Inter-domain Source Address Validation (SAVNET) Architecture

Dan Li, Li Chen, Nan Geng, **Libin Liu**, Lancheng Qin

March 17, 2025

SAVNET WG, IETF 122

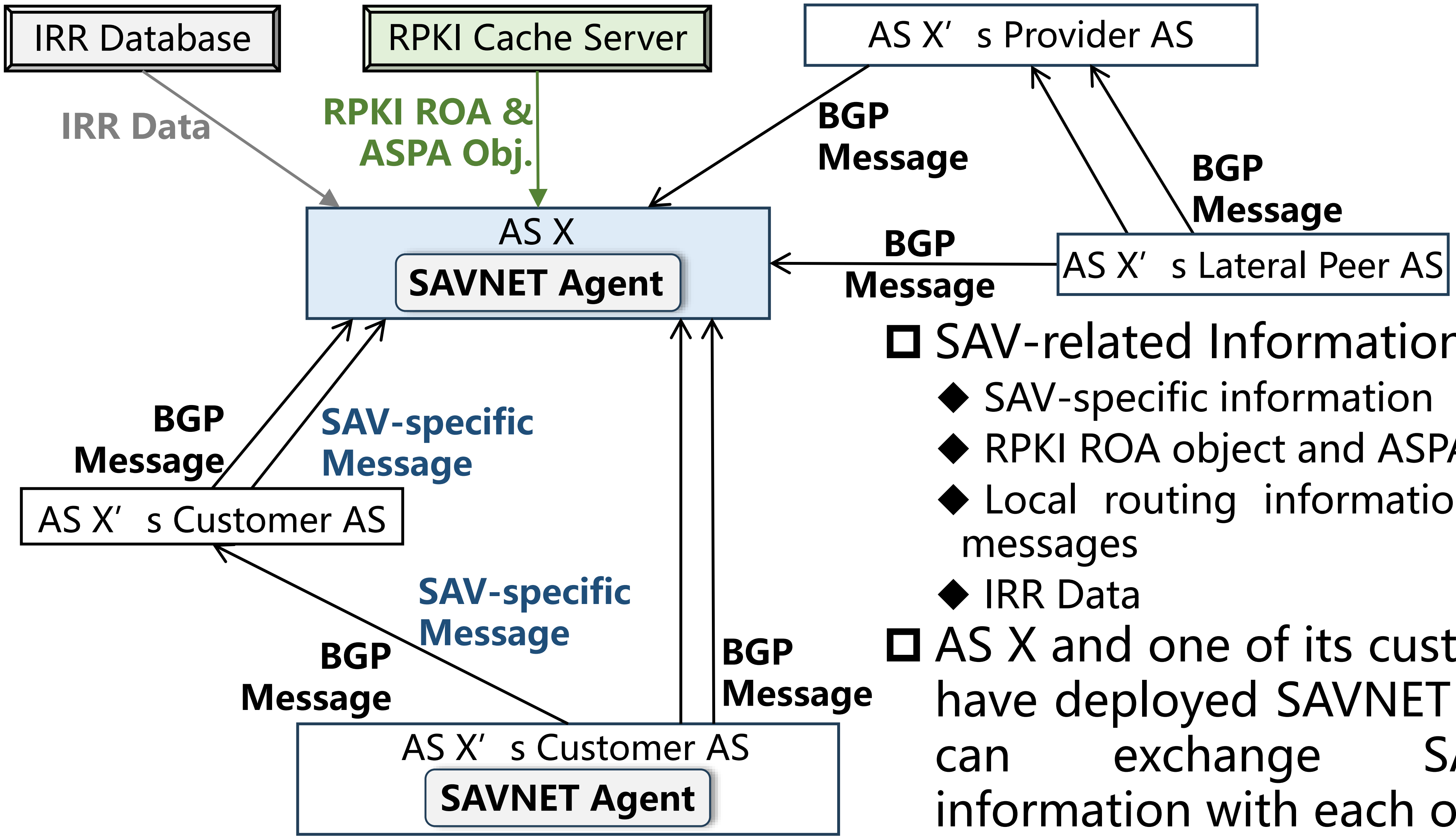
Background

- Inter-domain SAVNET architecture aims to provide a comprehensive framework for developing new inter-domain SAV mechanisms
  - Address the problems of existing inter-domain SAV mechanisms
  - Meet the requirements proposed in [draft-ietf-savnet-inter-domain-problem-statement]
- Historical versions
  - draft-wu-savnet-inter-domain-architecture-00, IETF 115 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-01, IETF 116 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-03, IETF 117 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-05, IETF 118 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-07, IETF 119 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-09, IETF 120 SAVNET WG
  - draft-wu-savnet-inter-domain-architecture-12, IETF 121 SAVNET WG
  - **draft-ietf-savnet-inter-domain-architecture-01, IETF 122 SAVNET WG**

