



Joint Meeting: SSAC & ALAC
18 September 2022



- **ALAC Topics:**
 - Response to DNS Abuse Questions (ALAC) 20-minutes
- **SSAC Topics:**
 - NCAP (SSAC lead: Jim Galvin and Matt Thomas) 20-minutes
 - SAC121 Routing Security (SSAC lead: Russ Mundy) 20-minutes
 - SSAC New Member Outreach 5-minutes
 - SSAD (SSAC lead: Steve Crocker) ...time permitting
 - Addendum to SAC114 (SSAC lead: Rod Rasmussen) ...time permitting

ALAC Questions

Response to DNS Abuse Questions (ALAC)

Name Collision Analysis Project

Jim Galvin and Matt Thomas (Co-Chairs)

See also this [detailed presentation](#) provided to the CPWG on 03 August 2022

NCAP Background

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board on name collisions
 - Specific advice regarding .home/.corp/.mail
 - General advice regarding name collisions going forward
- Studies to be conducted in a thorough and inclusive manner that includes other technical experts
 - 25 discussion group members, including 14 SSAC work party members
 - 23 community observers
 - Chaired by James Galvin and Matt Thomas

- Case Study of Collision Strings
 - Studies of .corp, .home, .mail, .internal, .lan, and .local using DNS query data from A and J root servers.
 - Highlight changes over time of the properties of DNS queries and traffic alterations as a result of DNS evolution.
- A Perspective Study of DNS Queries for Nonexistent Top-Level Domains
 - Aims to understand the distribution of DNS name collision traffic throughout the DNS hierarchy
 - Provide insights into where and how DNS data can be collected and assessed.

NCAP - Key Findings so far

- Name collisions are and will continue to be an increasingly difficult problem; case study indicates impact has increased
 - DNS service discovery protocols and suffix search lists are a continuing problem
- Critical diagnostic measurements (CDMs) are defined as a way to measure name collisions by informing the assessment of the risk of delegation
- Any root server identifier is representative of the CDMs seen in the root server system (RSS)
- Mitigation and remediation is problematic, increasingly difficult as the volume and diversity of CDMs increases
- Existing measurement platforms could be extended to help inform applicants

NCAP - Critical Diagnostic Measurements

- Query Volume
- Query Origin Diversity
 - IP address distribution
 - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
 - Open-Source Intelligence (OSINT)

- **Impact (or Harm) is determined by evaluating both Volume and Diversity across all CDMs**

- The NCAP discussion group is developing a framework to assess name collisions
 - How the Board is going to assess name collisions
 - Guidance on how to consider the risks of delegation given the existence of name collisions
- The initial framework, along with findings from other studies, will be published for public comment in 4Q2022

NCAP - How to Participate

- Review the report as soon as it is released for public comment
- Attend or review recording
 - NCAP Discussion Group (19 September 14:30 UTC)
 - NCAP Update (20 September 14:30 UTC)
- [Join the discussion group](#)

Recent SSAC Publications

SAC121: SSAC Briefing on Routing Security

SAC121: SSAC Briefing on Routing Security

- **Background Technical Information**
- **Routing Security and the Domain Name System (DNS)**
- **Efforts to Enhance Routing Security**
- **Operating Secured Infrastructure**
- **Key Takeaways**

