Credential Management Lifecycle: Operational Best Practices

Yazid AKANHO
ICANN OCTO/TE

POLL

Compromised credentials are at the top of data breaches

1. True
2. False

Course Description

- Attacks in the DNS landscape continue to be a significant problem for registries, registrars, registrants and the users of their sites.
- This training course will discuss the best practice guidelines that can help these parties to enhance the security of domain names and the systems that support them and explains the credential management lifecycle in detail.
- It is an outcome of the recommendations from the ICANN SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle.
- It is primary intended to DNS infrastructure, but these best practices apply overall to other infrastructures such as RIR.

Agenda

- Introduction to Credential Management
- DNS Ecosystem
- Compromises in the DNS Ecosystem
- Credentials used in DNS
- Credential Management Lifecycle
- Credential Management Best Common Practices

Introduction

What is a Credential?

- A cornerstone of all security strategies is an organization's ability to control access to data and systems.
- Virtually all **access controls** rely on the use of credentials to validate the identities and permissions of users, applications, and devices.
- A credential is a data that is transferred to establish the claimed identity of an entity (user, device, application, ...)
- for authentication purposes, access control, integrity checking, and/or confidentiality.

Types of Credentials

- **Physical World**
  - Passport
  - Drivers License

- **Virtual World**
  - Passwords/Passphrases
  - Digital Certificates
    - cryptographic keys based on a **public and private keys** are used for authentication and digital signatures.
  - Security tokens
    - Typically one-time-passwords or PINs generated via a physical device (e.g. hardware token) or via a program running on a computer (e.g. software token).
  - Biometric attributes
    - Identify a user by a feature of their biology, including fingerprints or iris scans.

Why Credential Management?

- Credentials hold significant potential for abuse if not appropriately managed
- Bad actors can misappropriate credentials
- Has emerged as a serious business challenge that goes far beyond traditional password management

Credential Compromise in the News

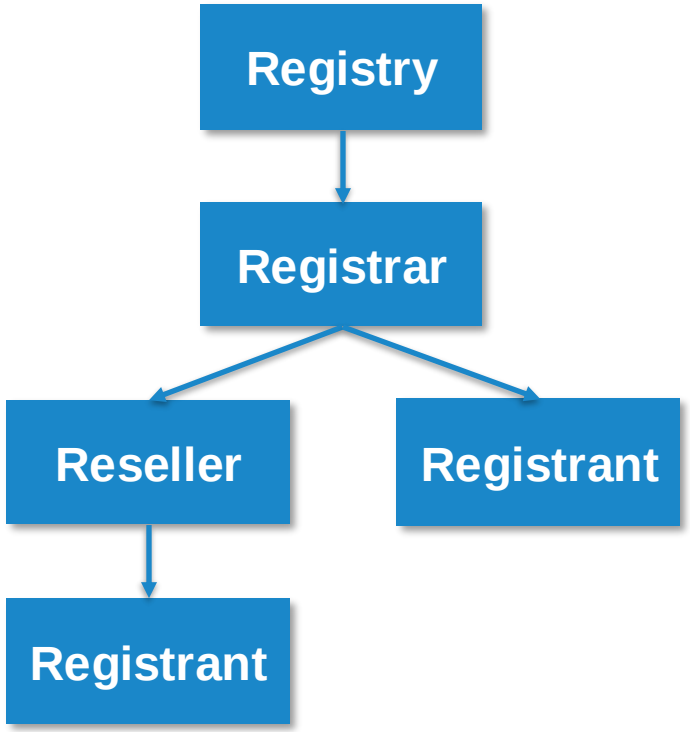
How Credentials Get Compromised

- Phishing attack
- Stolen laptop
- Shared password
- Re-using same password on multiple 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
- Cracked or hacked due to weak credentials etc.

