TCR Sandwich attack

Definitions

Collateral ratio: the ratio of the value of a quantity of ETH collateral to its corresponding LUSD debt
CR: Collateral ratio of an individual trove
TCR: Total collateral ratio of the Liquity system
CCR: TCR threshold at which Liquity enters Recovery Mode - 150%.
MCR: Minimum collateral ratio for an individual trove - 110%.

Tables and graphs are found in this spreadsheet:

https://docs.google.com/spreadsheets/d/12giKKXbwFqnYNALW-bQKUWr9N_zhXSoQwdCnr8t-0Vo/edit?usp=sharing

Attack Description

First, the attacker waits for a significant price drop - i.e. a Chainlink price update transaction.

The Attacker provides the following sandwich transaction bundle to a miner:

- Open a huge 110% CR trove which pulls the TCR close to 150%.
- Deposit the borrowed LUSD into the Stability Pool.
- Chainlink price update - which causes the system to enter Recovery Mode
- Batch liquidate as many troves below 150% as possible until the system leaves recovery mode, optimizing the liquidation order to maximize the liquidated ETH
- Withdraw the stability deposit
- Close the trove

The attacker pays:

- Borrowing fee
- Gas costs

and earns:

- Liquidation gas compensation
- Stability Pool ETH gain

resulting in a net profit.

Attack Channels

The sandwich attack can be performed via Flashbots or similar protocols.

The attack is not feasible via the public gas auction, as although the attacker could front run the price update, they could not guarantee the ordering of transactions after the price update and they would therefore run a significant risk of their trove being liquidated by someone else.

Attack profitability

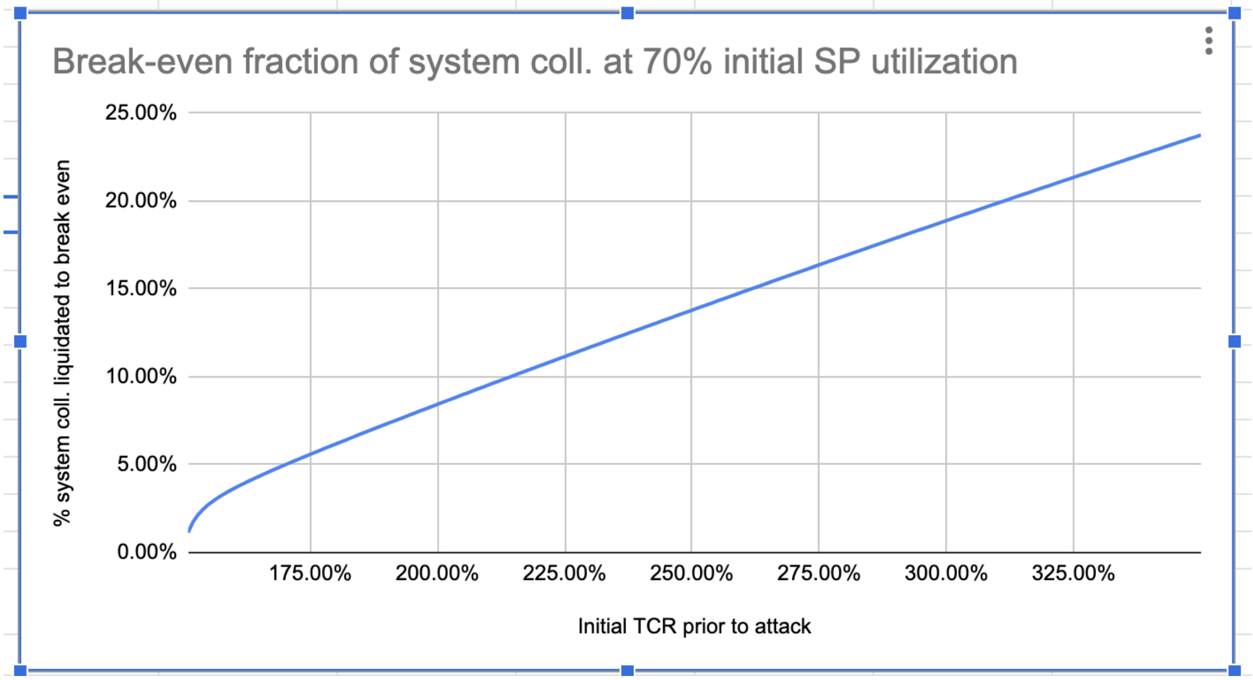
The profit calculator is found in this table:
https://docs.google.com/spreadsheets/d/12giKKXbwFqnYNALW-bQKUWr9N_zhXSoQwdCnr8t-0Vo/edit?usp=sharing

