IETF 122 Hackathon

VRO: Verifiable Routing Origins via AS Cooperations

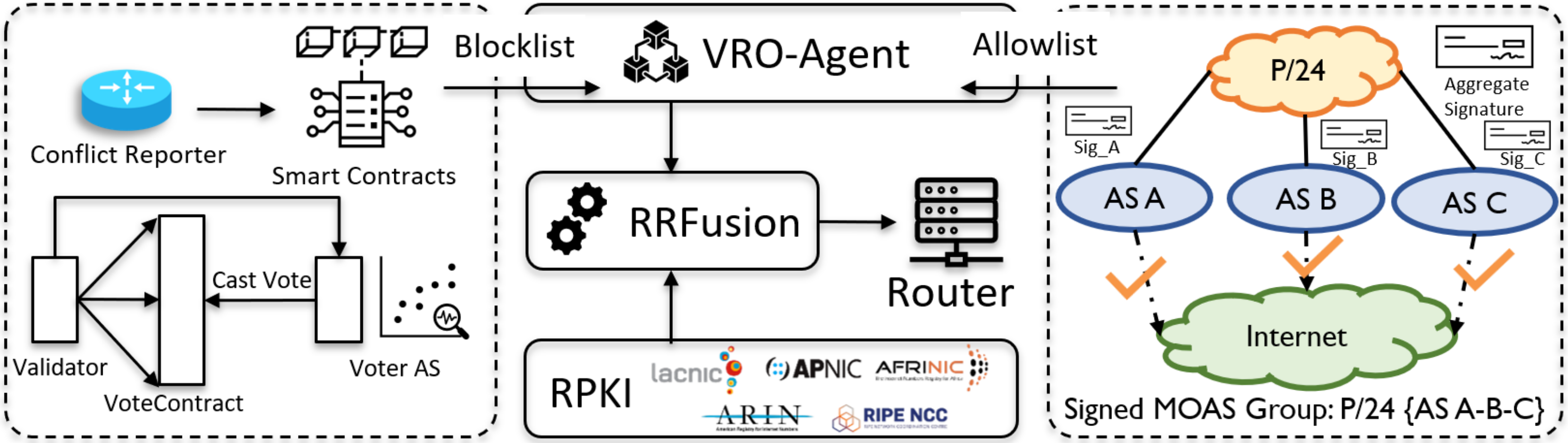
March 15-16, 2025， Bangkok

Members: Qi Li, **Shenglin Jiang**
Zhongguancun Laboratory

I E T F

How to distinguish legitimate MOAS from malicious attacks

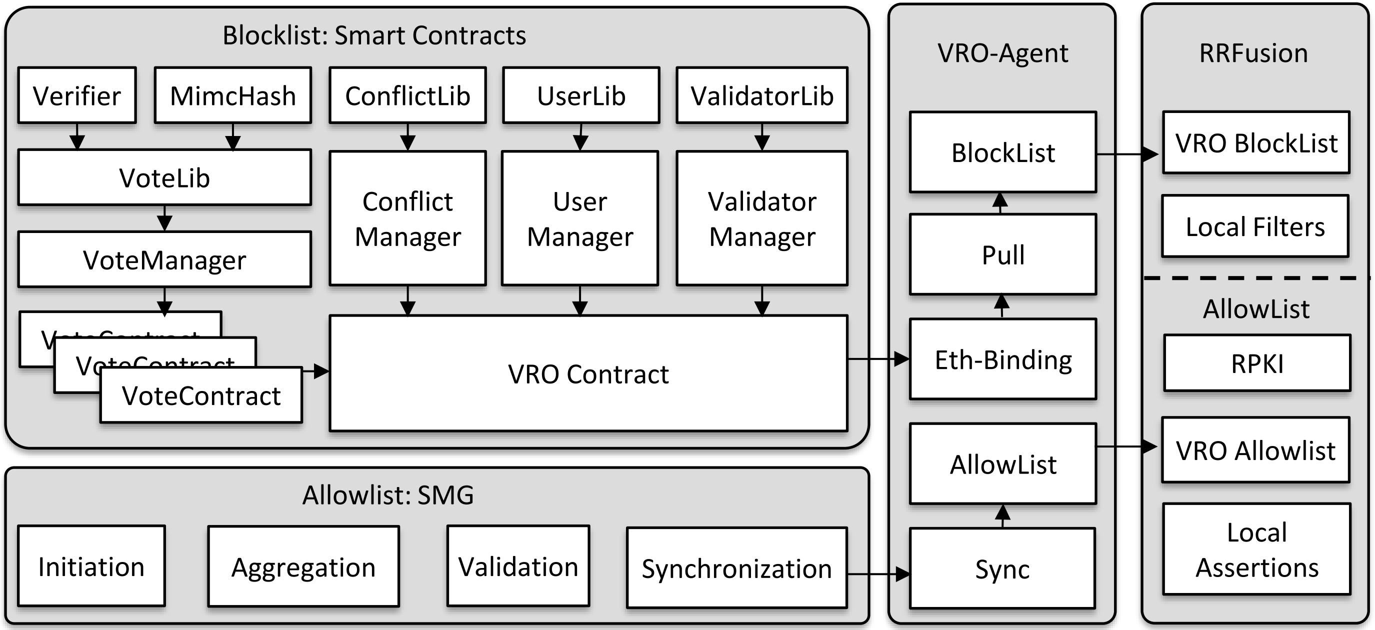
- **Background**: Existing mechanism may not adequately distinguish legitimate MOAS from malicious attacks, potentially misclassifying legitimate traffic.
- **Goal**: Design a verifiable cooperative system among ASes "Verifiable Route Origin（VRO）" to enhance the trustworthiness of the routing origin



Verifiable Route Origin

(Signature-based) Allowlist + (Vote-based) Blocklist + (Multi-source)RRFusion

Code Link: https://github.com/VRO-Project



Allowlist & Blocklist

- Allowlist: ASes collaboratively sign same prefixes using aggregate signatures, forming a Signed MOAS Group (SMG).
- Blocklist: Neighboring ASes vote on the most credible AS based on local data in case of prefix-origin conflicts.

```
RpkiSignedMoasGroup: {
    SignedMoasGroupObject: {
        version INTEGER DEFAULT 0,
        ipAddressPrefix IPAddressFamily,
        asList SEQUENCE (SIZE(0..MAX)) OF ASId,
    },
    DigestAlgorithmIdentifier,
    Digest
}
Attestation //Individual signature or Aggregate signature
```

```
MOAS_Conflict {
        uint256 ConflictID;
        string IP_Prefix;
        uint[] MOAS;
        address Validator;
        address Reporter;
        uint[] Voters;
        uint Status;   uint Options;
        string[] OptionNames;
        uint Result;
}
```

Wrap Up

Team members:

On-site
Shenglin Jiang: jiangshl@zgclab.edu.cn
Ke Xu: xuke@tsinghua.edu.cn
Qi Li: qli01@tsinghua.edu.cn

Remote
Qi Li: liq23@zgclab.edu.cn
Zhuotao Liu: zhuotaoliu@tsinghua.edu.cn

Code Link:
https://github.com/VRO-Project

We have summited two IETF drafts in SIDROPS WG.

- Problem Statement: Route Origin Registry Problem Statement (draft-jiang-sidrops-psvro-01)
- Allowlist mechanism Profile: A Profile for Signed Group of Multiple-Origin Autonomous Systems for Use in the Resource Public Key Infrastructure (RPKI) (draft-li-sidrops-rpki-moasgroup-01)