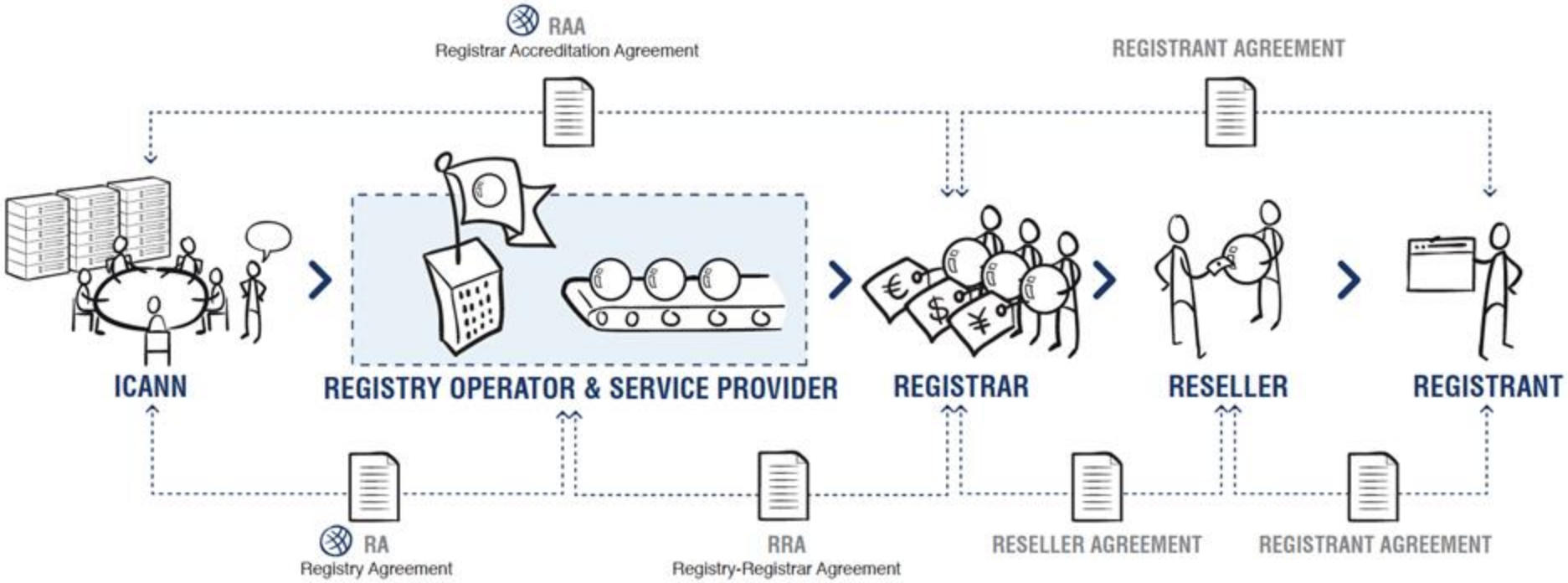
DNS Ecosystem

DNS Ecosystem Players

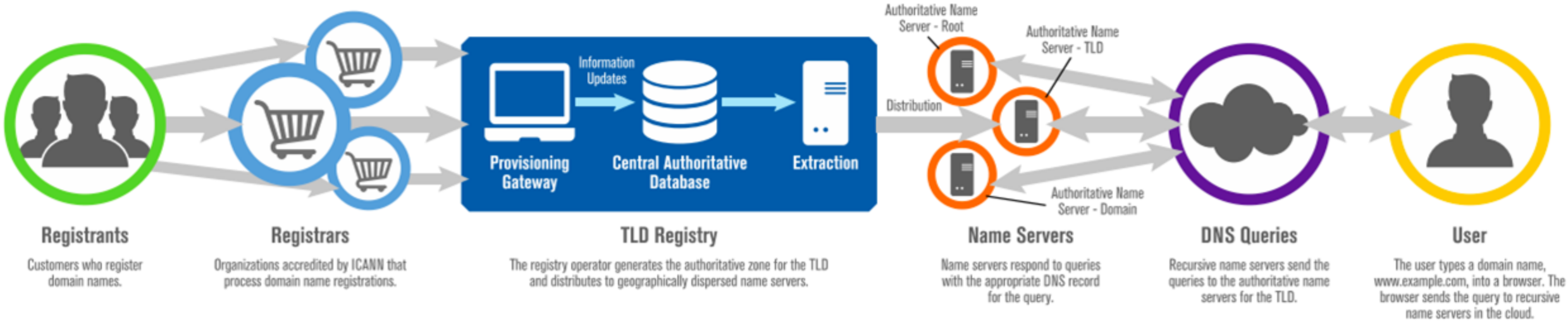
- **Registry**: Database of domain names and registrants
- **Registrar**: Primary agent between registrant and registry
- **Registrant**: A holder of a domain name registration