The input params in blue can be varied to calculate profitability for different scenarios.

The higher the initial TCR, the larger the attacker’s Trove (relative to system size) needs to be in order to bring the TCR to 150%.

However, the larger the attacker’s trove, the larger their borrowing fee - and so the more collateral the attacker needs to liquidate to break even.

The attacker’s break-even liquidation volume can be plotted as a function of the initial system TCR and for a given initial Stability Pool utilization prior to the attack:



We can hence track the TCR, the Stability Pool utilization and the vulnerable collateral, and thus know whether an attack would be profitable at a given point in time.

Upper bound on vulnerable collateral

The upper bound on vulnerable collateral is found to be the fraction of the system that is under 150% CR after the price drop occurs. We label this fraction **q**.

In practice, the vulnerable collateral may be less than this upper bound, due to the fact that the liquidation sequence terminates once enough collateral has been removed to raise the TCR above 150%

Thus, the rational attacker solves an optimization problem. They attempt to maximize their profit, subject to constraints:

- The distribution of collateral across the troves that are under 150% CR
- The maximum number of troves that can be liquidated given the block gas limit and the gas costs of their bundle transactions

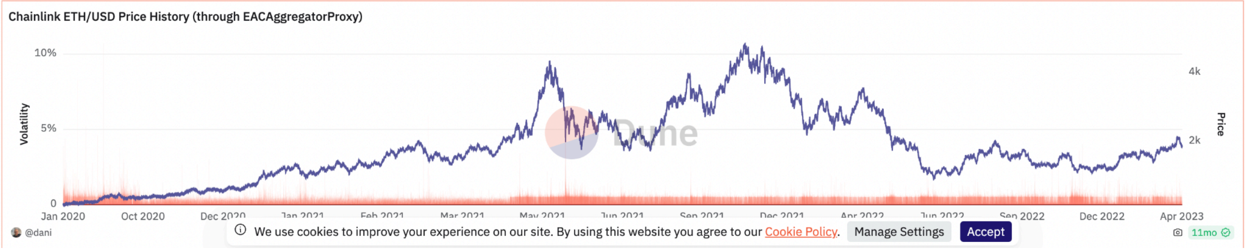
They also gain a “freebie” liquidation due to the fact that the last trove in the liquidation sequence may bring the TCR above the CCR. Rationally, they would put a large trove at the end of the sequence.

The amount the attacker can liquidate before bringing the TCR above 150% also depends on the TCR immediately after the price drop - the lower the TCR, the more the attacker can liquidate before the TCR rises above the CCR and the liquidation sequence exits.

How large can Chainlink price drops be?

Historical Chainlink price update volatility can be found here:

https://dune.xyz/queries/266838



Chainlink ETH/USD Price History (through EACAggregatorProxy)

We use cookies to improve your experience on our site. By using this website you agree to our Cookie Policy.

We see that the price tends to change by >1% a few times per month, but is nearly always well under 5%.

See Table 2 for estimates of the maximum liquidateable amount given an initial TCR. A collateral-weighted average CR is used to simplify the calculation.

Generally, for larger price drops, the attacker may be able to liquidate **q**. For smaller price drops well under 1%, they may only be able to liquidate **< q**.

A definitive analysis is difficult as it also depends on the distribution of collateral across troves at < 150% CR. Therefore we take the fraction **q** as the upper bound on vulnerable collateral.

Is there a safe maximum trove size?

Liquidation gas costs restrict the number of liquidated troves to 120-170, if a liquidation transaction were to fill the block.

