



TLD-OPS Update

Tech Day

March 7, 2016
ICANN55, Marrakech

Cristian Hesselman, .nl (chair)

TLD-OPS

- Technical incident response community for and by ccTLDs
- Brings together folks who are responsible for the overall security and stability of their ccTLD
- Goal: facilitate further increased level of security and stability of ccTLDs' services and of the Internet as a whole
- Approach: increase (i) reachability of ccTLD incident response contacts and (ii) level of shared knowledge on security alerts
- Open to *every* ccTLD, irrespective of ccNSO membership
- Oversight by TLD-OPS Standing Committee
 - ccTLD reps and Liaisons (SSAC, IANA, ICANN's security team)

TLD-OPS Mailing List

- Regular automated emails with incident response info
 - Contact persons, phone numbers, and email addresses
 - Info of all subscribed ccTLDs in one email
 - Easily and quickly look up contact through (local) inbox
- Share security alerts, such as
 - Attacks (DDoS, reflection attacks, phishing, etc.)
 - Software vulnerabilities, malware
- Model of personal trust
 - Personal email address and phone number (no role-based accounts)
 - Contributes to further increasing trust within the ccTLD community
 - Approval model via IANA admin contact, bootstraps trust
 - Low entrance barrier, unlike vouching model

TLD-OPS Membership Stats

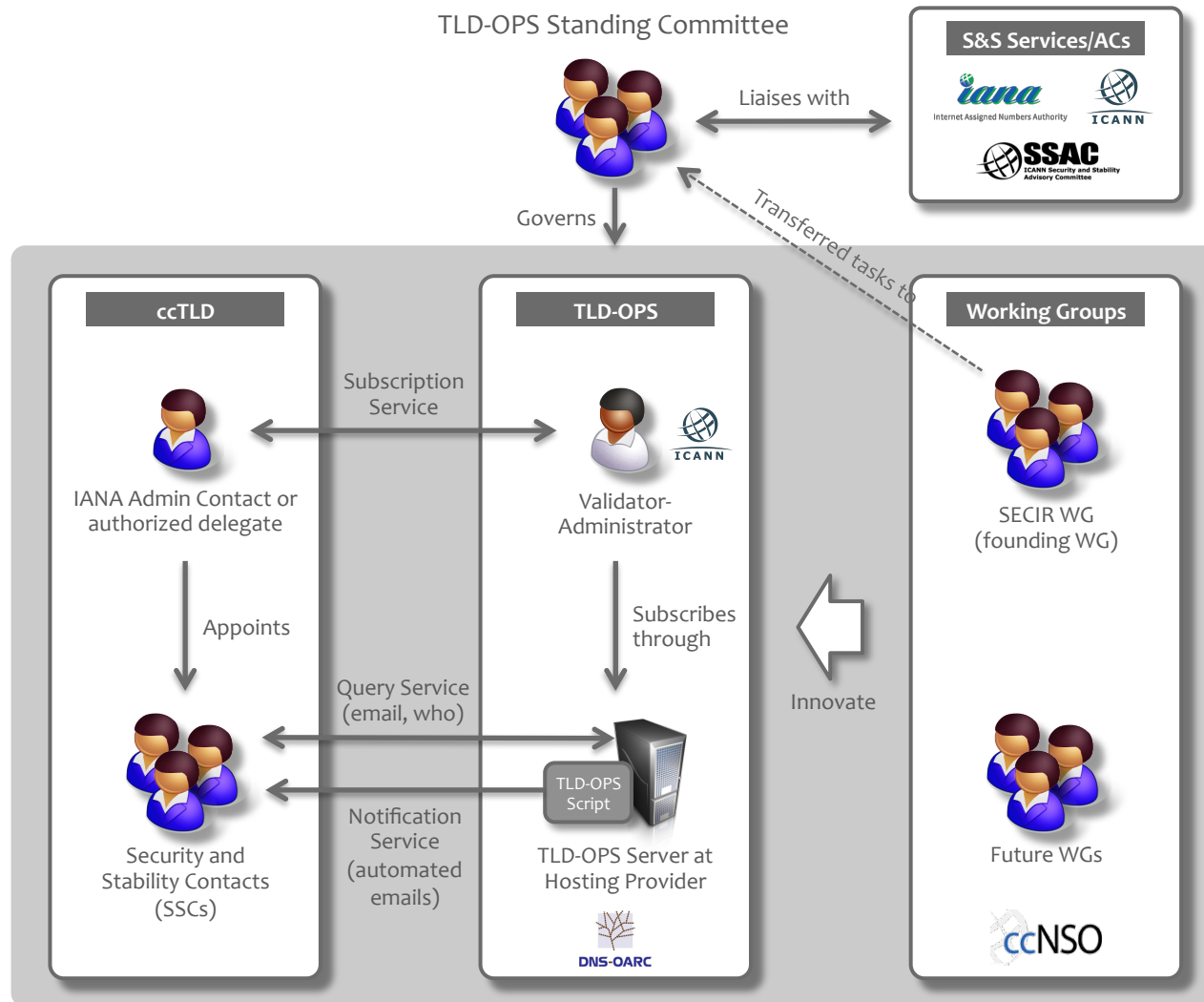
All	Members	%	Missing	%	Total
Total	173	60%	117	40%	290

