Credential Management Lifecycle: Best Practices

ISPCP & OCTO Capacity Building Webinar Series

Champika Wijayatunga

15 May 2025

Agenda

- Introduction to Credential Management
- DNS Ecosystem and the Compromises
- Credentials used in DNS
- Credential Management Lifecycle and BCPs

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.
- Credentials assert the identity of the user, device or application.

Why Credential Management?

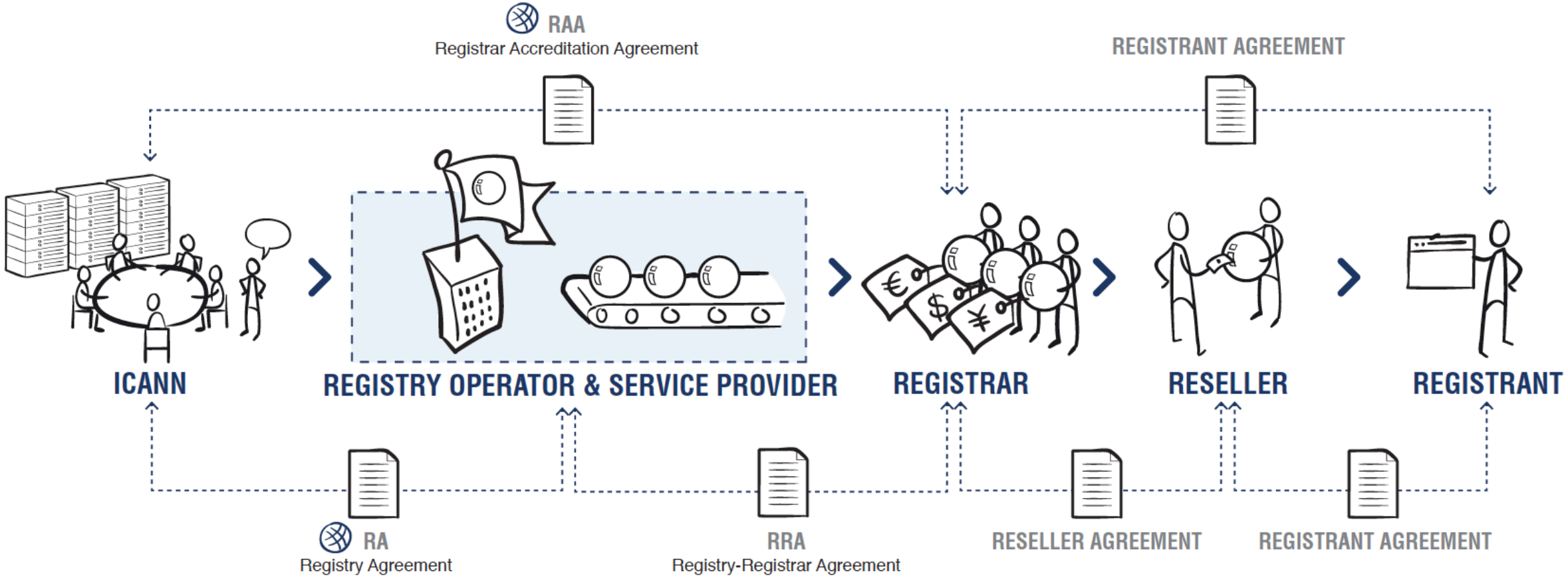
- Credentials hold significant potential for abuse if not appropriately managed
- Bad actors can misappropriate credentials
- Has emerged as a serious business challenge that goes far beyond traditional password management

