ICANN 80 POLICY FORUM

Joint Session
SSAC and ALAC

11 June 2024

Agenda

- **Welcome and Opening Comments - Jonathan Zuck, ALAC Chair and Ram Mohan, SSAC Chair (5 mins)**
- **The Safer Cyber Campaign (25 minutes)**
  - Overview of SAC074 and its Relevance to Registrants (Merike Kaeo, SSAC)
  - Brief update on OCTO on Credential Management Training (Yazid Akanho , ICANN OCTO)
  - Discussion on Disseminating SAC074 (Jonathan Zuck, ALAC Chair and Ram Mohan, SSAC Chair).
- **Briefings on SSAC Advice on Name Collision Analysis (25 minutes)**
  - Overview of NCAP Study 2 Report and SAC124 (Matt Thomas / Suzanne Woolf)
  - Overview of SAC124 (Ram Mohan)
  - Discussion: What is the risk of data manipulation and name collisions?
- **Closing Comments and Next Steps - Jonathan Zuck, ALAC Chair and Ram Mohan, SSAC Chair (5 mins)**

Safer Cyber Campaign (Let’s start with SAC074)

Merike Kaeo, Yazid Akanho, Ram Mohan

Why Advisory on Credential Management?

- Existing Advisories
  - SAC040 - Measures to Protect Domain Registration Services Against Exploitation or Misuse (Aug 2009)
  - SAC044 - A Registrants Guide to Protecting Domain Name Registration Accounts (Nov 2010)
- Credential Compromise Still a Significant Issue
  - https://ccnso.icann.org/en/meetings/durban/workshop.htm
  - DNS Hijacking by Maarten Van Horenbeeck
    - One of top 3 issues is registrar account compromise: “Attacker attempts to authenticate using a list of frequent passwords, or using password stolen from another registry authentication database.”

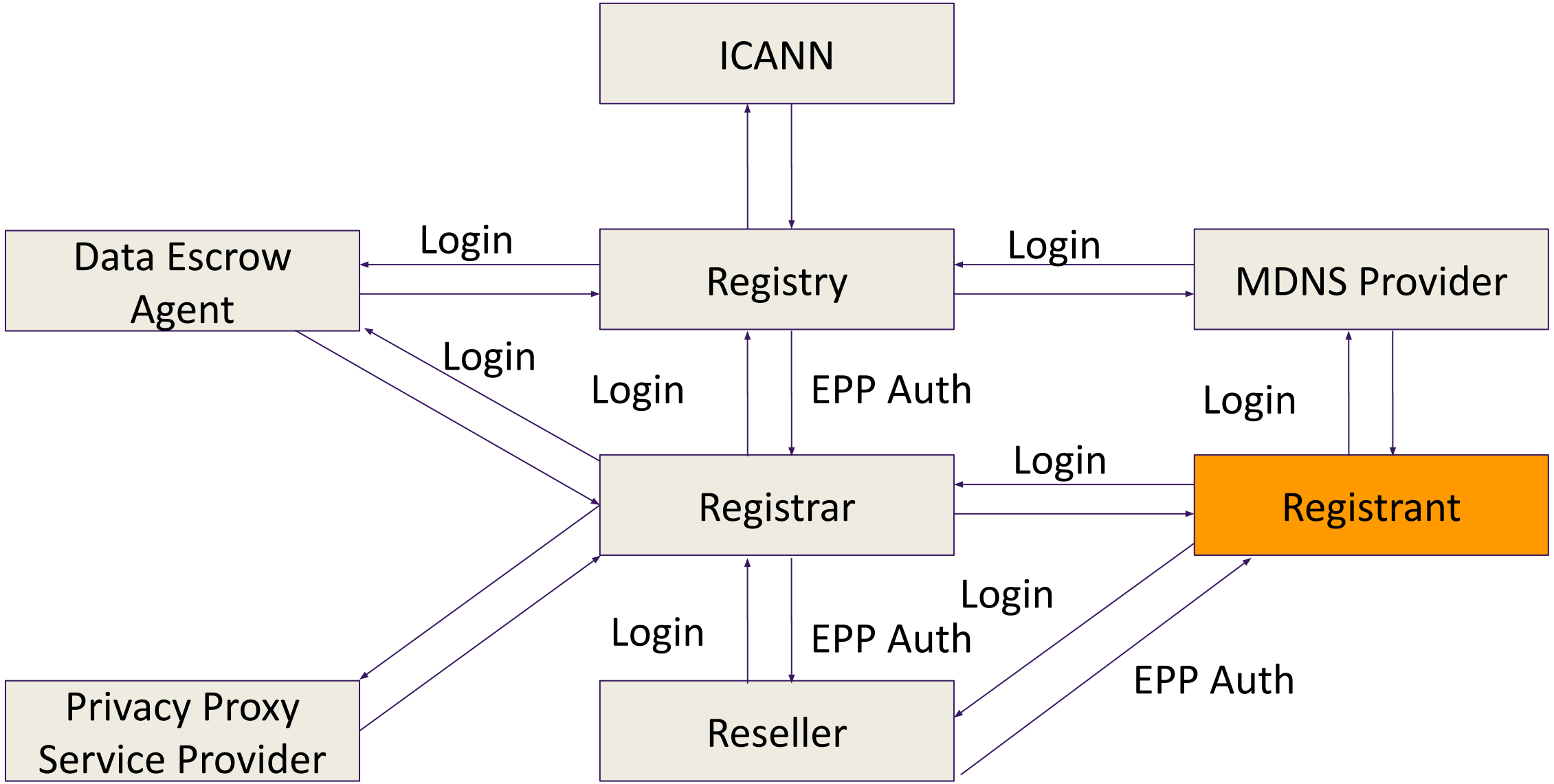
DNS Ecosystem Credential Types and Purpose

