Scenario 3 - Huge Trove and Redistribution TCR attack

Attack outline

- Underwater Troves at CR < MCR exist, witch total underwater debt d_A greater than the funds in the SP
- Attacker opens huge low CR trove, drops TCR to ~CCR
- Attacker liquidates the underwater Troves and causes redistribution, with or without SP offset (If the SP has funds it must be very small relative to underwater Trove debt for a net TCR reduction here: the TCR drop from the removal of the gas compensation collateral has to be greater than the TCR increase from the closing of the the Troves that get offset against the SP)
- The redistribution triggers RM
- Attacker deposits again to the (empty) Stability Pool
- Attacker liquidates some Troves (other than his) which have CR < CCR
- Attacker repays his Trove to bring TCR > CCR
- Attacker closes his Trove

b: ratio of huge Trove debt to system initial debt
D: Initial total system debt
C: initial total collateral
d_T: Debt of Trove that attacker opens to drag TCR to ~CCR
S: total LUSD in SP before liquidation 1
d_A: total underwater debt before attack i,e. with CR_A = MCR
k: Initial ratio of SP to total debt
s: Attacker's share of SP before liquidation 1
f: Initial ratio of underwater debt to total debt i.e. $0<f<=1$
h: Fraction of outstanding LUSD supply that attacker owns and deposits to SP after liquidation 1 and redistribution
q: Fraction of debt liquidateable after redistribution and RM

Attack constraints

1. **Underwater Troves must exist,** i.e the underwater debt $d_A > 0$.

2. **Redistribution must drag TCR down below CCR**. This boils down to a constraint on the ratio of the SP size S to the total debt liquidated d_A. We can derive this constraint:

Assume the state before redistribution has the system with total collateral C and total debt D at TCR = CCR:

1) $C / D = CCR$

Collateral c_l and debt d_l is liquidated. This liquidation is split across the SP (subscript s) and redistribution (subscript r). So:

2) $c_l = c_s + c_r$

3) $d_l = d_s + d_r$

Assuming liquidation occurs at the MCR, then both liquidation parts have effective collateral ratios equal to MCR:

4) $c_s/d_s = MCR$

5) $c_r/d_r = MCR$

Gas compensation pays out 1/200 of the collateral liquidated i.e. c/200.

However, when liquidations are offset with the Stability Pool the corresponding collateral c_s is removed from the system (those Troves are closed), and the gas compensation for the offset part is also taken out of this collateral c_S.

So we only need to explicitly account for the gas compensation coming from the part of the liquidation that is redistributed

Let C' and D' be total system coll and debt after the liquidation, respectively. C' is given by:

6) $C' = C - c_s - c_r/200$

And the total system debt is reduced only by the offset debt, i.e:

7) $D' = D - d_s$

And the condition for the TCR drop below CCR is:

8) $C' / D' < C/D$

i.e.

9) $(C - c_s - c_r/200) / (D - d_s) < C/D$

So:

10) $- c_s - c_r/200 < -Cd_s/D$

i.e.

11) $c_s + c_r/200 > Cd_s/D$

Rewriting collateral parts in terms of their corresponding debt and collateral ratios:

12) $MCR\ d_s + MCRd_r/200 > CCRd_s$

13) $(CCR - MCR)d_s < MCRd_r / 200$

This gives a ratio between the SP offset amount and the redistributed amount:

14) $d_S < MCRd_r / 200\ (CCR - MCR)$

For a ratio of the SP offset d_s to total liquidated debt d_l, we can rewrite it:

15) $d_S < MCR\ (d_l - d_s) / 200\ (CCR - MCR)$

i.e.

16) $d_s\ (1+ MCR/200(CCR - MCR)) < MCR\ d_l / 200\ (CCR - MCR)$

For simplicity let A = MCR and B = 200(CCR - MCR). Then

17) $d_s\ (1+ A/B) < A\ d_l/B$

18) $d_s < Ad_l/B(1+A/B)$

19) $d_s < Ad_l\ /(B + A)$

20) $d_s < MCR\ d_l / (MCR + (CCR - MCR)200)$

Giving us the ratio of the SP offset debt to the total debt liquidated.