How credentials get compromised

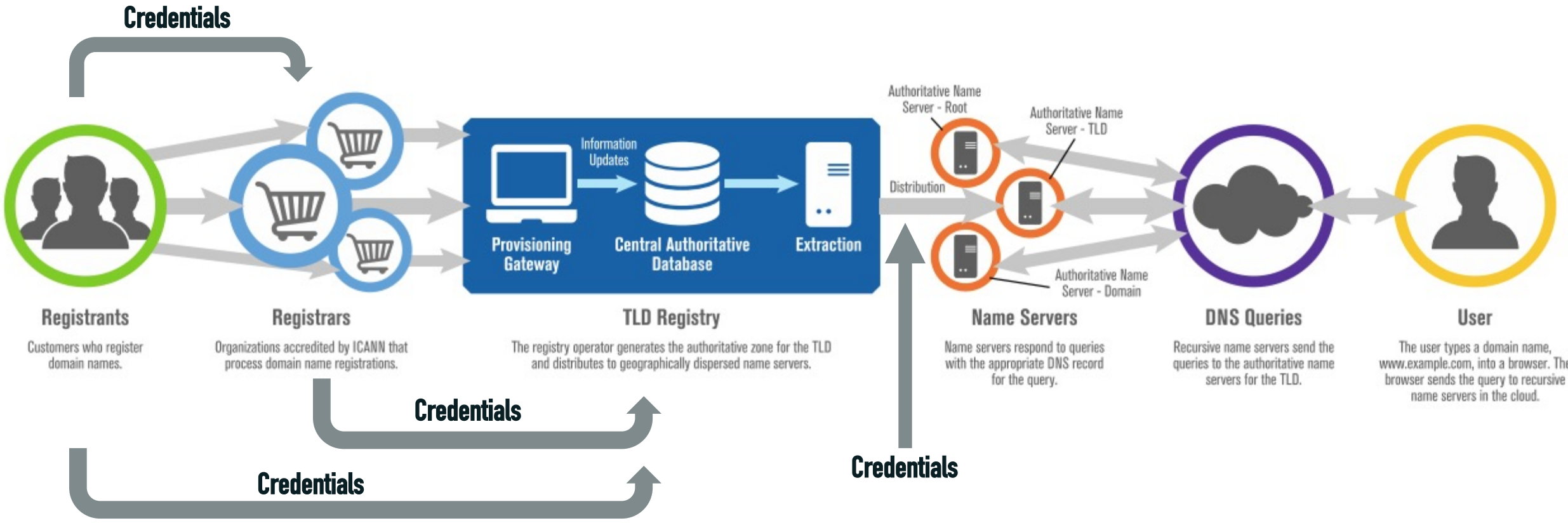
- Phishing attack
- Stolen devices
- Shared password
- Re-using same password on multiple systems
- Spyware on your device installed a keylogger
- Storing your private key in an easily accessed file
- Sending credentials in cleartext emails
- Unpatched security vulnerabilities are exploited
- Cracked or hacked due to weak credentials etc.

DNS Ecosystem and the compromises

The DNS Ecosystem



The DNS Ecosystem – Where credentials are used



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 can 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

Deficiencies in Credential Management

- Failure to change the default credentials on certain systems
- Re-using the same username/password combination
- In some orgs the departing person provides all access info to their successor
- Storing and sending credentials insecurely (e.g. cleartext)
- Incident Response issues
  - Registrants can discard the emails that notify them of the breach as a suspected phish.

Credentials used in DNS

Credentials used in DNS

- User ID
- Password/Passphrase
- Public/Private Keys
- Symmetric Keys
- Digital Certificates
- Domain AuthInfo Codes
- Multi-Factor Authentications
- One Time Passwords (OTP)

Credentials used in DNS

- Once authenticated, registrants can
  - Register new domains
  - Transfer ownership
  - Remove existing domains
  - Modify DNS records etc.

Credential Management Lifecycle and BCPs

Credential Management Lifecycle

- Phases
  - Designing
  - Creating
  - Distributing
  - Storing
  - Changing
  - Renewing
  - Transferring
  - Revoking
  - Recovering
  - Destroying
- Credentials must be protected at all stages of this lifecycle

Credential Management Lifecycle Phases - Designing

- Decision about how the registrar or registry will validate an identity
- Most registrants are identified by e-mail addresses or account IDs and are validated through the use of passwords/passphrases
- Stronger validation measures
  - Two-factor/Multi-factor authentication
  - Source-IP- address validation
  - Key based authentications

Credential Management Lifecycle Phases - Designing

- Automated password generation and management
  - Password length, strength, expiration, recovery etc.
- Decide how much access the user has once authenticated, and how long until the credential needs to be validated again
- Design should include risk assessment, abuse and incident response plans

Credential Management Lifecycle Phases - Creating

- Creation steps can include:
  - Validating the authenticity of the creation request
  - Assigning the credential to the appropriate user
  - Integrity checks, distribution and storage procedures
- Registries and registrars can enforce policies at creation time
  - Registrant to pass a CAPTCHA as evidence of human creation
  - Provide certain government-issued identification
- 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 Lifecycle Phases - Distributing

