And now... BGPSec

Alexander Azimov

<aa@qrator.net>
RFC 8205: BGPsec Protocol Specification
RFC 8206: BGPsec Considerations for Autonomous System (AS) Migration
RFC 8207: BGPsec Operational Considerations
RFC 8208: BGPsec Algorithms, Key Formats, and Signature Formats
RFC 8209: A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests
RFC 8210: The Resource Public Key Infrastructure (RPKI) to Router
RFC 8211: Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)
Origin Validation

Route Objects:
• Not in all RIRs;
• AS-SET can’t be signed;
• Vulnerable to AS Path poisoning;

RPKI:
• Vulnerable to replay attacks.
AS Path Poisoning

Attacker prepends its path with victim’s AS and... bypass any filters
BGPSec

Every segment + Target AS are signed, not AS Path Poisoning!