Internet Routing for DNS Query

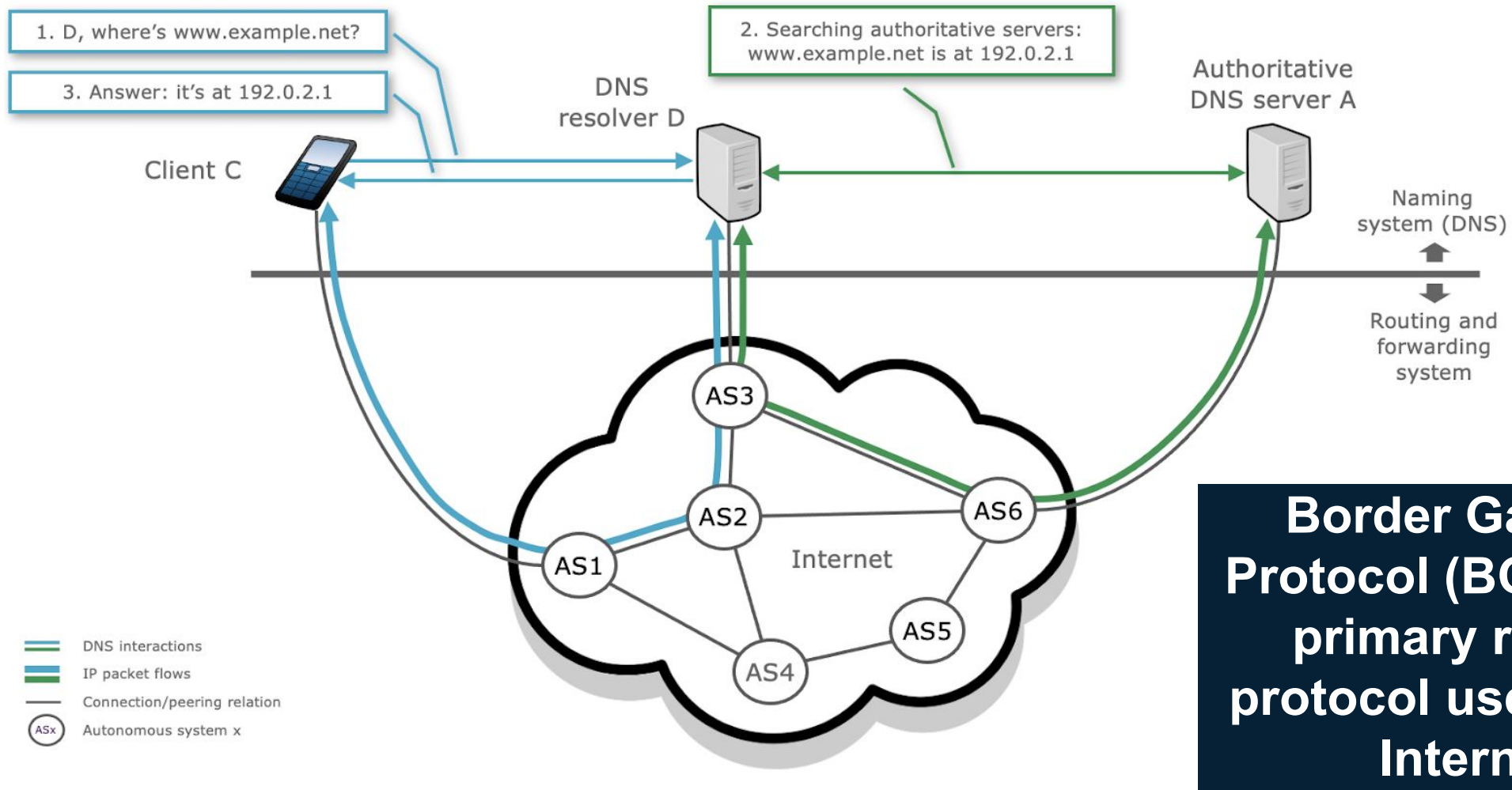


Figure 1: DNS traffic passing through multiple autonomous systems

Route Hijack for DNS Query

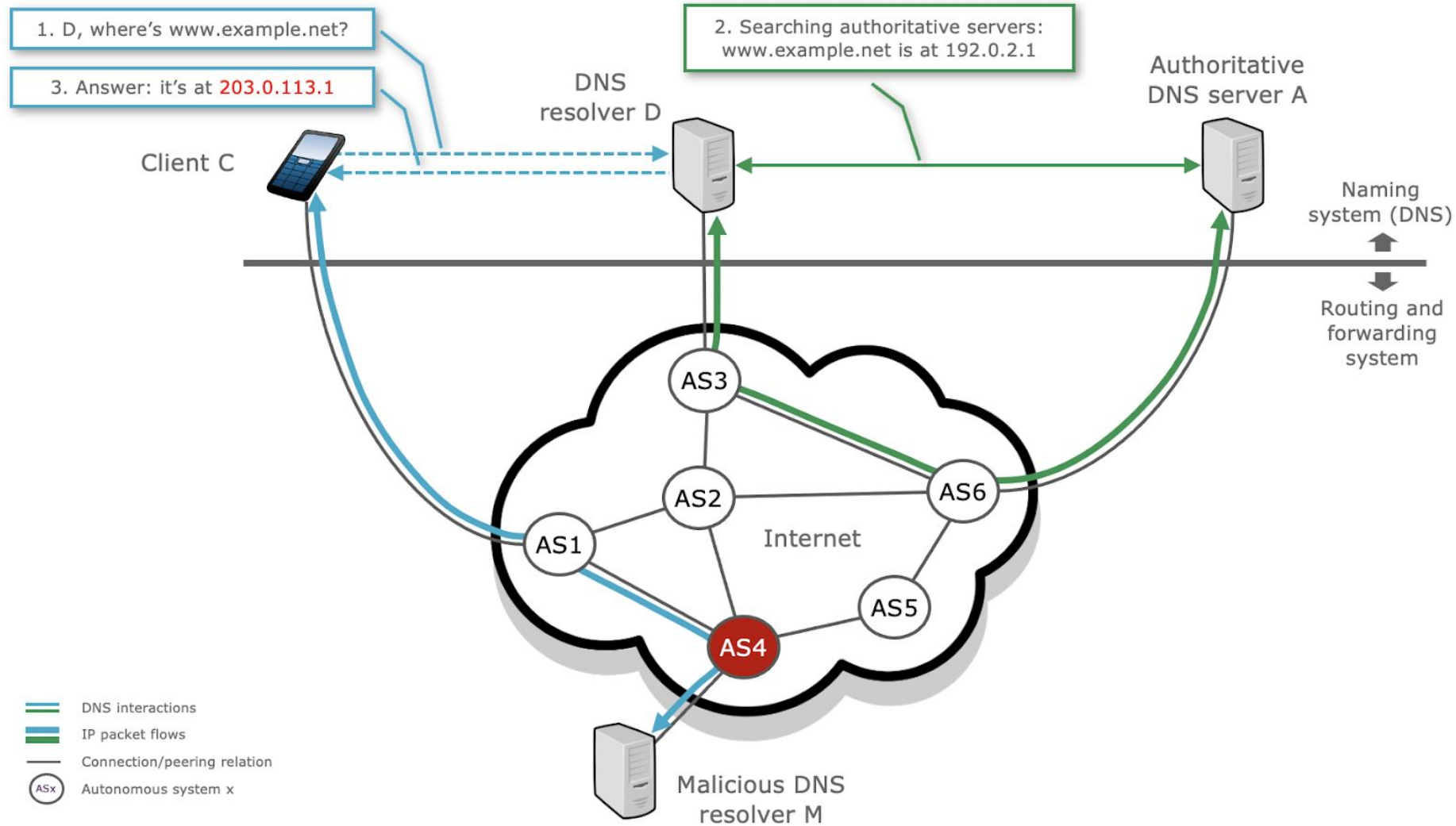


Figure 2: Hypothetical Route Hijack affecting the DNS

Routing Incident: MyEtherWallet / Route53

MyEtherWallet (myetherwallet.com) was attacked by unidentified criminals using a BGP hijacking attack

