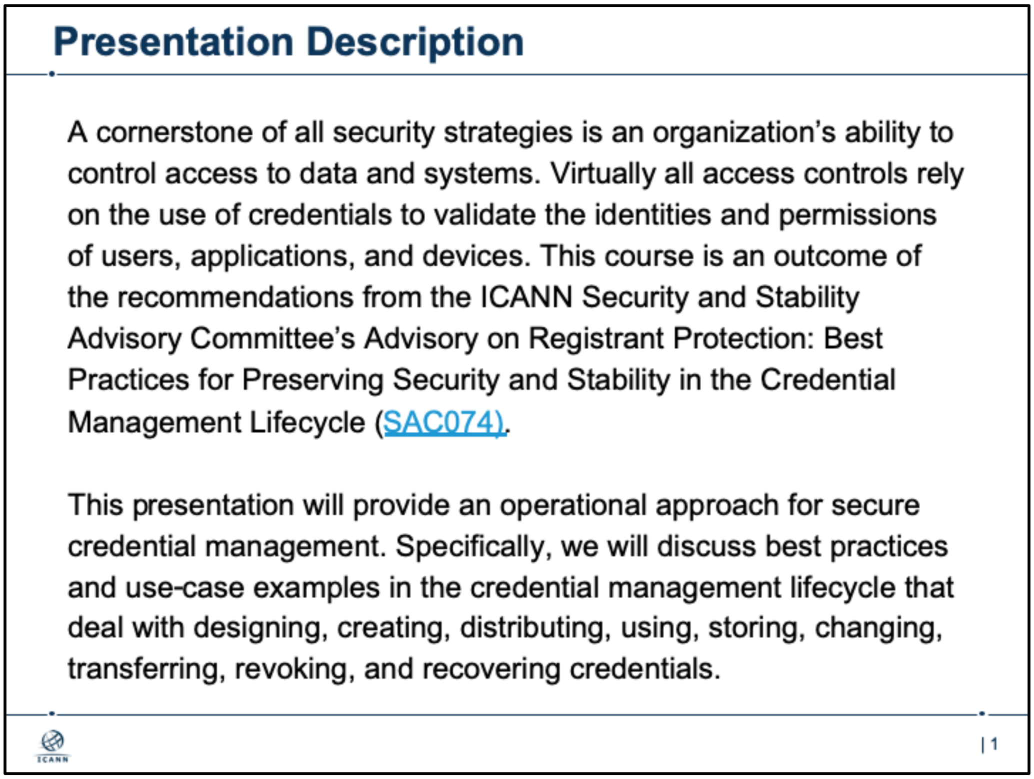
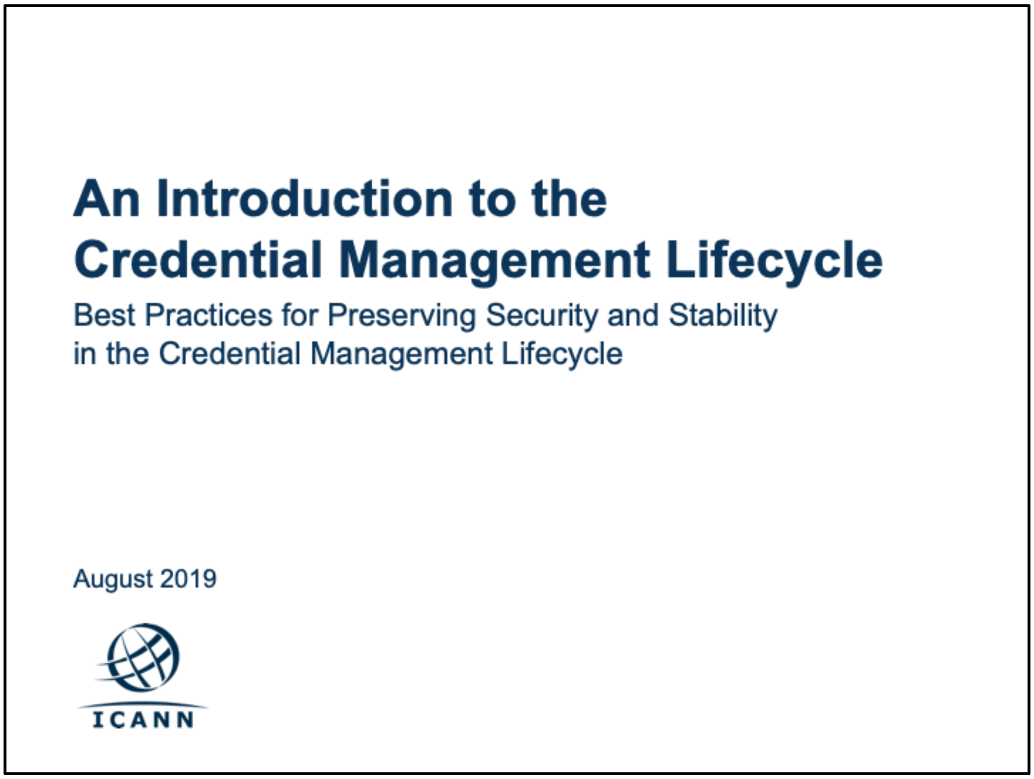