Quick Review of WG Version-01

- Summarizing the incentive of inter-domain SAVNET architecture
- Illustrating the design goals of inter-domain SAVNET architecture
- Introducing the detailed inter-domain SAVNET architecture
  - Inter-domain SAVNET architecture overview
  - SAV-specific information and general information
  - SAV rule generation based on various SAV information sources
- Describing the SAVNET communication mechanisms
  - SAV-specific information communication mechanism
  - General information communication mechanism
  - Management information communication mechanism
- Illustrating the use cases of inter-domain SAVNET architecture
- Describing how to meet the design requirements proposed in the PS draft

Inter-domain SAVNET Architecture Overview



- SAV-related Information
  - SAV-specific information
  - RPKI ROA object and ASPA object
  - Local routing information from BGP messages
  - IRR Data
- AS X and one of its customer ASes have deployed SAVNET agent and can exchange SAV-specific information with each other.

Summary of Comments and Responses

- Priorities recommendation of different SAV-related information (Sriram)
  - **Comments on the mailing list during IETF 121**: The draft enumerates 5 types of data that can be helpful for constructing SAV tables. It seems premature to assign priority labels to them. In any case, as the draft also says, they are complementary to each other for SAV. IMO, BGP data and RPKI data (ROA, ASPA) are not less important than SAV-specific data. I do see that the draft tries to soften it all by stating, "It is noteworthy that the priority ranking of SAV information sources in Figure 5 is recommended rather than mandated."
  - **Comments during IETF 121 SAVNET WG meeting**: It is suggested to remove prioritization recommendation for the different types of data sources.
  - **Our response**: We have revised the recommendations for using SAV information sources as we discussed.

Updates on Recommendations for Using SAV Information Sources

- Inter-domain SAVNET architecture can use SAV-related information from different sources to generate SAV rules
  - Currently, it recommends using the information from all the available sources which are verified as trustworthy to generate SAV rules, and SAV information sources complement each other for SAV.
  - SAV-specific information: Each AS deploying inter-domain SAVNET can utilize a specific security mechanism as discussed to validate the received SAV-specific information from other ASes to guarantee its trustworthiness.

<table>
<tr><th colspan="2">SAV Information Sources</th><th>Trustworthiness</th><th>SAV Usage</th></tr>
<tr><td colspan="2">SAV-specific Information</td><td>Specific security mechanism</td><td rowspan="4">Complementing each other</td></tr>
<tr><td rowspan="3">General Information</td><td>ROA and ASPA Obj.</td><td>X.509 certificates</td></tr>
<tr><td>Local Routing Information</td><td>ROV, Route leak detection</td></tr>
<tr><td>IRR Data</td><td>Low level of trust</td></tr>
</table>

Updates on Recommendations for Using SAV Information Sources

- Inter-domain SAVNET architecture can use SAV-related information from different sources to generate SAV rules
  - RPKI ROA and ASPA objects: They use x.509 certificates [RFC5280] to protect the objects and guarantee the trustworthiness.
  - Local routing information: They rely on some techniques, such as ROV and route leak detection (e.g., ASPA or OTC) for achieving the trustworthiness of their information.
  - IRR data: They have lower level of trust compared to others.

SAV Information Sources		Trustworthiness	SAV Usage
SAV-specific Information		Specific security mechanism	Complementing each other
General Information	ROA and ASPA Obj.	X.509 certificates	
	Local Routing Information	ROV, Route leak detection	
	IRR Data	Low level of trust	

Security Considerations

- The security threats faced by SAV-specific communication mechanism in inter-domain networks can be categorized into two main aspects:
  - Session security threats
    - Session identity impersonation and session integrity destruction
  - Content security threats
    - Message alteration, message injection, and path deviation
- Existing security mechanisms can be used or a new security mechanism should be designed to secure SAV-specific information
  - The detailed security design of SAV-specific communication mechanism is out of scope for this document.

Acknowledgements

- Many thanks to Alvaro Retana, Kotikalapudi Sriram, Rüdiger Volk, Xueyan Song, Ben Maddison, Jared Mauch, Joel Halpern, Aijun Wang, Jeffrey Haas, Xiangqing Chang, Changwang Lin, Mingxing Liu, Zhen Tan, Yuanyuan Zhang, Yangyang Wang, Antoin Verschuren, Olaf Struck, Siyuan Teng etc. for their valuable comments and feedback on this document.

Thanks! ☺