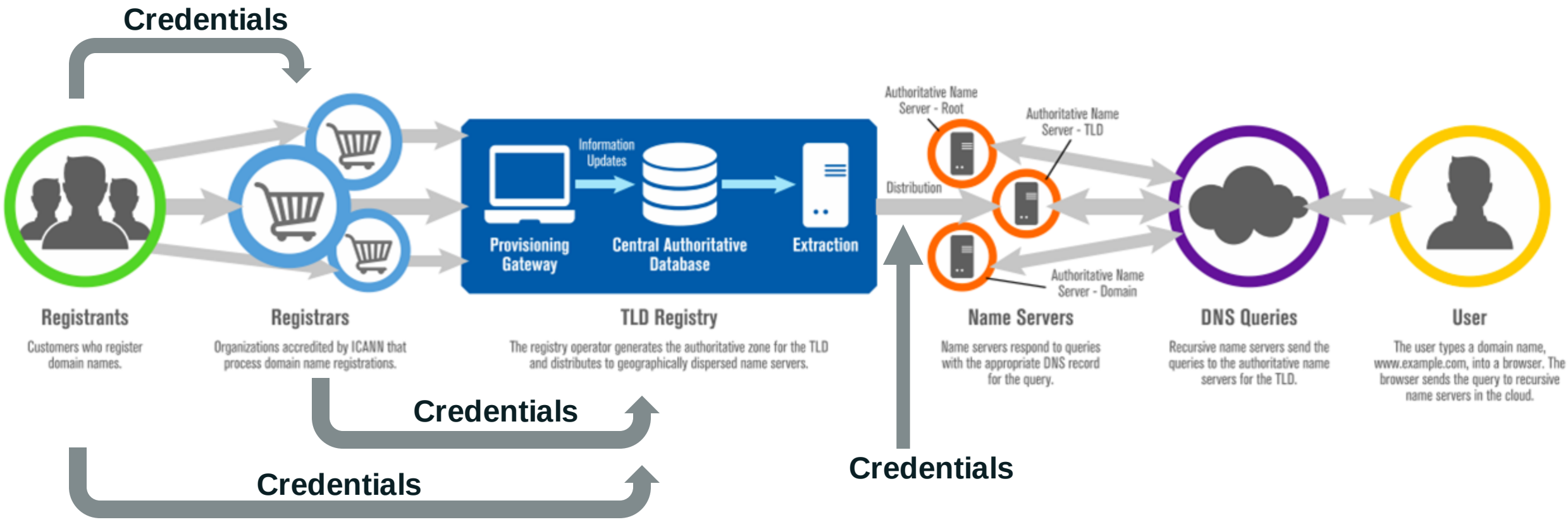
DNS Ecosystem - Relationships



The DNS Ecosystem – How it works



The DNS Ecosystem – Where Credentials are used



DNS Ecosystem and the Credential Management

- Credential management in DNS to preserve security and stability in domain name management ecosystem
  - DNS Services (e.g. running DNS zones)
    - DNS Service Providers
    - Registries
  - Name Provisioning services (e.g. registration services)
    - Registries
    - Registrars
    - Resellers
    - Privacy Proxy
  - Name Usage (e.g. web hosting services)
    - Hosting facilities

Compromises in the DNS Ecosystem

Compromises in the DNS Ecosystem

- **Registrant Compromise**
  - Allow attacker to pose as registrant and change domain data, Registrant data or DNS settings of domain names
  - Can severely disrupt business operations and cause significant financial and reputational harm
- **Registrar Compromise**
  - Attacker breaks into registrar system and change customer data
  - The compromise of an entire registrar is highly critical as all customer data and systems can be exposed
- **Registry Compromise**
  - Attacker can modify any domain data administered by the registry
- **Note**: Here we refer to data beyond WHOIS/RDAP. (e.g. technical data accessible on their portals)

Compromises in the DNS Ecosystem

- **Phishing and Spear Phishing Attacks**
  - High-value credentials that allow access to critical systems or data such as those held by the staff members of a registrar or registry can be targeted through spear phishing
  - A successful detection strategy is to identify suspicious access patterns

- **Watering hole Attacks**
  - A targeted attack to **compromise** users within a specific organization or group by infecting websites they typically visit.
  - Goal is to **infect** the user's device with malware and gain access to the organizations network.

Compromises in the DNS Ecosystem

- **Domain Shadowing**
  - Using stolen or phished credentials, the malicious actors **create numerous subdomains** associated with existing, reputable domains in the registrant's portfolio
  - The new subdomains are pointed to IP addresses that further **serve up malicious content** such as malware and ransomware
  - Registrants may not regularly monitor for additions to their zone data, and their existing legitimate DNS entries continue to function normally
  - These malicious subdomains often go **unnoticed** for extended periods of time

Example Compromise

1. Attackers need only guess, phish, or apply social engineering techniques on a single point of contact to gain control of a domain registration account.

2. Once the attackers compromise the user account and password, attacker can gain control of an organization's entire domain name portfolio including zone file data.

3. Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL injection). A successful exploit of vulnerable application code can result in the disclosure of account credentials for many domain accounts.

4. Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity.

Example Compromise - contd

5. Attackers can block delivery of email notifications to targeted registrants by altering DNS configuration information.

6. Even when unauthorized modification of DNS information is discovered quickly, the process of restoring DNS information to correct for a malicious configuration can be a lengthy due to the distributed nature of the DNS and related TTL values.
   - These information are stored in recursive resolver caches which are not under the registrant or registrar control and are distributed in thousands of networks.