Credential	Purpose of Credential	Entity Using Credential	Entity Validating Credential
EPP AuthInfo code	Initiate registrar-to-registrar transfer	Registrant, Registrar / Reseller	Registry
Registrant username and password at registrar / reseller	Access to domains, DNS settings, payment methods, etc.	Registrant	Registrar / reseller
Username / password and certificate for registry access	Gives registrar access to TLD registry. SSL certificate and encryption required for communication between the Registrar's client system and the registry; authentication by user/pass required for session establishment.	Registrar	Registry
IP Addresses	Controls access to registry; access is restricted from known registrar IPs via address filter.	Registrar	Registry
Payment credentials (credit card number and CVV code, etc.)	Pay for services	Registrant	Registrar / Reseller, payment processor
Privacy/proxy account	Privacy/proxy services are designed to mask data about the registrant and other domain contacts so that it is not published in WHOIS. Data about the underlying contact is stored at the service provider, which may or may not be associated with the domain registrar.	Registrant, Registrar, Privacy / proxy service provider	Registrant, Privacy/proxy service provider

DNS Ecosystem Credential Types and Purpose(2)

Credential	Purpose of Credential	Entity Using Credential	Entity Validating Credential
Registrar account funding credentials. May involve bank account numbers, credit card account details, etc.	Transaction accounts at registries; each time the registrar performs a billable transaction.	Registrar, Registry	Registry, bank
Registry-registrar security passphrases and service usernames and passwords.	Authenticate the registrar's requests to tech support, finance department, etc.	Registrar	Registry
Registrar-registrant - security passphrases, PIN numbers, and service usernames and passwords.	Authenticate the registrant's requests to the registrar.	Registrant	Registrar
Credentials for access to registry's or registrar's internal systems or hardware	May involve usernames/passwords; firewalls and VPNs; and/or two-factor methods such as security tokens, biometrics, ID documents, etc.	Registrar or Registry	Registrar or Registry
DNSSEC Key-Signing Key (KSK)	A key that signs the set of all keys for a given zone, including itself	Registrants, Registrars and Registries	Registrants, Registrars, and Registries
DNSSEC Zone-Signing Key (ZSK)	A key hat signs data within a given zone	Registrants, Registrars and Registries	Registrants, Registrars, and Registries