Let's plug in our constants for Liquity i.e. MCR = 1.1 and CCR = 1.5:

21) $d_s < 1.1\ d_l / (1.1 +80)$

22) $d_s <11\ d_l\ / 811 \sim= 0.0136\ d_l$

So the SP offset must not be larger than 11 / 811 (1.36%) of the total liquidated debt.

We can turn this into a relation between the SP fraction of total debt (k), and the underwater fraction of total debt (f). We have d_s = kD and d_l = fD, so:

23) ds<11 dl / 811
24) kD <11 fD / 811

So

25) $k < 11f / 811$

An underwater fraction f of (say) 20% then gives us $k < 11f / 4055$, i.e. $k < 0.27\%$.

That is, the SP must be a very small fraction of total system size - likely well under 0.5%, depending on underwater debt - in order for the liquidation to drop the TCR below CCR.

3. Attacker must be able to close their Trove

This seems fairly easy since they hold the LUSD they borrowed from it. They just have to obtain an extra 0.5% of their debt (borrow fee) and whatever debt their Trove received in redistribution, which could be a few extra percent on top of their initial debt.

The conservative assumption is that these extra amounts are always obtainable. The redistribution itself only increases their profit (since it is a net gain).

4. Capital requirements - bringing TCR to ~CCR by opening a Trove

The attacker opens a Trove to bring the TCR down close to the CCR such that the subsequent redistribution will pull it below.

They need to drag it down to within some percentage point margin m such that the subsequent redistribution drags TCR < CCR due to the payout of the gas compensation collateral.

The exact value of m depends on the underwater debt, but we can conservatively assume m is no bigger than 1%, since only 0.5% of collateral gets paid out in gas compensation.

We have the initial system state with collateral C and debt D:

26) $C / D = TCR_{initial}$

And the post-condition after the attacker opens Trove with collateral c_T and debt d_T is that the TCR drops to within m of the CCR:

27) $(C + c_T)/ (D + d_T) = CCR + m$

The attacker’s Trove collateral ratio is at the MCR:

28) $c_T / d_T = MCR$

Using 26) and 28) in 27):

29) $(TCR\ D + MCRd_T) / (D + d_T) = CCR + m$

Rearrange and expand:

30) $DTCR + MCRd_T = DCCR + Dm + d_TCCR + d_Tm$

Collecting terms:

31) $D(TCR - CCR - m) = d_T(CCR - MCR + m)$

i.e.

32) $b = (TCR - CCR - m)/(CCR - MCR + m)$

This gives us the attacker's debt as a fraction of initial system size which is needed to drop the TCR to within m of the CCR. Plotted here: https://www.desmos.com/calculator/uyvnuvqtoe

At 250% TCR and m = 0, the attacker needs to open a Trove with 2.5x the initial system debt.

Profitability derivation

Attacker costs:
The Borrow fee for the huge Trove is 0.5%.

From above, the Trove size needed to drag down to the ~CCR is a function of the TCR (see 32).

So , the attacker's cost as a function of initial system debt is:

33) $cost = D * (TCR - CCR - m)/(200(CCR + m - MCR))$

m is the max buffer above CCR at which drag down to from redist. can occur. The lower m the greater the fee, so larger m → more profit. A conservative value for m is 1% since only 0.5% of liquidated collateral gets removed at redistributions.

Attacker gains

The attacker gains:

34) liq_1_SP_gain + liq_1_redistribution_gain + liq_1_gas_comp + liq_2_SP_gain + liq_2_gas_comp

Liquidation 1

The **SP gain** is given by their share of the SP multiplied by collateral surplus of liquidated Troves i.e:

35) liq_1_SP_gain = 0.1sS = 0.1skD

And the gas compensation is given by:

36) liq_1_gas_comp = 1.1d_A/200 = 1.1fD/200

Since the attacker has a huge Trove in the system, they also make a net gain from **redistribution**. The attacker's trove has debt bD and thus collateral 1.1bD.

The total system debt after they open the Trove is:

37) D(1+b)

and thus total system collateral is:

38) TCR*D(1+b).

In a redistribution, active Troves receive shares of the liquidation in proportion to their collateral.