Presentation Description

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. This course is an outcome of the recommendations from the ICANN Security and Stability Advisory Committee's Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle (SAC074).

This presentation will provide an operational approach for secure credential management. Specifically, we will discuss best practices and use-case examples in the credential management lifecycle that deal with designing, creating, distributing, using, storing, changing, transferring, revoking, and recovering credentials.

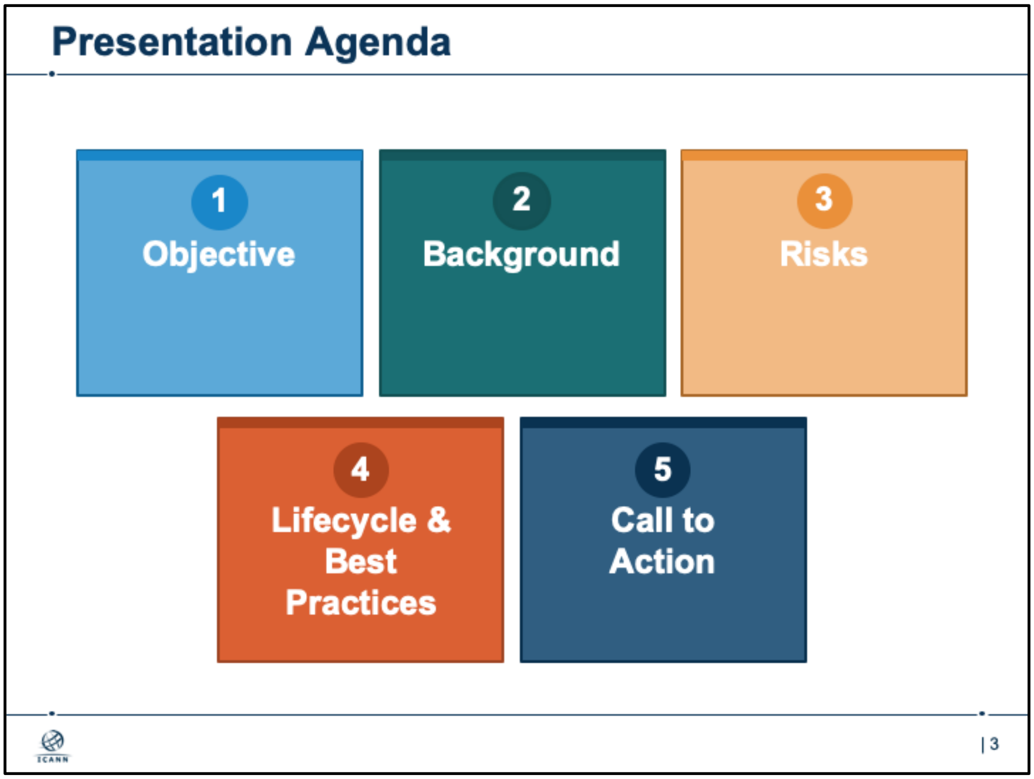


An Introduction to the Credential Management Lifecycle

Best Practices for Preserving Security and Stability
in the Credential Management Lifecycle