- Getting the credential to every person or process that needs to use it
- Credentials must be protected while they are distributed
- 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
- Verification of message integrity

Credential Management Lifecycle Phases - Storing

- Credentials need to be stored in a way that minimizes the risk of revealing them
- Any storage of a credential should be as a protected version so that the credential is not revealed if the file is read (e.g. encryption, use of proper authentication protocols etc.)
- Passwords/passphrases, private keys etc. should never be documented in places where this information may be compromised (e.g. in debug logs, wikis or trouble tickets etc.)
- 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

Credential Management Lifecycle Phases - Storing

- 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 Lifecycle Phases - Changing

- Changes to credentials are important
  - Send change notifications to the users
- Changes can be done via
  - a web session
  - encrypted email
  - helpdesk
- Registries and Registrars can implement controls such as,
  - Processes that monitor change logs for suspicious patterns
  - Credential reuse policies
  - Protection of information that can be used to change a credential at the same level of protection given to the credential itself.

Credential Management Lifecycle Phases - Changing

- Important Steps
  - Validate
    - Change request must be a validated (Names, phone numbers, IP addresses, email addresses, security questions etc.)
  - Apply
    - Good practices applied during the credential creation phase
  - Acknowledge
    - Message to the user in a medium different from that used to change the credential
  - Log
    - Change should be logged but not the value of the new credential.
- Credential change phase can also contain opportunities for attacks

Credential Management Lifecycle Phases - Changing

- A registrar or registry should notify its customers of a breach once detected
- If credentials or the credential management system may have been compromised, customers should be contacted 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 Lifecycle Phases - Renewing

- Credential renewal is a change required by the service provider after a certain amount of time
- The frequency of change that is advisable varies with the credential type selected during the design phase
- Stronger credentials, such as hardware tokens and cryptographic certificates, need to be changed less frequently

Credential Management Lifecycle Phases – Transferring

- Registrars and registries need to have policies to transfer sponsorship of a domain at the request of the registrant
- EPP protocol offers the facility where one party can pass identity validation information to another
  - As per ICANN's Inter-Registrar Transfer Policy all gTLD registries use EPP
  - A valid EPP AuthInfo code is required to initiate a registrar-to-registrar transfer
  - Registrars must protect the AuthInfo codes they assign and receive
  - Registrars can change a domain’s AuthInfo code after the domain has been transferred

Credential Management Lifecycle Phases – Revoking

- Revocation commonly occurs when credentials have been,
  - Compromised
  - Changed (the old credential may be revoked after the new one is installed)
  - Personnel leave the organization
- A revoked credential is actively removed from credential caches, active sessions terminated, and the use of the credential blocked as quickly as possible
- Common structures in use for revoking credentials include revocation lists such as certificate revocation lists (CRL)

Credential Management Lifecycle Phases – Recovering

- Credential recovery occurs when a user has forgotten their user ID, password, or other credential material
- Recovery processes vary among different registrars
  - Usually a link sent to the account's registered e-mail address, a predefined password hint provided by the Registrant, or a series of security questions and answers
  - Recovery via helpdesk may need a PIN number or similar mechanism
- These recovery processes can also be targeted for attacks attempting to gain unauthorized access
  - If attacks are successful, the attacker gains the ability to change nearly anything relating to the domains and the domain management account

Credential Management Lifecycle Phases – Destroying

- Destroying a credential is the end of its lifecycle
  - Anything used in any phase of the credential lifecycle, including information used in recovering, transferring, or renewing, should be destroyed carefully
- The credential file and any information associated with the account or account validation should be deleted
- Can write junk to the credential file on disk, and then delete it to make sure digital forensics could not recover the file from the disk
- Treat hard drives that have stored credential information as sensitive and physically shred or degauss the drives when they are retired

Summary

- Covered the overview of Credential Management
- Introduced the DNS Ecosystem and the key players such as Registries, Registrars and Registrants
- Discussed the compromises in the DNS Ecosystem
- Discussed about the type of credentials used in DNS
- Detailed discussion about the Credential Management Lifecycle and the Best Common Practices in Credential Management

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