Deficiencies in Credential Management

- Failure to change the default credentials on certain systems
- Re-using the Same Username/Password Combination
  - Users employ the same username/password combination across different accounts or on different websites
- When personnel turn over at registrars, registries, or corporate registrants the departing person sometimes provides all access information to their successor
  - If the successor doesn't change the credentials, it allows the former employee to potentially still have access to the registrar account

Deficiencies in Credential Management

- Storing and Sending Credentials in Cleartext
  - Credential data is sensitive and needs protection both in transit and at rest to minimize the chance of disclosure
  - Insecure transmission of credentials includes,
    - Unencrypted email
    - Unencrypted browser sessions
    - Sending passwords over the phone etc.

Deficiencies in Credential Management

- Incident Response Errors
  - Registrants can discard the emails that notify them of the breach as a suspected phish.
    - Registrants should **know the format** of incident response notifications ahead of time
    - Notification emails should come from a **trusted and recognizable** domain name, digitally signed, and the password change service is on a known site
    - Registrant is to have an "**out of band**" communication method with registrars/registry so that even if the domain is compromised they can still receive notifications
    - Registrars should have **more than a single way** to notify the registrants

Credentials used in DNS

Credentials used in DNS

- For registrants to prove their identity and authenticate to DNS operators, registrars etc.
- Once authenticated, registrants can:
  - Register new domains
  - Transfer ownership
  - Remove existing domains
  - Modify DNS records etc.

Credentials used in DNS

- **User ID**
  - Unique character string (often an email address) used by a system to identify a specific user
- **Password/Passphrase**
  - A string of characters from a set of acceptable characters that is a secret shared between a user (client) and the systems (servers) to which that user authenticates.
- **Public/Private Keys**
  - An encryption and authentication scheme based on a pair of cryptographic keys that is owned by each party
- **Symmetric Keys**
  - An encryption or decryption key that is known only by authorized parties (i.e. two parties share the same secret key)

Credentials used in DNS

- **Digital Certificates –** To certify the ownership of a certificate associated with a domain name
  - Associates a public key with the identity of a process or system as verified and signed by a trusted entity, called a Certificate Authority (CA)
  - CA is an independent third-party whose primary function is to certify the ownership of a certificate associated with a domain name
  - Any CA must have mechanisms in place to verify what it is that they are signing.
  - The strength of the verification defines the protection level of the certificate.
  - An entity validating a digital certificate must be able to check the digital signature by using the public key of the trusted signing entity
  - These public keys are pre-installed in web browsers and operating systems.

Credentials used in DNS

- **Domain AuthInfo Code**
  - A secret code shared between a registrar and a registrant
    - Registrar and Registrant have to keep and process this code securely
  - A measure designed to **prevent unauthorized domain transfers.** The registrar relies on the code to initiate the transfer of a domain name from another registrar
  - In gTLDs, every registrar is required by ICANN's Inter-Registrar Transfer Policy to give the AuthInfo code to the registrant
  - Registrant can give it to any other registrar to initiate a valid transfer request

Credentials used in DNS

- **Multi-Factor Authentication**
  - Combining at least two methods of proving an identity from three distinct categories:
    - Something you **know** (commonly a password or a passphrase)
    - Something you **have** (e.g. a value displayed by a security token fob, or a one- time password sent to a known mobile phone number)
    - Something “that you **are**” (something about you that is unlikely to change over time, such as a biometric attribute).
  - Many variations on how and when a multi-factor model could be implemented
    - Especially the web application environments could benefit from the proper implementation of such a methodology

Credentials used in DNS

- **One Time Password (OTP)**
  - A password that is valid for only one login session or transaction on a digital device
  - An OTP might be generated by a hardware token or a software module.
  - Another method of using an OTP is for the authentication server to send it to the user via an out-of-band trusted communications channel
    - OTP applications such as Google Authenticator, Microsoft Authenticator, Duo etc.

Credentials used in DNS

Credential	Purpose of Credential	Entity Using Credential	Entity Validating or Storing the 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/password required for session establishment.	Registrar	Registry
IP addresses	Controls access to registry; access is restricted to known registrar IP addresses via address filters (Access Control Lists).	Registrar	Registry
Payment credentials (credit card number and CVV code, etc.)	Payment for services	Registrant	Registrar/Reseller, payment processor

Note: Entities can also be DNS service providers that are not registrars

Credentials used in DNS

Credential	Purpose of Credential	Entity Using Credential	Entity Validating or Storing the Credential
Registrar account funding credentials. May involve bank account numbers, credit card account details, etc.	Transaction accounts at registries; used each time the registrar performs a billable transaction.	Registrar, Registry	Registry, bank or payment processor
Registry-registrar security passphrases and service usernames and passwords.	Authenticate the registrar's requests to registry tech support, finance department, etc.	Registrar	Registry
Registrar-registrant - security passphrases, PIN values, 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	Authenticate authorized individuals to internal resources.	Registry or Registrar	Registry or Registrar

Note: Entities can also be DNS service providers that are not registrars

Credentials used in DNS

Credential	Purpose of Credential	Entity Using Credential	Entity Validating or Storing the Credential
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.[30]	Registrant, Registrar, Privacy/proxy service provider	Registrant, Privacy/proxy service provider
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 that signs data within a given zone	Registrants, Registrars and Registries	Registrants, Registrars and Registries

Note: Entities can also be DNS service providers that are not registrars

Credential Management Lifecycle

Credential Management Lifecycle

- **Why?**
  - For their initiation, maintenance and associated support
- Credentials must be **protected at all stages** of this lifecycle, from creation to destruction
- Each phase of the lifecycle has its own **challenges**, **requirements**, and **recommendations**.

