Accelerate Standardization and Support Adoption of BGP Security Technologies

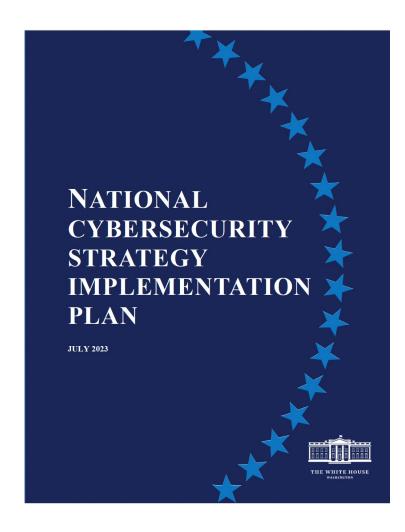
Doug Montgomery (dougm@nist.gov)

Manager, Internet Technologies Research Group

National Cybersecurity Strategy

Invest in a Resilient Future

- 4.1 Secure the Technical Foundation of the Internet.
 - 4.1.4 Accelerate the development, and standardization, and support the adoption of foundational Internet infrastructure capabilities and technologies.
 - The NIST will collaborate ... to address BGP and IPv6 security gaps by driving development, commercialization, and adoption of international standards.



NIST Trustworthy Networks Research

Trustworthy Networks Program

- Working with industry to advance research, standardization and adoption of technologies necessary to resolve systemic vulnerabilities in existing and emerging critical network infrastructures.
 - BGP, DNS, IPv6, Zero Trust, IoT, Virtualized Networks, O-RAN/5G.











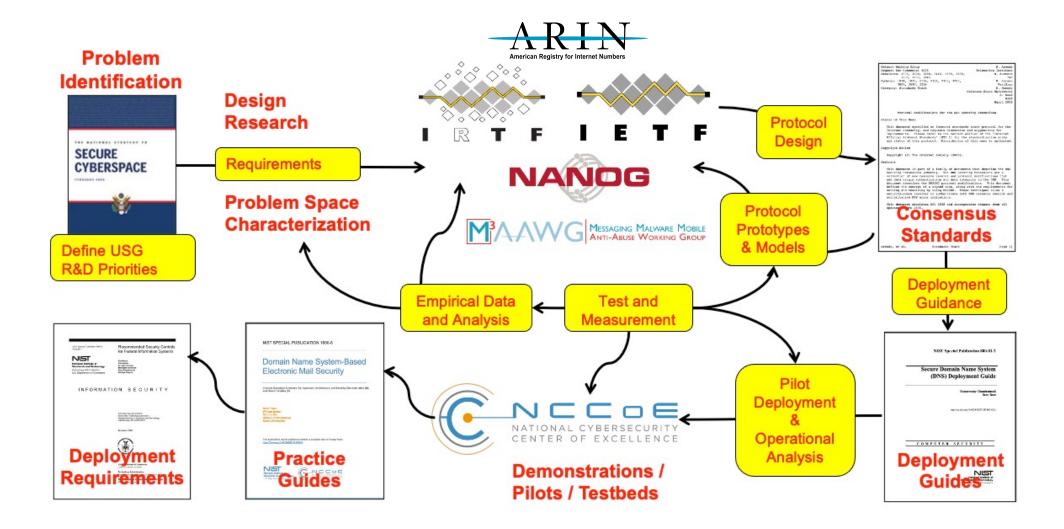




Robust Inter-Domain Routing Project

- Working with industry to design, standardize, and foster deployment of technologies to improve the security and resilience of Internet Routing
 - Ongoing effort since 2003.

