Source Address Validation enhances its security using blockchain

draft-guo-savnet-enhances-sav-security-00

X.Guo  D.chen  Z.xiong  J.Chen  X.Liu
March 2023
SAV rules are generated based on routing information or non-routing information. If the routing information is poisoned by an attacker, there will be no way to verify the authenticity of the routing information and the generated SAV rules will be incorrect.

The main security threats to SAV come from the following areas:
- RPKI was attacked
- Wrong AS prefix advertisements
- Malicious router
Problem

- RPKI cannot resist malicious acts initiated by CAs for the benefit of countries and organizations, and the tree structure of RPKI has the defect of single point of failure, and the whole network may be paralyzed after the attack of high-level CAs, so RPKI has the problem of being centralized and tamperable.

- Depending on the centralized trust model, once the Authority node is misconfigured or attacked, it raises security issues and is difficult to avoid from the mechanism.

- 2014.1, a Nigeria network’s ROA was failed due to its parent's RC was overwritten.
The existing routing protocols cannot guarantee the integrity of AS prefix advertisements and cannot authenticate whether the AS advertisement IP prefix authorization is legitimate, causing security events such as origin hijack, traffic eavesdropping, and traffic black holes. The attacker disguises the malicious router as a peer node, propagating false advertisement messages or tampering with legitimate advertisement messages, which will not only destroy the SAV function but also affect the entire routing domain.
Blockchain technology, due to its natural attributes of decentralization, tamper-proof and traceability, is supported by distributed node authentication and consensus mechanisms, allowing any two nodes in a distributed network to reach an unmediated trust.

Another advantage of applying blockchain to SAV is that it can add additional security without changing the BGP protocol, and by using blockchain SAV can be protected in several ways.

- Replace RPKI
- AS Prefix Advertisement Information Authentication
- Malicious router discovery
Through resource transaction record and resource retrieval of blockchain's smart contract technology, the IP address and ASN registration and allocation information are recorded, and the tracking of their usage is supported, so as to realize the authorization authentication of IP address and ASN network resources, prevent the security threat of prefix hijacking and avoid the repeated allocation of resources.
Solution

- The blockchain smart contract is used to record the IP address authorization. When the AS prefix advertisement is required, the prefix advertisement of the source AS can be stored on the blockchain. After receiving the source AS advertisement information, the destination AS determines the integrity of the received AS advertisement information through the transaction information saved on the chain.

- Store the routing topology relationship in the blockchain. When the AS discovers the malicious advertisement information of the AS through the blockchain verification, the network location of the malicious router can be located in a timely manner by routing topology relationship stored in the blockchain.
You are welcome to join in this project.

Contact with: guoxs@chinatelecom.cn

Thank you!