Credential Management Lifecycle

- **If registry/registrar allowing credit cards or direct debit access methods,**
  - Special care should be taken regarding the holding and management of credentials associated with credit cards and banking information
  - Payment Card Industry Data Security Standards (PCI DSS) must be met.
  - PCI DSS provides a comprehensive baseline of credential management and security measures, and are updated by the major credit transaction networks periodically

Credential Management Lifecycle phases

1. Designing
2. Creating
3. Distributing
4. Storing
5. Changing
6. Renewing
7. Transferring
8. Revoking
9. Recovering
10. Destroying.

Credential Management Best Common Practices

Some Questions To Consider

- Do you utilize two-factor authentication?
- How do you store credentials, and how do you manage your backups?
- What do you do with credentials of users who are no longer customers?
- Do you force customers to change their passwords?
- What do you consider adequate password strength and username types?

Some Questions To Consider

- What type of system are you using for password recovery? What are the options to authenticate the entity?
- How do you ensure customer compliance?
- What kind of know-your-customer programs do you have to review credentials and make sure everything is up to date?
- What kind of measures do you employ to detect compromised credentials, or attempts to compromise them (e.g. brute-force attacks)?

POLL

How many stages a credential could go through during their lifecycle ?

1. 2
2. 5
3. 10
4. 20

Credential Management Best Common Practices

- There are practical improvements that can be made to all stages of the credential management lifecycle
- Registries and Registrars are recommended to refer to community vetted and standards-based documents
  - CIS Critical Security Controls
  - ISO 27000 family of standards
  - ISO 27001 - requirements for an Information Security Management System (ISMS)
  - ISO 27002 - best practice recommendations on information security management
  - PCI DSS provides a comprehensive baseline of relevant credential management and security measures
  - W3C guide to help implement strong multi-factor authentication
  - NIST SP 800-57 Rev. 5 - Recommendation for Key Management
  - NIST SP 800-63B - Digital Identity Guidelines, Authentication and Lifecycle Management

Credential Management BCP - Designing

- Design should include risk assessment and incident response plans
- Carefully designed multi-factor authentication system is important
  - e.g. text messages containing a PIN to a customer-authorized mobile phone number, OTP applications such as Google Authenticator, Microsoft Authenticator, Duo etc.
- Encourage security-minded credential management
  - Password length and strength
  - Password expiration
  - Password recovery
  - …

Credential Management BCP - Designing

- Decide **how much access** the user has once authenticated, and **how long** until the credential needs to be validated again
  - Providing the least access and least privilege while still permitting the user to perform the task
  - Relatively short inactivity timeout once logged in
- Create and implement an **abuse and fraud detection** plan
  - Can monitor DNS activity to reduce current attacks such as domain shadowing
- Create and implement an **incident response** plan

Credential Management BCP - Creating

- Credential creation involves **trust in policies and procedures**
  - May not be completely tamper-proof
  - The risk must be managed, as it cannot be eliminated
- **Checks and audits** to detect misuse are critical
- Common **creation-time requirements** for cryptographic credentials
  - Intended lifetime
  - How large (in bits)
  - Key protocol

Credential Management BCP - Creating

- **Password requirements** should include:
  - Minimum length (as high as 14-character minimum)
  - Character type mixtures (letters, symbols, and numbers)
  - Prohibitions against repeated characters
  - No password re-use
  - Whether the password is in a commonly used password-cracking table (and thus easily guessable)
  - History of recently used passwords

Credential Management BCP – Distributing and Using

- Credentials must be **protected** while they are distributed to or used by the authorized parties
- Protections include:
  - Transmitting only over an **encrypted channel** (e.g. HTTPS, SSH)
  - Authorized parties should be **limited** to single individuals
  - If multiple individuals share a role, they should still obtain **unique credentials** to better track abuse or misuse
  - Enables simplify reassignment of credentials when only one employee of those with the shared role no longer requires access
  - Attempts to **brute-force attack** password-protected user accounts by supplying entries from a list of commonly used passwords should be detected and mitigated
  - The values of supplied passwords (and incorrect attempted passwords) **should not be recorded in logs**