That is the attacker's share of the redistribution J_1 is given by:

39) J_1 = attacker_active_coll_1 / total_active_coll_1

The denominator must exclude the collateral of the liquidated Trove. That is:

40) total_active_coll_1 = TCR*D(1+b) - 1.1fD

So:

41) J_1 = 1.1b / [TCR*(1+b) - 1.1f]

And using 27) for the TCR:

42) J_1 = 1.1b / ((CCR + m)(1+b) - 1.1f)

The underwater debt fD gets liquidated, with S offset against the SP - so fD - S gets redistributed. Assuming liquidation at MCR, the net gain from this Trove is then 0.1(fD-S), i.e. 0.1D(f-k).

Now, the huge Trove receives a share of this net gain, proportional to its share of system collateral. So the huge Trove receives:

43) liq_1_redistribution_gain = 0.1D(f-k)J_1

And we already have the expression for b - the ratio of the huge trove to initial system debt (i.e. d_T / D) - given by 32).

Liquidation 2

The total debt after liquidation 1 is D - S, i.e. D(1-k).

After redistribution, some portion of remaining system debt is liquidateable, with aggregate CR < CCR. Let the fraction be q, i.e. qD(1-k) is liquidateable.

The attacker owns a fraction h of the remaining LUSD supply, i.e. hD(1-k), and deposits this to the SP. Since a redistribution occurred in liquidation 1, the attacker is now the only depositor in the SP.

Their **SP gain** is their deposit multiplied by 0.1. This gain is the based on the minimum of liquidateable debt and the fraction of remaining LUSD supply they hold, i.e.

44) liq_2_SP_gain = 0.1min(h, q)D(1 - k)

A second **redistribution** occurs if q > h, i.e. if the liquidated amount is greater than the attacker's SP deposit.

So the redistributed debt is max(q-h, 0)D(1-k), and the total net gain for all active troves from redistribution is

45) total_net_gain_redistribution_2 = 0.1max(q-h, 0)D(1-k).

*(Note: the liquidation in RM can have an aggregate CR > 1.1, but the system caps the net gain from such liquidations at 0.1 * debt).*

The attacker gets a share of this pro-rata to their active Trove collateral.

The attacker's active trove collateral is given by its initial collateral plus its gain from redistribution 1:

46) attacker_active_coll_2 = 1.1bD + 1.1(fD-S)H_1

The total system collateral is now:

47) total_active_coll_2 = D[(CCR + m)(1+b) - 1.1k - r_qq(1-k)]

That is, it's equal to the total_active_coll_1 (equation 40), minus the collateral removed by liquidation 1 against the SP and minus the current liquidateable coll.

r_q here is the collateral ratio of the liquidateable Troves. Since the system is in RM, then 1.1 < CR_q <1.5, and we parameterize this metric.

The attacker's share of redistribution 2 is given by:

48) J_2 = attacker_active_coll_2 / total_active_coll_2

49) J_2 = (1.1b + 1.1(f-k)J_1] / [(CCR + m)(1+b) - 1.1k - r_qq(1-k))

Then, using total_net_gain_redistribution_2 (eqn 45), the attacker gets the following net gain from the redistribution:

liq_2_redistribution_gain = 0.1max(q-h, 0)(1-k)J_2

Profit equation

Their profit is given by:

39) profit = liq_1_SP_gain + liq_1_redistribution_gain + liq_1_gas_comp + liq_2_SP_gain + + liq_2_redistribution_gain + liq_2_gas_comp - cost

40) profit = D[0.1sk + 0.1(f-k)J_1 + 1.1f/200 + 0.1min(h, q)(1 - k) + 0.1max(q-h, 0)(1-k)J_2 + 1.1q(1-k)/200 - (TCR - CCR - m)/200(CCR + m - MCR)]

Plotting it:
https://www.desmos.com/calculator/4ylcnyyv6r

Variant: attacker creates underwater debt

The attacker could create the underwater debt themselves. Doing so has two potential advantages:

- It gives the attacker more flexibility with timing - they need not wait for other Troves to drop below MCR.

- By controlling the underwater debt fraction, they are able to cause a TCR drop from redistribution for a larger relative SP size.