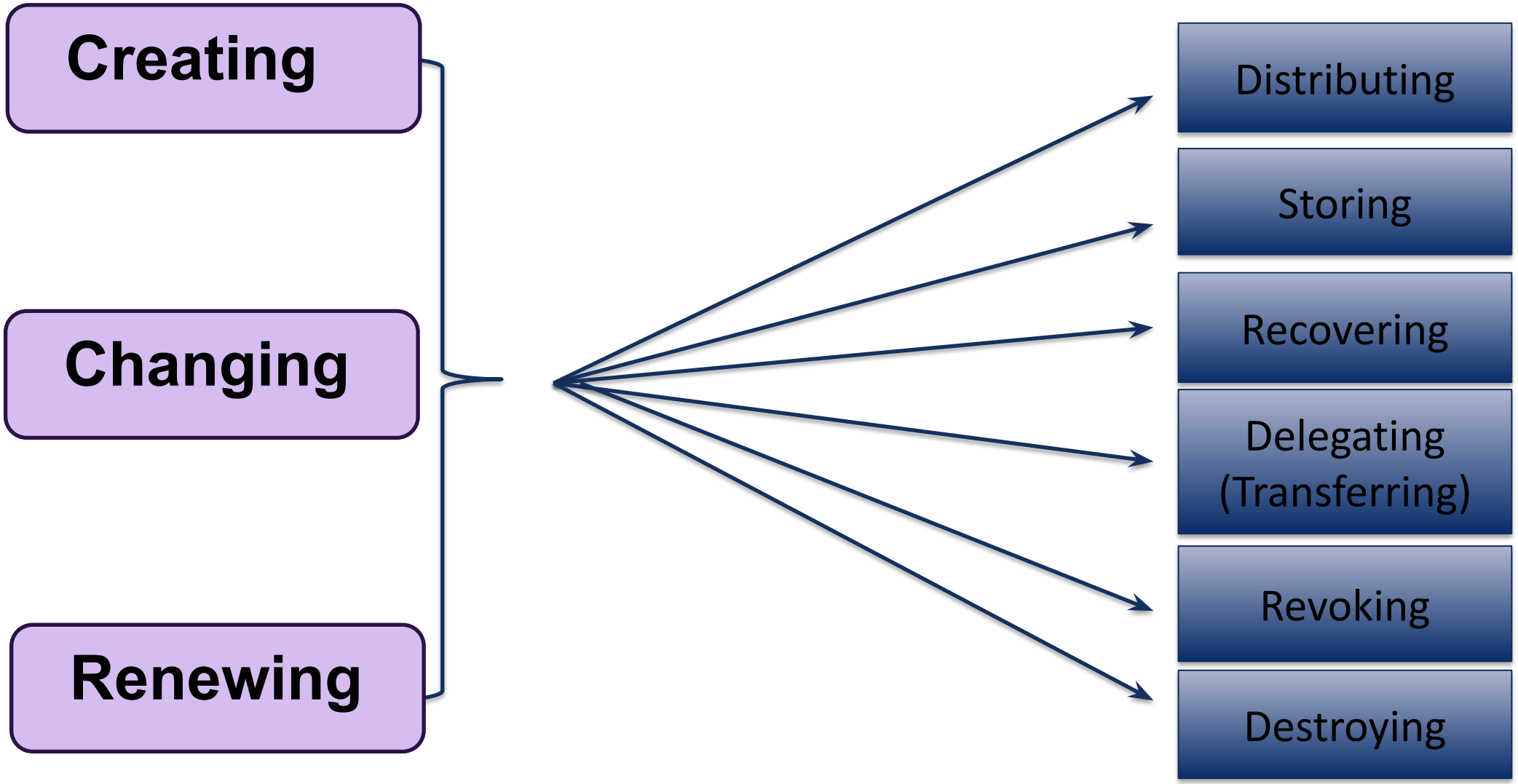
DNS Ecosystem Credentials



How Credentials Get Compromised

- Being victim of a phishing attack
- Laptop gets stolen
- Sharing your password with another person
- Re-using same password on many systems
- Spyware on your computer installed a keylogger
- Storing your private key in an easily accessed file
- Sending credentials in cleartext emails
- Unpatched security vulnerabilities are exploited