Attackers injected more specific routes for Amazon's Route53 DNS service

Attackers pretended to be the Route53 authoritative DNS servers

Their servers returned SERVFAIL for all queries, except those for MyEtherWallet

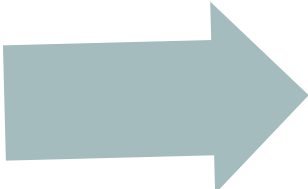


Attackers stole about \$150,000 in Ethereum in ~2 hours

For ~2 hours all DNS zones hosted at Route53 were effectively broken

The Relevance of Routing Security for the DNS

The DNS protocol and DNS resolution are susceptible to routing incidents

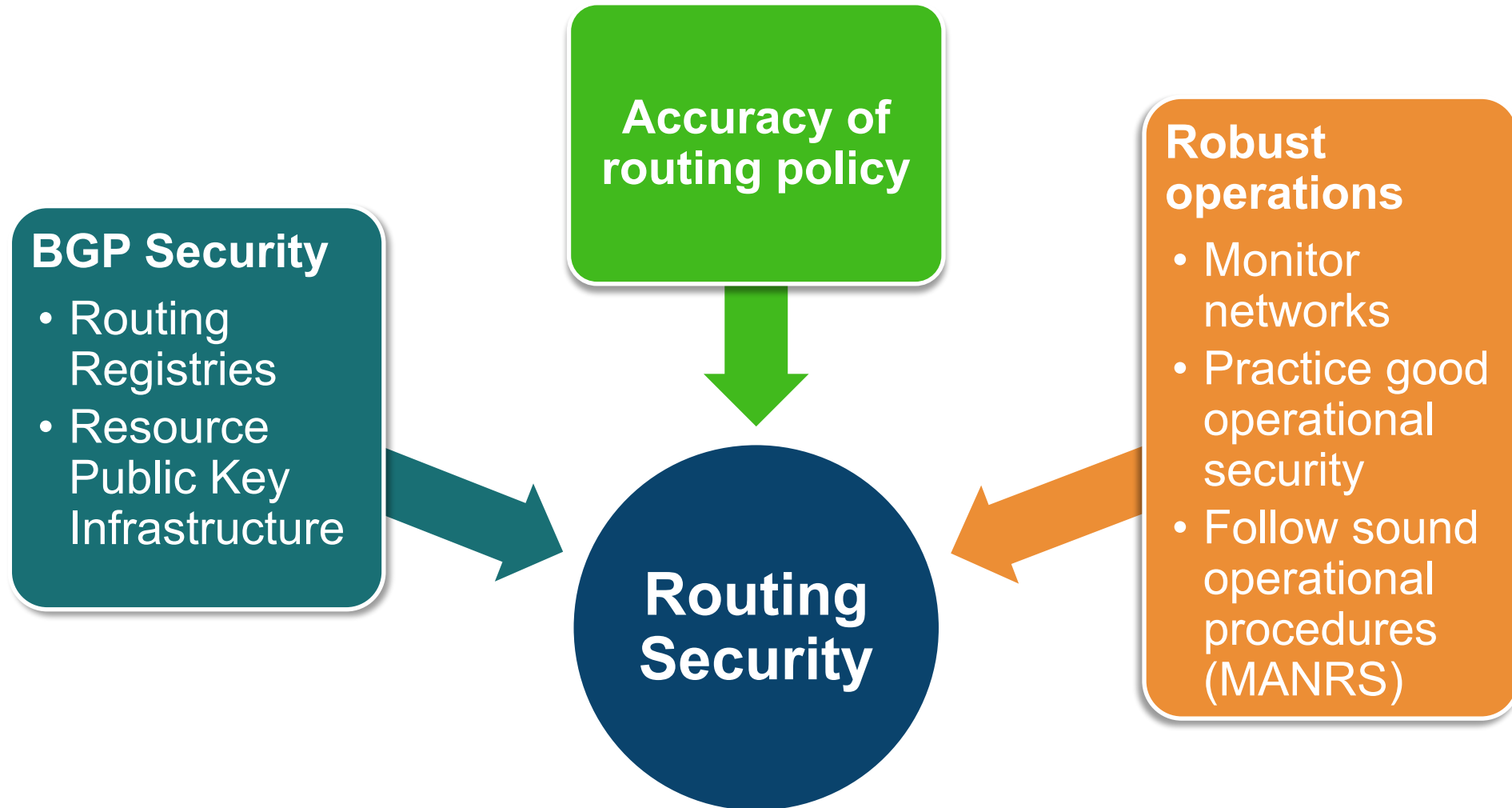
- Many authoritative DNS servers answer any query they receive
 - Many DNS clients do not authenticate the identity of the server that provides the answer, and do not perform DNSSEC validation
 - Stub resolvers have no visibility into which authoritative servers provide answers to queries
 - Vast majority of DNS queries are in the clear and use UDP as the transport protocol
- 
- A routing attack can substitute one DNS server for another without the awareness of the client
 - Routing attacks can alter the network path of a query, allowing third parties to inspect DNS queries or otherwise eavesdrop on transactions.