Since the attacker needs to include other transactions in their bundle - borrow, deposit, price update, withdraw - the maximum number of liquidated troves will be fewer - around 100-150.

For a given amount of vulnerable collateral we can easily compute a maximum trove size above which the attack is not profitable - see Table 3.

However, it only takes **one** trove above this size to make liquidating a series of troves potentially profitable. Given this, it would be difficult to coordinate borrowers to stay below the maximum safe size - one large risk taker could put many others at risk.

Impact: borrower losses and attacker profits

Liquidations in Recovery Mode seizes a maximum of `1.1 * debt` worth of ETH. Thus, the maximum net loss for a liquidated borrower is `0.1 * debt.`

Systemically, the maximum potential loss for borrowers is given by
`0.1 * totalSystemDebt *` **`q`**

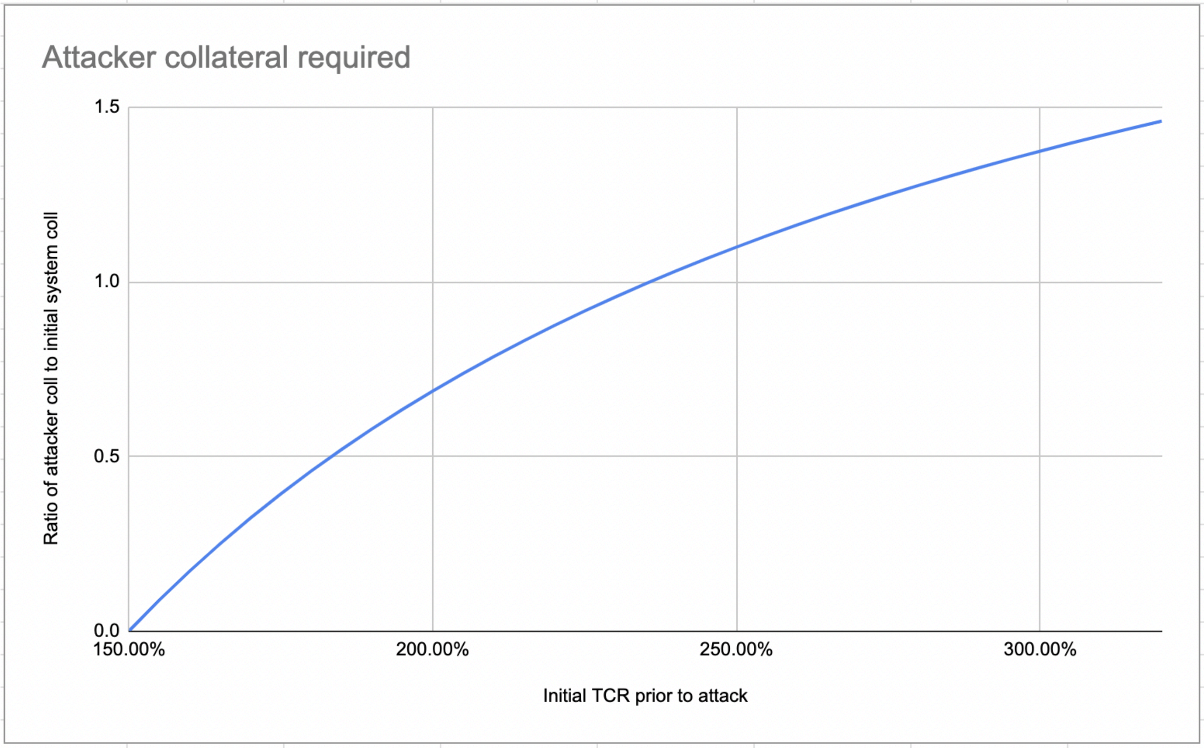
Not all of this value is extracted by the attacker as profit though. Some value is directed to LQTY stakers (borrow fees), and some is captured by other Stability Pool depositors.

Once performed, the attack could not likely be repeated - borrowers would be strongly deterred from keeping an individual CR below 150%. The fraction of vulnerable collateral would be greatly reduced, which would likely make further attacks unprofitable.

