
.....
3 1613. spin_lock(&gt->gt_spin);
1614. gt->gt_logd_secs = ...;
4 1615. gt->gt_quota_quantum = ...;
.....
1624. spin_unlock(&gt->gt_spin);
.....
1628. }
(b) Data inconsistency in the GFS2 file system
Thread 1
FILE: drivers/scsi/lpfc/lpfc_hbadisc.c
1859. lpfc_register_fcf(...) {
.....
1 1864. spin_lock_irq(&phba->hbalock);
.....
2 1873. if (!(phba->fcf.fcf_flag &
FCF_REGISTERED)) {
// phba->fcf.fcf_fag is
//changed by Thread 2
4 1874. phba->fcf.fcf_flag |= ...;
.....;
5 1883. spin_unlock_irq(
&phba->hbalock);
6 1884. return;
1885. }
1886. spin_unlock_irq(
&phba->hbalock);
.....
1908. }
Thread 2
FILE: drivers/scsi/lpfc/lpfc_hbadisc.c
6962. lpfc_unregister_fcf_rescan(...){
.....
3 6979. phba->fcf.fcf_flag = 0;
.....
7009. }
(c) Double fetch in the LPFC SCSI driver