NIST's Roles and Contributions



NIST Contributions: Current Examples

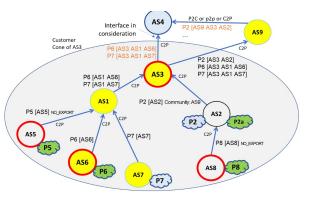
Advance Standardization

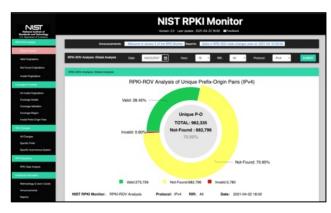
- Problem Definition
 - "Problem Definition and Classification of BGP Route Leaks" IETF RFC7908.
- Design and Standardization
 - Design Discussion of Route Leaks Solution Methods
 - BGP AS PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects
 - Methods for Detection and Mitigation of BGP Route Leaks
 - Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)

Foster Commercialization and Adoption

- Reference Implementations
 - NIST BGP-SRx suite contains an implementation of ASPA verification.
- Tools for Implementors
 - <u>NIST BGPSec-IO</u> test harness can of generate Internet scale synthetic ASPA data and provides ASPA interoperability test suites.
- Tools for Operators
 - NIST RPKI Monitor being extended to track completeness and quality of ASPA rollout in RPKI.







NIST Collaborations







NIST BGP Security Guidance

- NIST 800-189 Resilient Interdomain Traffic Exchange
 - Security recommendations address broader scope of BGP security, DDoS mitigation, anti-spoofing techniques.
 - 65 specific security recommendations for federal enterprises and/or their internet service providers, addressing:
 - RIR enrollment for number resources
 - Use of RIR IRR services
 - RPKI enrollment for number resources
 - ROA creation for addresses announced to public Internet
 - Including guidance on ordering, max-length etc.
 - Use ROV in enterprise and ISP BGP operations
 - Ingress / egress BGP address filtering guidance
 - Route leak avoidance
 - Source address filtering (SAV) and other anti-spoofing techniques.
 - DDoS mitigation using BGP signaling (e.g., RTBH, flowspec)

NIST Special Publication 800-189

Resilient Interdomain Traffic Exchange:

BGP Security and DDoS Mitigation

Kotikalapudi Sriram Doug Montgomery

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-189

COMPUTER SECURITY



NIST BGP Practice Guides

- NIST 800-14 Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation (2019).
 - NCCoE RPKI-ROV demonstration project (Cisco, Juniper, AT&T, Comcast, CenturyLink, Paloalto, George Washington University).
 - Demonstration of viability of early RPKI-ROA infrastructure technologies and early commercial router ROV implementations.
 - Focused on scale, stability and robustness issues router interfaces to RPKI-caches.
 - Used NIST synthetic data tools to present Internet scale ROA sets to commercial routers.

NIST SPECIAL PUBLICATION 1800-14

Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Haag Doug Montgomery William C. Barker Allen Tan

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-14

The first draft of this publication is available free of charge from: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800-14-draft.pdf





NIST BGP Security Controls

- NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations
 - SC-7 Boundary Protection
 -

2023-07-31

- (f) Prevent unauthorized exchange of control plane traffic with external networks;
- (g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
- (h) Filter unauthorized control plane traffic from external networks.
- Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5



NIST: Future Work.

USG RPKI enrollment

 Work with ARIN to address questions associated with large scale RPKI enrollment.

Update NIST security guidance

- RPKI enrollment, ROA creation
- ROV implementation
- DDoS mitigation
- Source address validation

Work with interagency

- Drive deployment In USG networks and in USG infrastructure service providers.
- Collaborate with interagency roadmaps and plans

Complete ASPA standards and tools.

- Verification specification
- ASPA Prototypes and traffic generators

Further research and development

- Commercially viable path validation
- RPKI ROV and DDoS Mitigation
- BARSAV further research on the leverage of RPKI based technologies for SAV.

Questions / More Information

- For more information:
 - NIST Robust Inter-Domain Routing Project
 - https://www.nist.gov/programs-projects/robust-inter-domain-routing
 - Trustworthy Networks Program
 - https://www.nist.gov/programs-projects/trustworthy-networks-program

• **DISCLAIMER** Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.