Routing Incident: MyEtherWallet / Route53

MyEtherWallet (myetherwallet.com) was attacked by unidentified criminals using a BGP hijacking attack

- sequence
 - Attackers injected more specific routes for Amazon's Route53 DNS service
 - Attackers pretended to be the Route53 authoritative DNS servers
 - Their servers returned SERVFAIL for all queries, except those for MyEtherWallet
- consequences
 - Attackers stole about \$150,000 in Ethereum in ~2 hours
 - For approximately two hours all DNS zones hosted at Route53 were effectively broken

Efforts to Enhance Routing Security



BGP Security: Routing Registries

Network operators can register their autonomous systems and the prefixes they originate in a routing registry.



Highlights

- Allows other operators to see what prefixes and routes a given AS should be announcing
- Most useful when carefully and continuously managed for consistency, coverage, and accuracy



Limitations

- When routing registries take on too broad of a scope or are not actively managed their consistency and utility falls.
- The contents of different routing registries may not be mutually consistent and there is no clear way to resolve conflicts between them.

BGP Security: Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure (RPKI) is a way for entities with functional control of IP Address prefixes to assert which autonomous systems are permitted to originate those prefixes.



Highlights

- Builds upon routing registries by designating the autonomous systems that are permitted to originate a routing announcement for a prefix
- Provides some protection from common sources of routing incidents
- Discussions on the efficacy of the RPKI are ongoing, but it may soon be required by some regulators

Limitations

- Not a complete solution to routing security
- All participants always need access to all the data
- No notification to relying parties when they need to update their data
- RPKI cannot secure the full path, only couples the origination of prefixes to ASes

Operating Secured Infrastructure

Organizations should practice good operational security and monitor their routes in order to detect anomalies and failures.

Endogenous Monitoring

- Monitoring from within the network being monitored
- Monitor ability to reach other networks
- Most important is connection to upstream provider

Exogenous Monitoring

- Monitoring from outside the network being monitored
- Monitor connectivity from external networks
- Important, but more expensive than endogenous
- Anycast adds additional complexity

Operator Coordination

- Every org needs access to routing expertise to help remediate issues
- Network operator groups (NOGs) help facilitate relationship building & information sharing

MANRS for Network Operators

- Filtering
- Anti-spoofing
- Coordination
- Global Validation

Key Takeaways

The routing system today is subject to a continuous stream of routing anomalies that affect its integrity and that sometimes cause large DNS outages.

Internet routing security is a combination of BGP protocol security, accuracy of routing policy, and robust operations

Organizations should monitor their routes in order to detect anomalies and failures.

Routing security is not a substitute for other technologies also key to securing the DNS. It is only one part of a complete approach to securing a network.

