A Profile for Traffic Origin Authorizations (TOAs)

Authors: Lancheng Qin (Zhongguancun Lab)

Ben Maddison (Workonline)

Dan Li (Tsinghua University)

Igor Lubashev (Akamai)

Nov, 2025

Quick Review of TOA

- Key Challenge in current SAV mechanism
  - The current system for **validating the right to originate traffic** with a given source address has been **built almost entirely on top of** mechanisms designed to **validate the right to originate routes** to that IP address
  - This approach works when the two align, but **creates ambiguity and misalignment when they diverge**
    - In scenarios where traffic is unidirectional and there is no need to attract return traffic via route announcements, or where the return traffic is intentionally directed to another location (e.g., the CDN and DSR scenario), this approach will **improperly block legitimate traffic**
- Purpose of a Traffic Origin Authorization (TOA)
  - A new **RPKI signed object**
  - Explicitly **authorize an AS to originate traffic** using a given prefix as a source address, **even when that AS is not authorized to originate any BGP routes** to that prefix

Quick Review of TOA

- TOA attracted significant attention and inspired lively discussions during and after IETF 123

[savnet] Discussion on the Traffic Origin Authori… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Michael Richardson
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Dan Li
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng Qin
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng Qin
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Siyuan Teng
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: [EXTERNAL] Re: draft-haas-savnet-int… gengnan
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: draft-haas-savnet-inter-domain-scali… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering

[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Sriram, Kotikalapudi (Fed)
[savnet] Re: Discussion on the Traffic Origin Aut… Sriram, Kotikalapudi (Fed)
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: draft-haas-savnet-inter-domain-scali… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Sriram, Kotikalapudi (Fed)
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: [Sidrops] Re: Re: Discussion on the … Aijun Wang
[savnet] Re: [Sidrops] Re: Re: Discussion on the … Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Michael Richardson
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: [Sidrops] Re: Re: Discussion on the … Lancheng Qin
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Aijun Wang
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng Qin
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng Qin
[savnet] Re: Discussion on the Traffic Origin Aut… Gert Doering
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Michael Richardson
[savnet] Re: Discussion on the Traffic Origin Aut… Lubashev, Igor
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… gengnan
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Sriram, Kotikalapudi (Fed)
[savnet] Re: [EXTERNAL] Re: draft-haas-savnet-int… Jeffrey Haas
[savnet] Re: [EXTERNAL] Re: draft-haas-savnet-int… gengnan
[savnet] Re: [EXTERNAL] Re: draft-haas-savnet-int… Lancheng

[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Jeffrey Haas
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng
[savnet] Re: Discussion on the Traffic Origin Aut… Lancheng

Offline discussions during IETF123:

- Lancheng Qin, Jeffery Haas, Job Snijders
- Lancheng Qin, Antoin Verschuren

Igor Lubashev (Akamai Technologies) joins as a new co-author

- Document history
  - draft-qin-sidrops-toa-00, IETF 123
  - **draft-qin-savnet-toa-00, IETF 124**

Main Updates

We make the following updates based on discussions

- Further clarify the challenge and use cases in Section 1
- Add Section 6 to provide operational recommendations
- Add Section 8 to summarize discussion results

Section 6: Operational Recommendations

- Considerations
  - A TOA is primarily useful in scenarios where the traffic origin AS and the route origin AS differ
  - When the same AS is both authorized to originate routes (via an existing ROA) and to originate traffic from a given prefix, creating a duplicated TOA would add unnecessary storage and transmission overhead in the RPKI system
- Recommendations: operators are RECOMMENDED to follow these practices:
  - Operators SHOULD NOT register a TOA that is identical to or covered by an existing ROA, unless there are valid operational reasons
  - TOA registrations SHOULD be periodically reviewed and updated to reflect current operational practices

Section 8: Summary of Discussions

- Discussion #1: Whether it would be feasible to create a special ROA for an AS that is not authorized to originate a route to a given prefix, as an alternative to implement TOA
  - The TOA authors consulted ASN.1 experts on this approach, who strongly advised against it because this requires extending ROAs or overloading their semantics to cover this use case. Other SIDROPS participants also recommended against overloading ROA semantics
- Decision #1: The current consensus among the TOA authors and several SAVNET/SIDROPS participants is that defining a dedicated TOA object represents a more appropriate and robust solution

Section 8: Summary of Discussions

- Discussion #2: How about creating a conventional ROA for such scenarios even though the AS is not authorized to originate routes to the given prefix
  - Semantic conflict: a ROA allows the AS to originate routes to the given prefix
  - Additional risks of forged-origin hijacking: an attacker could impersonate the AS listed in the ROA and announce a BGP route that would be considered RPKI-valid
- Decision #2: The choice of how to authorize the traffic origin rests with the prefix holder
  - If the prefix holder wishes ROAs to include only ASes authorized to originate routes to its prefix, there is a clear need to register a TOA to authorize other ASes to source traffic from the prefix
  - Conversely, if the prefix holder is unconcerned about semantic ambiguity, forged-origin hijacking, or other potential risks, they may instead choose to register a conventional ROA

Relationship to Other SAV Mechanisms

- Several ongoing SAV solution drafts reference the TOA as an input to enhance SAV accuracy and robustness
  - draft-ietf-sidrops-bar-sav
  - draft-li-sidrops-bicone-sav
  - draft-li-savnet-source-prefix-advertisement
- TOAs can complement multiple SAV solutions and provide useful SAV-specific information for improving their effectiveness

Acknowledgements

- The authors would like to thank Jeffrey Haas for his valuable contributions in enriching the use cases and clarifying the challenges described in Section 1
- Special thanks also go to Job Snijders, who provided expert feedback on the ASN.1 considerations discussed in Section 8

Thanks

Backup

Open Discussion

- Suppose a prefix holder has an existing ROA {AS1, Prefix1} and wishes to create a TOA { (AS1, AS2, AS3), (Prefix1, Prefix2, Prefix3) }. In this case, the portion {AS1, Prefix1} is already covered by the ROA and is therefore redundant within the TOA. How to handle?
  - Option #1: Split the TOA into smaller objects, such as { (AS1), (Prefix2, Prefix3) } and { (AS2, AS3), (Prefix1, Prefix2, Prefix3) }
  - **Option #2 (preferred):** Register a single consolidated TOA covering all relevant ASes and prefixes
- When different ASes are authorized for overlapping prefixes (e.g., there are two TOAs { AS1, 1.2.0.0/20 } and { AS2, 1.2.0.0/24 }), does SAV consider both AS1 and AS2 authorized to source traffic from the more specific prefix (1.2.0.0/24), or only AS2?
  - In the current context, both AS1 and AS2 could be interpreted as authorized for the more specific prefix. If the intent is to restrict AS1 from the more specific prefix, the first TOA could be modified to explicitly exclude the more specific prefix