Credential Management BCP – Storing and Backing Up

- Credentials need to be stored in a way that **minimizes the risk of revealing** them to adversaries during the credential's lifetime
- Passwords/passphrases, private keys, or secret keys should **never be documented in places where this information may be compromised** (e.g. debug logs, wikis or trouble tickets etc.)
- Any storage of a credential should be as a **protected version** so that the credential is not revealed if the file is read
  - Encrypting the data
  - Use of proper authentication protocols
  - Use of one-way functions
- Can use Software credential managers or hardware credential managers

Credential Management BCP – Storing and Backing Up

- Credential manager needs to **store credentials properly** during all phases of their use
- When a credential is used or validated, the validator should store it in memory for as little time as possible, and zero the memory when done
- Backups need to be stored offline or otherwise physically separated to minimize compromise
- Backups can be encrypted with one master backup key. This master key needs to be highly protected
- Registries and registrars should have clear policies and procedures for storing or backing up credentials

Credential Management BCP – Changing

- Registrars and registries should perform 4 steps during credential creation:
  1. **Validate the user** requesting the change: must be a validated authentic user who is allowed to request the change
  2. **Install** the new credential following all the **good practices** applied during the credential creation phase
  3. **Acknowledge** the change with a **message to the user in a medium different** from that used to change the credential and not relying on the credential just changed
  4. **Log the change** but not the value of the new credential.

Credential Management BCP – Changing

- Registrars and registries should apply credential **reuse restrictions**
- If credentials or the credential management system may have been compromised or a breach detected, customers should be **notified and advised to change** their credentials
- Customers should be able to **confirm or authenticate breach notices**, since some may mistake authentic breach notices for phishing attacks
- Breach notification emails should be sent from a **trusted and recognizable domain name**, and the password change service should be on a known site.

Credential Management BCP – Renewing

- Selecting a **frequency** for which customers must renew or change their credentials.
- Stronger credentials, such as hardware tokens and cryptographic certificates, need to be changed less frequently.

Credential Management BCP – Transferring

- Registrars and registries are required to follow ICANN's Inter-Registrar Transfer Policy for handling AuthInfo codes.

Credential Management BCP – Revoking

- Registrars or registries should revoke credentials,
  - When credentials are **compromised**
  - When credentials must be **renewed** (old credential is revoked)
  - When personnel **change roles or depart** the organization.
- Cached credentials cannot be revoked
  - Registrars and registries should **set short cache times**
  - Web sessions or other interactive log-ins should be **actively terminated**

Credential Management BCP – Recovering

- Credential recovery processes are **common targets for adversaries**
- Password recovery processes for registrants require special consideration
  - A domain name can be used to redirect email sent to the domain.
  - Not safe to send credential recovery instructions for a domain to an email address within that domain
- Email accounts may expire due to infrequent use, or the expiration of the associated domain name
  - An adversary can access affected accounts and use the “forgot” process to change the password for domain management
- Registrars should pay attention to non-delivery notices for email sent to email accounts

Credential Management BCP – Destroying

- Credentials, and any information that can be used to recover or create credentials, should be **destroyed when no longer needed**.
- Destruction should include:
  - Overwriting the relevant file with junk
  - Destroying the physical storage media
  - Hardware used to store and process credentials should be shredded or degaussed when it is time for disposal
- Registrars and registries should have well-formed processes to ensure that **all copies** of a credential are destroyed during this phase, **including any backups**.

POLL

What do you consider the biggest challenge in credentials management? (multiple choice)

1. Compliance to regulation
2. Proper permissions management
3. Weaknesses in infrastructure and operations processes and management
4. Human

References and Further Reading

- SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle (SAC074)
  https://www.icann.org/en/system/files/files/sac-074-en.pdf
- Measures to Protect Domain Registration Services Against Exploitation or Misuse (SAC040)
  https://www.icann.org/resources/pages/sac-040-2012-02-25-en
- A Registrant's Guide to Protecting Domain Name Registration Accounts (SAC044)
  https://www.icann.org/resources/pages/sac-044-2012-02-25-en
- Understanding the Payment Card Industry Data Security Standard version 4.0
  https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf
- ICANN Inter-Registrar Transfer Policy
  https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org** Email:

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann

AFRINIC WEBINAR SERIES

Credentials management applied to AFRINIC's members

Presenter: Musa Stephen HONLUE
Date: 17 October 2024

AFRINIC
The Internet Numbers Registry for Africa

https://twitter.com/afrinic
https://www.youtube.com/afrinic
https://facebook.com/afrinic