SSAC Skills and Potential New Member Outreach

Julie Hammer

SSAC Member Skills

- The skills of SSAC members span the following categories:

Domain Name System	IP Addressing/Routing
Security	Registration Services
Abuse	Internationalized Domain Names
Root Server System	Information Technology
Non-Technical (e.g., legal, risk management, business skills)	

- The [SSAC Skills Survey](#) is used to document the skills of all existing and potential SSAC Members

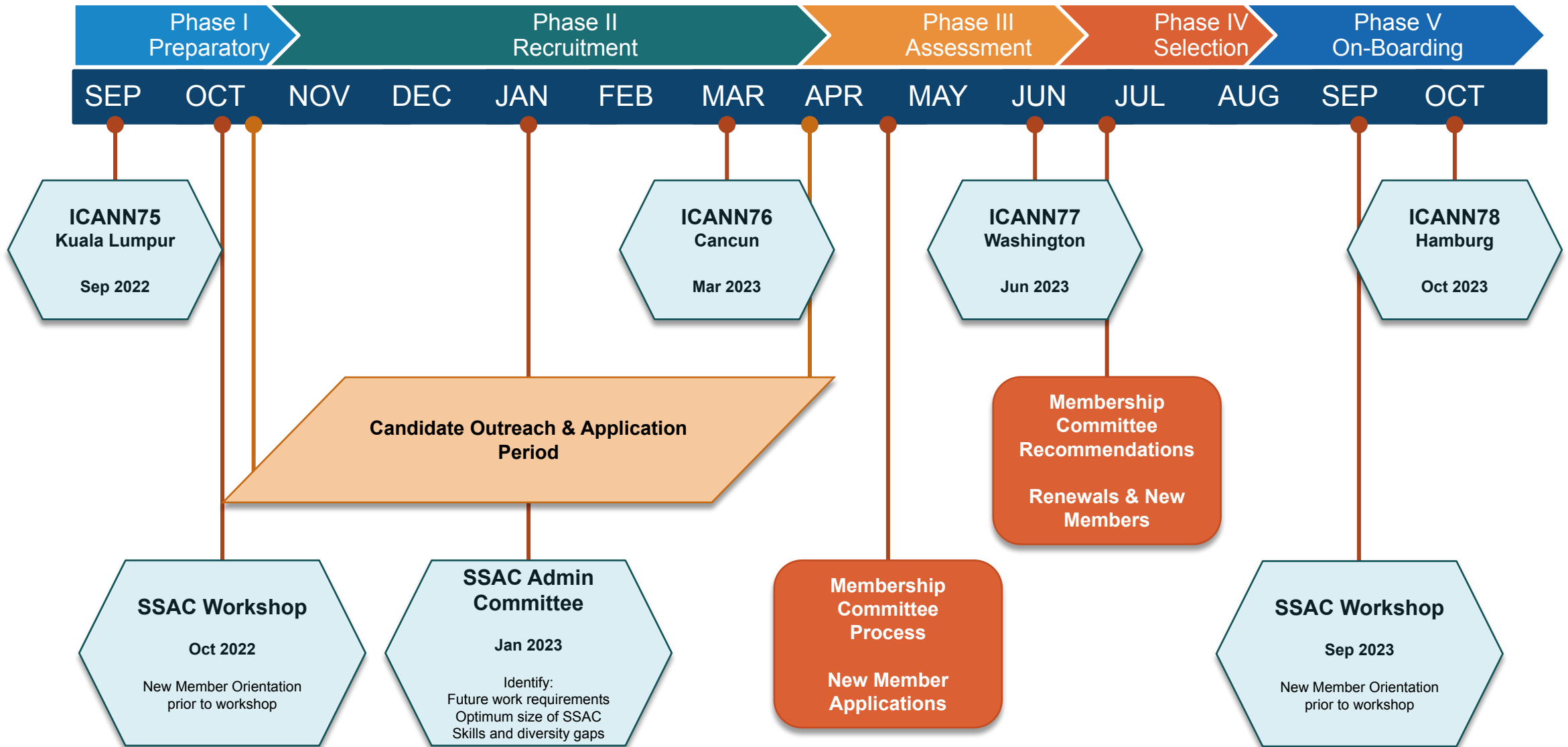
SSAC New Member Outreach

- SSAC is looking for motivated professionals who have skills in the SSAC skills categories and, in particular, expertise or background in:

ISP operations	Large-scale measurement
Large-scale Registrar Operations	Cloud/hosting experience
Browser Development/Testing	Mobile Apps Development/Testing
Low bandwidth resource-constrained Internet connectivity	Red Team experience

- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific
- The SSAC is interested in increasing membership from an academic background

SSAC Membership Outreach – 2023 Timeline



SSAC Contact for Potential New Members

Individuals who are interested in enquiring about SSAC membership should:

- Contact Rod Rasmussen or Julie Hammer,
- Contact any member of SSAC Support Staff, or
- Send an email to ssac-staff@icann.org

SSAD

Steve Crocker

- SSAC published SAC118v2 on 17 November
- Steve Crocker participated in the GNSO's
 - SSAD Operational Design Assessment (ODA)
 - Accuracy Scoping Team
 - EPDP Phase 2 Implementation Review Team (IRT)
- SSAC has responded to ICANN org's understanding request on SAC118v2
- SSAC currently awaiting for ICANN Board and GNSO Council's decision

Recent SSAC Publications

Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References (Rod Rasmussen)

Addendum to SAC114: Background

- SSAC published SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report on 11 Feb 2021
- SAC114 contains commentary on both the final report of the GNSO Subsequent Procedures Working Group and observations and recommendations on wider issues tied to increasing future delegations of new gTLDs
- SSAC reconvened a work party to consider the community's feedback and provide additional context for the language and recommendations in SAC114
- Overall, SSAC remains concerned that the gTLD Subsequent Procedures have been crafted without adequate learning from the prior expansion round

Addendum to SAC114: Context for Rec. 1

Looking forward, the SSAC has short- and long-term concerns regarding the future of the root zone:

Short-term Concerns	Long-term Concerns
<ul style="list-style-type: none">● SSAC finds substantial evidence that some new gTLDs have amplified the already considerable challenges with domain name abuse● SSAC agrees that a holistic solution is needed to handle such abuse● However, waiting until efforts to mitigate DNS abuse can be equally applied to all existing and new gTLDs effectively cedes the ground to malicious actors	<ul style="list-style-type: none">● ICANN community is continuing with another round of root zone expansion without agreeing to an overall, long-term strategy for the root zone● Without a documented long-term strategy it appears that ICANN intends to continue to approve root zone expansion in an ad hoc manner● The root zone is complex and it is difficult to predict failure of the root zone before it occurs● It is therefore advisable from a security, stability, and resiliency perspective to take a conservative approach in expanding the root zone

Addendum to SAC114: Context for Rec. 1

SAC114 Recommendation 1: *The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN’s strategic objective to “evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.” This review should be considered an input towards updating ICANN’s strategic goals in conjunction with implementing the CCT Review Team’s recommendations. Such a fundamental review should include at least the following areas of study based on prior rounds of the New gTLD program: Impacts on root server operations; Impacts on SSR issues; Impacts on overall DNS operations; Analysis of how all metrics for success were met; Risk analysis*

- The SSAC would like to see the ICANN Board and Community document a long-term strategy for root zone expansion
- Recommendation 1 is intended to provide the impetus to have the ICANN Board consider the short- and long-term concerns related to continuous root zone expansion
- The review mentioned in Recommendation 1 would be a useful starting place for developing the strategy

Addendum to SAC114: Context for Recs. 3 & 7

SAC114 Recommendation 3: *The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds.*

SAC114 Recommendation 7: *The SSAC recommends that the ICANN Board, prior to authorizing the addition of new gTLDs to the root zone, receive and consider the results of the Name Collision Analysis Project, pursuant to Board Resolution 2017.11.02.30.*

- Community feedback revealed some confusion as to the intended timing of Recommendations 3 and 7 - these recommendations could be addressed concurrently with other necessary work to plan for, support, and enable a program to introduce additional gTLDs to the root zone
- The constraint that motivated the timing included in Recommendation 3 is that proceeding without documenting best practices, baseline contract provisions, and policies prior to the launch of the application window leads to transactions where applicants are committing to contracts without essential information
- While it would be best to have NCAP completed before the launch of the application window, it seems essential to have it completed before delegation of such gTLDs

Thank you