Attacker capital requirement

The capital required to reduce the TCR to 150% depends on two factors:

- Liquity system size prior to attack
- TCR prior to attack



At 250% TCR, the attacker would need ~1.2x the total system collateral. At lower TCRs, the attacker needs less capital.

At a very low TCR of 155%, an attacker would need 0.1x the total collateral. For a system with significant TVL (i.e. hundreds of millions of USD worth of ETH), the attacker's required capital is still large - e.g. a USD value in the tens of millions.

Attacker's risk

Since the attack involves separate transactions, upfront capital is needed (rather than a flash loan), and therefore the attack is not risk-free.

Technically, there is a chain re-org risk: it could be that only the attacker's borrow transaction gets validated, and not their liquidation and/or withdrawal transactions. The attacker is then exposed to liquidation risk, and a potential net loss, after the price update transaction is mined.

In the 30 days preceding 11/04/2024 there were ~700 blocks forked:
https://etherscan.io/blocks_forked

Given an average block time of 12 seconds, that yields around `3600*24*30/12 = 216000` blocks produced per month.

Therefore, `700/216000` blocks were forked in the past 30 days, i.e. around 0.3%. Once a block is broadcast, its transactions are public and any block builder could include only the attacker's first transaction, and include their own liquidation transaction after the price drop, to liquidate the attacker.

This poses a significant risk and deterrent to the would-be attacker.

There is also even a risk that the attacker's intended validator double-crosses them in the same manner. Rogue validators in Flashbots get banned, but if the profit is large enough they may be tempted.

The attacker would need a large amount of capital - as mentioned above, even at a low TCR of 155%, for a significant system size ($500m+ TVL) they would need $50m+ worth of ETH to open a trove at 110% CR. A Chain re-org or validator double-cross would expose them to up to a ~10% loss, i.e. $19m, depending on their share of the Stability Pool.

An attacker with sufficient capital takes on not only financial risk, but also potential legal and reputational risk - since the attack itself can be considered an exploit. This would likely deter many regulated and/or publicly identifiable actors.

Likelihood of Attack

The attack would require significant preparation, and funds would need to be kept ready to be deployed at very short notice. The attacker must also have patience in waiting for a significant price drop.

Summary

- The upper bound on vulnerable collateral is **q,** the fraction of system collateral at <150% CR after the price drop.

Attack profitability depends on:

- **q**: there is a break-even threshold for a given TCR
- Initial TCR: lower -> higher profits
- Initial Stability Pool size: larger -> lower profits
- Borrowing fee: higher -> lower profits

Factors that can reduce the vulnerable collateral q:

- Distribution of collateral across troves in the <150% range: more collateral at lower CRs -> less can be liquidated before returning the TCR to above 150%

- Percentage by which the price drops: a lower price drop -> TCR after price drop is closer to 150% -> less can be liquidated before bringing the TCR to above 150%

- Sizes of troves at <150% CR: when the low-CR Troves are small enough -> the block gas limit constrains the amount that can be liquidated

Attacker's capital requirement depends on:

- System size
- Initial TCR

Risk:

- Attacker takes on financial risk as well as potential reputational and legal risk.

Implications for users

As recommended by Liquity comms and docs since system launch, borrowers should be aware of the importance of maintaining a CR of >150% to be safe from liquidation.

Borrowers with Troves at <150% CR should understand that whales have a big influence on the TCR, and they risk being liquidated in Recovery Mode if it were to be suddenly triggered.

Monitoring and Analytics

It's possible to keep track of the TCR, the Stability Pool size, and **q,** the fraction of system collateral below 150% CR - and therefore, know when a profitable attack is possible based on the break-even threshold.

Given that it's the fraction of system collateral <150% *after* the price drop that matters, we add a buffer for the potential price drop for monitoring purposes. If we track the fraction of system coll <160%, that would correspond to the fraction of coll <150% after a 6.25% price drop (an estimated upper bound on the Chainlink price drop given historical values).

We have thus created a Dune query (https://dune.xyz/queries/270161/508325) that shows the current fraction of collateral below 160% and have set up automated alerts using Forta.