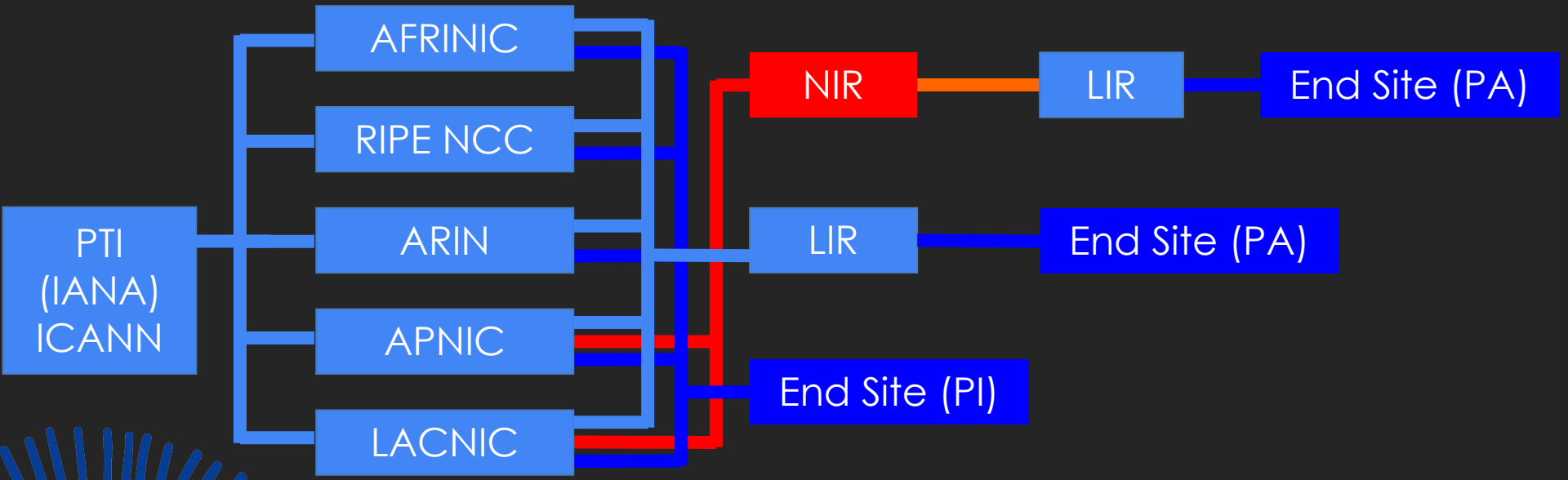
AGENDA

- The RIR Ecosystem
- AFRINIC's systems
- Compromises in the RIR Ecosystem
- Protect your credentials

Corporate Mission:

To serve the African Internet community by delivering efficient services in a global multi-stakeholder environment.