ASCII	Members	%	Missing	%	Total
Total	145	59%	99	41%	244
AF	22	45%	27	55%	49
AP	42	51%	41	49%	83
EU	62	95%	3	5%	65
LAC	16	38%	26	62%	42
NA	3	60%	2	40%	5

IDN	Members	%	Missing	%	Total
Total	28	61%	18	39%	46

Last update: Mar 5, 2016

TLD-OPS Roles and Responsibilities



Progress Since ICANN54

- Added 6 ccTLDs (Egypt, Algeria, Barbados, Gibraltar, Moldova, Bosnia and Herzegovina)
- Updated TLD-OPS leaflet
 - Added value for members, governance
 - Based on ICANN54 feedback
 - <http://ccnso.icann.org/workinggroups/tld-ops-enhanced-incident-response-capabilities-cctlds-14jan16-en.pdf>
- Extended TLD-OPS Standing Committee
 - Ali Hadji Mmadi of .km (Comoros, AF)
 - Warren Kumari (SSAC Liaison)
 - John Crain (Liaison to ICANN's security team)
 - Kim Davies (IANA Liaison)
- Working with ICANN Regional VPs to onboard more ccTLDs

Challenge #1: Sharing

- How to facilitate list members to share security alerts through the TLD-OPS list?
- Part 1: bootstrap
 - Package and share security info relevant for ccTLDs
 - In collaboration with ICANN’s security team
 - Later fully rely on ccTLD operators to provide alerts (“peer-to-peer”)
- Part 2: operational processes
 - How do we get TLD-OPS into ccTLDs’ operational processes?
 - On check lists, for example
 - *Unresolved, please let us know if you have any suggestions!*

Challenge #2: Include gTLDs

- Open up TLD-OPS for new and legacy gTLDs?
 - 1.000+ TLDs to be expected (57%*1.500 nTLDs + 170 ccTLDs)
 - ~65 nTLD back-end operators (1.500 nTLDs * 38 RSPs/918 nTLDs)

Pros	Cons
<ul style="list-style-type: none">• Strengthens incident response capabilities of all TLDs• Further increases security and stability of Internet at large• Reach critical mass, making TLD-OPS mandatory for all TLDs	<ul style="list-style-type: none">• Increases heterogeneity of TLD-OPS community• Increases complexity of governance and administration• Might increase ICANN involvement

- Get “room temperature” at ccNSO Members Day tomorrow

Objectives until ICANN56

- Increase the number of ASCII ccTLDs subscribed to the list to 185 by targeting specific ccTLDs with the help of ICANN's Regional VPs
- Get the list to be used more often through our collaboration with ICANN's security team (package and share security alerts)
- Develop a simple procedure for members to update their contact information (320 people on the list)
- Find a ccTLD representative from the Asia-Pacific region by approaching APTLD

Q&A

TLD-OPS Members

Frederico Neves, .br

Jacques Latour, .ca

Erwin Lansing, .dk

Ali Hadji Mmadi, .km

Cristian Hesselman, .nl (chair)

Abibu Ntahigiye, .tz

Warren Kumari (Liaison to SSAC)

John Crain (Liaison to ICANN's security team)

Kim Davies (Liaison to IANA)

ICANN Staff

Kim Carlson

TLD-OPS Home

<http://ccnso.icann.org/resources/tld-ops-secure-communication.htm>

Cristian Hesselman

+31 6 25 07 87 33

cristian.hesselman@sidn.nl

@hesselma