Credential Management Lifecycle



Multi-Factor Authentication

- Multi-factor authentication provides added layer of protection
- Varying types of MFA
  - Universal 2nd Factor (U2F)
  - Time based onetime passwords (TOTP)
  - HMAC-based onetime passwords (HOTP)
  - SMS Passcode
  - Phone Based Verification
- One good registry study is from Brazil
  - https://community.icann.org/display/CMTP/How+to+Guides

SAC074

- **SAC074 provides best practice guidelines to registries, registrars and registrants on protecting the credentials**
  - Explores the set of credentials a registrant manages
  - Introduces a credential management life cycle framework
  - Applies the framework on how to protect the registrant credentials
- **Recommendation 4: The ICANN Board should direct ICANN staff to facilitate global hands-on training programs for registrars and registries based on the best practices outlined in Section 6 of this document, with the goal to enable parties to learn practical operational practices for preserving security and stability of the credential management lifecycle.**

Brief update on OCTO on integrating credential management into ICANN training courses

ICANN 80 - Joint Session: ALAC and SSAC

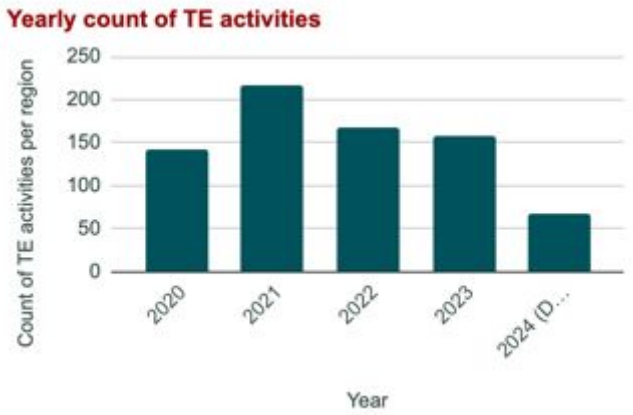
Yazid Akanho
Technical Engagement
Office of the CTO

June 2024

Technical Engagement: who we are ?

- A team within OCTO, mainly in charge of DNS secured operations outreach, training, capacity building and capacity development programs:
  - Develop and deliver technical content on DNS, DNSSEC, DNS security.
  - A more digestive approach: presentations, webinars, hands-on.
  - Language diversity: English, Spanish and French.

- Regionalized team to better align regional specificities and ICANN Strategic Goals.
  - Audience: ccTLDs, registrars, DNS hosting providers, ISPs, MNOs, Governments, LEAs, NOGs, Universities, …
  - Similarities and differences in needs and expectations from regions.



Courses containing Credential Management modules

Technical Engagement Training Course Catalog

If you are interested in having the Technical Engagement team present any of the courses listed in this catalog, or would like more information, please do not hesitate to contact us.

Course Code	Course	Description
TE01	ICANN's Technical Mission	PDF
TE02	DNS101	PDF
TE03	DNSSEC101	PDF
TE04	Advanced DNS	PDF
TE05	Advanced DNSSEC	PDF
TE06	Registry Operations for ccTLDs	PDF
TE07	OSINT: Fighting DNS Abuse (DNS Abuse for LEAs)	PDF
TE08	DNS Abuse: Threats and Mitigation	PDF
TE09	Introduction to RDAP for Domain Names Registrations	PDF
TE10	DNS Ecosystem Security	PDF
TE11	DNS for Internet Service Providers	PDF
TE12	Network Operation Security	PDF
TE13	UA: Email Address Internationalization (EAI)	PDF
TE14	UA: Universal Acceptance for Java Developers	PDF
TE15	Credential Management Lifecycle: Operational Best Practices	PDF