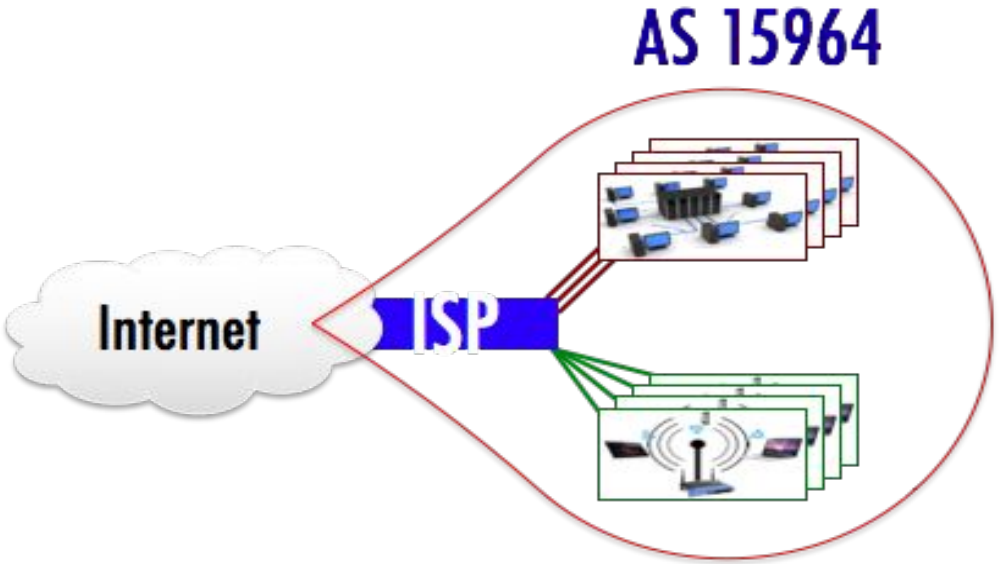
THE RIR Ecosystem



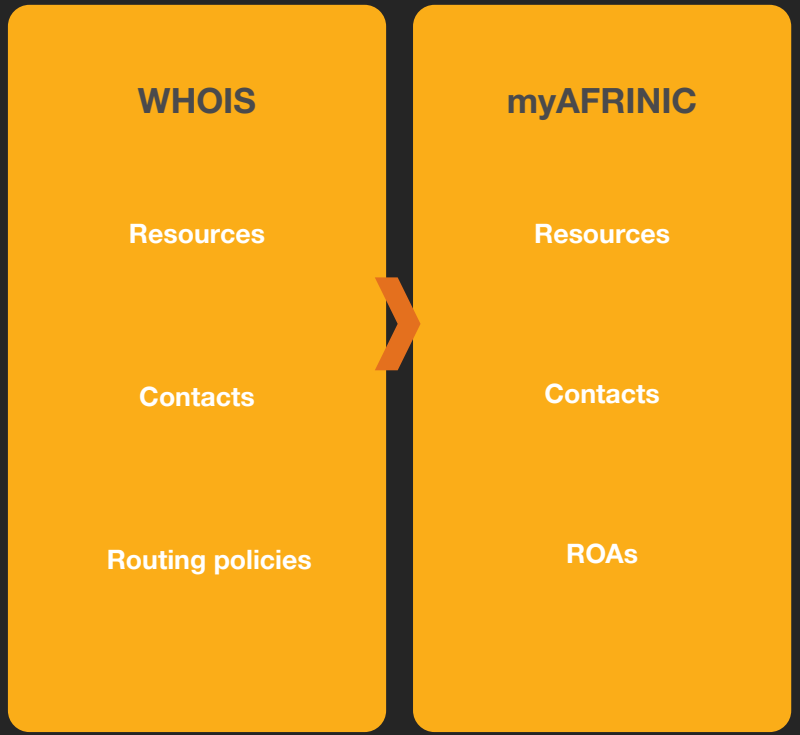
AFRINIC Resources

196.1.0.87

2001:db8:c001::face



AFRINIC main resource management platforms



What Members can do on these portals

WHOIS

Manage resources

Routing policies with route and route6 objects

Security with passwords and gpg keys

MyAFRINIC.NET

Manage resources

Sub-allocations

Assignments

rDNS management

Administrative tasks

Assign roles

Admin

Billing

Voting

Technical

Manage users and passwords

Routing Security

Create and revoke ROAs

Create and revoke IRR objects

AFRINIC and Credentials Management

WHOIS

passwords

GPG Keys

myAFRINIC

Passwords

2FA

RPKI

Certificates

Compromises

RIPE NCC Access: S Investigation

04 Jan 2024 • ripe ncc security news

We are currently investigating the compromise of a
services of the account holder being temporarily im

We have restored access to the legitimate account holder and are work
the integrity of the account. Our Information Security team is continuin
other accounts have been affected. Account holders who might be affe
by us.

We encourage account holders to please update their passwords and e
authentication for their accounts. If you suspect that your account migh
to security@ripe.net.

The risk of sharing your credentials to third parties

Published On - 15 March 2023

This is to alert AFRINIC Resource Members of a misleading email communication from purported representatives of a fictitious organization; targeted at AFRINIC Resource Members ("members"), soliciting them to sign a power of attorney form and surrender their MyAFRINIC portal credentials with them for the purpose of casting a vote for Board Member's seat. Here is an example of such an email.

Dear Mr [redacted]

Thank you for your time over the Phone.

As mentioned My name is [redacted], I am currently running for AFRINIC board position (SEAT 7-Non region)

My main aim when elected to the board will be to work hand in hand with all AFRNIC members to ensure that AFRINC offers fair and equal distribution of internet to number resources to the African internet Community , and to ensure the support of technology usage in order to develop African Internet accessibility and strengthen internet self-governance in Africa.

I kindly request your vote in the upcoming elections to be held in Mauritius, i have attached a Power Of Attorney which gives me a right to vote for myself in the 2023 election .

Please also find my attached profile.

I will highly appreciate your support.

Yours Sincerly,

[redacted] Relationship Manager

The risk

The MyAFRINIC portal is the platform used by members to manage the IP Number Resources delegated by AFRINIC. Access to this platform means that the third party can cast a vote (including for board members' elections) on behalf of the members. Moreover, the access also means one could modify information of the organization, delegated resources, and critical service configurations for Reverse DNS Delegations, RPKI ROAs, and Internet Routing Registry, causing misleading routing information for the global internet. Such access can also be used to trigger resource transfer. This can have serious consequences, not just for your organization, but for the entire Internet community.

Key advice

- Don’t share your password to any other entity.
- Change your passwords on a regular basis.
- Use strong passwords
- Don’t exchange plaintext passwords with your colleagues.
- Use password management systems such as keepassx.
- Ensure your contacts are up-to-date.

Thank You For Your Support and Attention.

Should you have any question in this regard,
please feel free to contact us

AFRINIC Ltd
11th Floor Standard Chartered Tower
19 Cybercity, Ebene | Mauritius
www.afrinic.net

t: +230 403 5100 | f:+230 466 6758