Let's see if/when it's profitable:

The attacker no longer profits from liquidation 1 since the underwater debt is all theirs. In fact they lose the collateral surplus, but regain part of it through their initial position in the SP, the redistribution and the gas compensation.

So their net gain from liquidation 1 is:
$-0.1fD + 0.1skD + 0.1D(f-k)J_1 + 1.1fD/200$

They also pay the borrow fee on the Trove they open, i.e. fD/200 (Hence, the gas compensation on the underwater debt cancels the borrow fee).

The profit equation becomes:

42) profit_attacker_creates_underwater_debt =
$D[\ \underline{0.1sk - 0.1f + 0.1(f-k)J_1 + 1.1f/200} + 0.1\min(h, q)(1 - k) + 0.1\max(q-h, 0)(1-k)J_2 +$
$1.1q(1-k)/200 - (TCR - CCR - m)/200(CCR + m - MCR) \underline{-\ f/200]}$

i.e.

43) profit_attacker_creates_underwater_debt =
$D[\underline{0.1sk - 0.1f + 0.1(f-k)J_1 + 0.1f/200} + 0.1\min(h, q)(1 - k) + 0.1\max(q-h, 0)(1-k)J_2 +$
$1.1q(1-k)/200 - (TCR - CCR - m)/200(CCR + m - MCR)]$

Plotting it:
https://www.desmos.com/calculator/t3sfcnsbfb

We see that now the profitable range depends on f in a non-linear way - increasing f first increases, but then decreases, the profitable range.

The profit is still very sensitive to q: the fraction of remaining debt that gets dragged down below CCR.

For q=0.1 (i.e. an unlikely/conservative/high fraction), the attack is only profitable for underwater debt up to ~11%.

So by 25) we have a minimum SP size in order to mitigate the attack, i.e. 11/811 * 0.11 =~0.15% of system size for q = 0.1.

Analysis of the attack

- A fairly large profitable attack ranges exists (up to 235% TCR) for a fairly low underwater debt fraction (0.1%) and some conservative dragged-down fraction q=10%. Therefore a fairly small underwater debt could be the catalyst for the attack, if the SP is empty or small enough such that the majority of it gets redistributed.

- At initial TCR of 250%, the attacker needs to open a Trove with 2.5x initial system debt, but the attack can all be done in 1 transaction and so they could use a flash loan for the capital.

- Realistic profits seem to be in the range of 2-3% of initial system debt i.e. order-of-magnitude higher than typical flash loan fees (e.g. ~0.1%).

- The attacker doesn't need a high initial share of the SP since most of their gain comes from the second liquidation in RM.

- Once RM is triggered, some fraction of remaining system debt becomes liquidateable (q). For even relatively small values of q, the attack is profitable at relatively healthy TCRs - e.g. for q = 10% and f = 5%, the attack is profitable at 255% TCR, and for q = 5%, it's profitable at 206% TCR.

- The attack can only be performed when the SP is a very small fraction of the underwater debt - 11/811.

- For realistic underwater debt values (i.e. <30% of total system debt) this means that the attack can only work when the SP is a very small fraction of total system debt, i.e. < 0.5%.

- The attacker has to beat other liquidators chasing the underwater debt, though would probably be willing to pay much more in gas / Flashbots fee as the attack allows them to extract larger profits

- Alternatively, the attacker could create the underwater debt themselves. This gives the attacker more flexibility with timing - they need not wait for other Troves to drop below MCR. For a drag-down fraction q=10%, the attack is profitable for up to ~11% underwater debt, which means the SP needs to be >0.15% of system size.

Conclusions

The attack is only possible when SP is < 11/811 (~1.3%) of system size in the worst case, but it can then be profitable and risk free for even pretty healthy initial TCRs.

If we assume roughly that the SP size would follow the LQTY rewards and halve in size every year, then starting at 55% of system size, it'd fall below 1.3% of system size at $60/2^6$, i.e. within about 6 years from now (01/2024).

As long as the SP remains at >1.3% of system size, then attack is not possible.

Ultimately, the borrowers that keep their Trove above 150% CR will be safe from liquidation in Recovery Mode (unless they're unlucky enough to get dragged down below 150% by the redistribution, but that's a low risk for realistic levels of underwater debt).