https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en

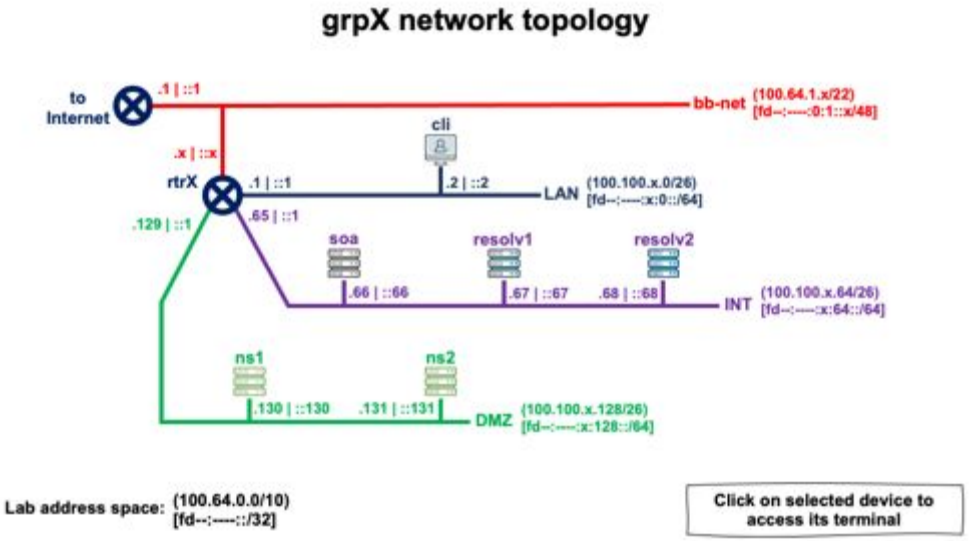
Request training and hands-on : email us at OCTO@icann.org

The Credential Management Lifecycle TE course

- **Description**: introduces the concept of ”credential” and its various lifecycle phases; exposes the management considerations and discusses the best practices considerations.
- **Audience**: Engineers, DNS administrators, Policy personnel
- **Duration** (online presentation): 2 hours (full hands-on lab material development in the pipe)
- **Prerequisite Courses**: DNS 101
- **Expected outcomes**: understand the credential management in detail, focusing on DNS.
- **Course Outline (default)**
  - Introduction to credentials and credential management
  - DNS Ecosystem
  - Compromises in the DNS Ecosystem
  - Credentials used in DNS
  - Credential Management Lifecycle
  - Credential Management Best Common Practices

The online lab platform quick overview

- A set of LXC containers running on AWS LightSail/EC2.
- Connect from anywhere: browser + Internet.
- Efficient:
  - Fast deployment compared to physical infrastructure.
  - Simultaneous multiple deployment.
- Scalable:
  - Parallel trainings (different audiences, configuration, and locations).
  - integration to ICANN learn (under analysis).
- 'Hardwareless':
  - hardware fault risk limitation: loss, physical damage, cabling, power issues, etc.
  - Helpful in locations with hardware restrictions or infosec cyber risk.



Discussion

- How could ALAC help to disseminate / amplify the SAC074 message to the registrant community?
- What are the roles SSAC, ICANN Org should play?

SSAC Advice on Name Collision Analysis

Matt Thomas, Suzanne Woolf and Ram Mohan

Problem Statement

- Name collisions can disrupt network traffic, expose sensitive data, and create attack surfaces in unmitigated collisions for malicious actors to exploit vulnerabilities.
- New technologies and evolving usage patterns introduce unforeseen collision scenarios
- Growing number of TLDs increases the likelihood of collisions
- Current methods for identifying name collisions are insufficient for several reasons:
  - Reliance on root server data, which is less informative than in 2012 due to advancements in DNS protocols, increase in IPv6 adoption, and legislative restrictions for Root Server Operators
  - Often reactive and decentralized, leading to inconsistent and incomplete protection
  - Decentralized approach lacks consistency as individual registries may not have the resources or expertise for thorough evaluation

Proposed Name Collision Risk Assessment Framework

NCAP Study 2 proposes a new **Name Collision Risk Assessment Framework** to address the documented limitations of the previous management framework.

Key Features:

- **Integrated Risk Assessment:** Embeds name collision assessment into the broader review process for new gTLD string applications.
- **Technical Review Team (TRT):** Introduces a dedicated team to evaluate proposed new gTLD strings based on empirical analysis.
- **Enhanced Data Collection:** Encourages the collection of additional quantitative and qualitative data from publicly available datasets for a more comprehensive risk assessment.
- **Multiple Assessment Methods:** Offers four methods for collecting and analyzing data to assess risk.

Proposed Process

Stage 0: Pre-Application

Applicants encouraged to proactively assess potential name collisions by reviewing publicly available data.

Helps identify potential conflicts as early as possible.

Stage 1: Initial Risk Assessment

TRT reviews publicly available data to assess the initial risk of name collisions

If “high risk:”

- TRT submits a recommendation to the ICANN Board, OR
- Applicants may propose mitigation plan for the TRT's review

Other applications proceed to Stage 2

Stage 2: Name Collision Assessment

ICANN temporarily delegates the TLD string to the root zone.

TRT conducts one or more of the following assessments:

- No Interruption
- Controlled Interruption
- Visible Interruption
- Visible Interruption and Notification

Stage 3: Board Decision

TRT submits risk recommendation to the ICANN Board; applicant may propose mitigation plan for TRT review

ICANN Board makes the final decision on approving the application or potentially assigning the string to the Collision String List.

Data Collection

You can't simply re-use the Collision detection methods you used in 2012.

- Controlled Interruption as implemented in the last round does not work for IPv6
- Root servers & Resolver operators have much less data now than in 2012
  - ➜ Due to technology and regulatory changes

To seriously analyze name collisions, you must collect data from a variety of sources.

- Impossible to build a generalized case for root causes
- Impact assessment may require large amounts of data over significant periods of time
- ICANN org has expressed concerns about risks to privacy and confidentiality with some of the proposed data collection methods
  - ➜ These concerns need to be thoroughly understood and addressed as the DG recommendations move towards implementation.

Technical Review Team is Critical

Properly evaluating name collision is a highly skilled activity

- There are no generalized solutions for name collision
- The TRT needs to be able to adapt to changing internet infrastructure

To ensure TRT's success

- Building a team with the right skills to perform the assessment is critical
- The TRT needs ready access to historical as well as longitudinal data in order to perform its assessment
- TRT needs to be given the full ability to determine assessment methods and the data needs of that assessment.

SAC124: SSAC Advice on Name Collision Analysis

- **Multiple privacy risks when considering name collision analysis**
  - ➔ **Delegation Risk:** High risk of exposing personal data in collisions go unnoticed during normal operation
  - ➔ **Assessment Risk:** Privacy risks associated with the execution of data collection needed to assess collisions
- **Trade-Offs:**
  - ➔ Avoiding Assessment Risk is a mistake—it leaves Delegation Risk unaddressed, compromising security and stability of the DNS
  - ➔ Focus on the bigger threat and prioritize mitigating Delegation Risk
  - ➔ Implement safeguards to protect collected data during assessment (data minimization, clear data handling policies)
- **SSAC Recommendations:**
  - ➔ Adopt the Proposed Framework with safeguards to address privacy concerns.
  - ➔ Prioritize mitigating Delegation Risk for a secure and stable next-gen gTLD rollout.

Addressing Privacy Concerns

- SSAC acknowledges ICANN org's privacy concerns and emphasizes:
  - Name collisions pose inherent privacy risks, and ignoring them doesn't eliminate these risks, it merely transfers them to others, potentially leading to greater harm
  - ICANN's role in ensuring the stable and secure operation of the Internet's unique identifier systems requires data collection to make informed decisions and proactively mitigate security and stability risks
- Proposed Framework's proactive approach is essential for protecting user privacy by minimizing the potential for harmful name collisions
- Proposed Framework itself does not explicitly detail how to balance privacy and SSR risks
  - The Board has the opportunity to ensure this balance is achieved by design through oversight of the Proposed Framework’s implementation
- SSAC welcomes the engagement from ICANN org and is committed to offer its expertise throughout the implementation process

Discussion

- What is the risk of data manipulation in name collisions?

Any Other Business