August 2019

ICANN



Presentation Agenda

1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action

| 3

The following are the five specific items we will be going through during this presentation:

We begin with a brief run-through of the presentation objectives, provide a background of credential management and why you should be paying attention to the topic in light of very real risks. We consider the credential management lifecycle and various good practices that registrars and registries might employ in consideration. And finally, we will provide a call to action, what you should be doing to ensure you're taking the right steps to protect your own and your registrants' credentials.

Presentation Agenda

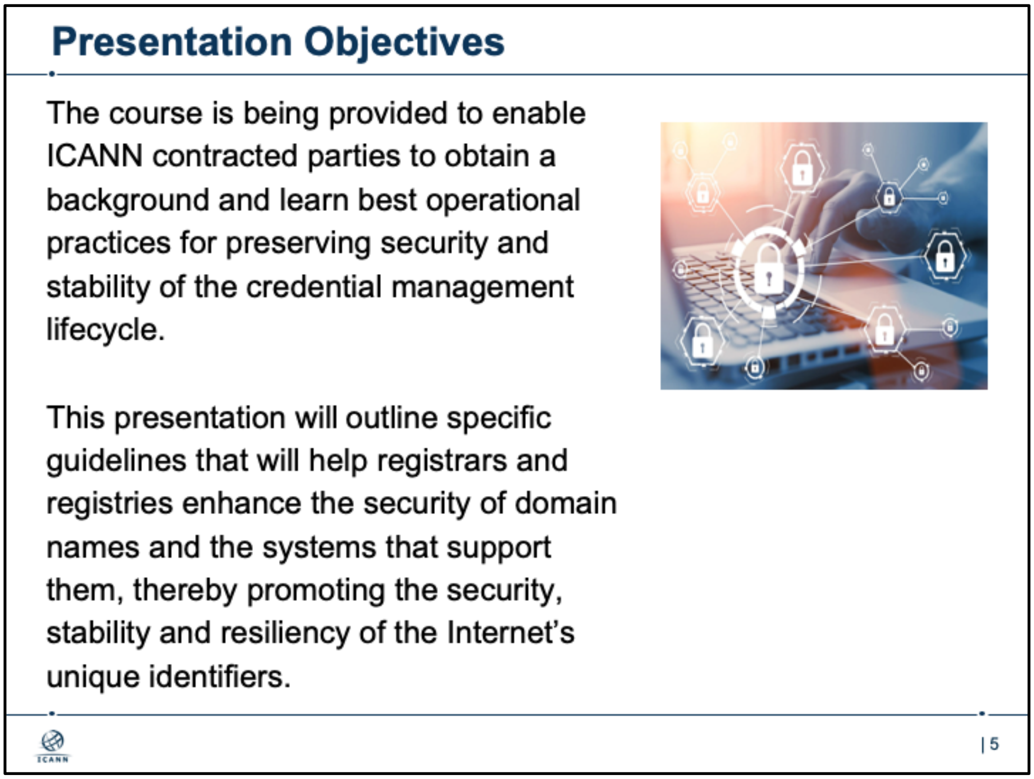
1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action



Presentation Objectives

The course is being provided to enable ICANN contracted parties to obtain a background and learn best operational practices for preserving security and stability of the credential management lifecycle.

This presentation will outline specific guidelines that will help registrars and registries enhance the security of domain names and the systems that support them, thereby promoting the security, stability and resiliency of the Internet's unique identifiers.

The presentation is being provided to enable ICANN contracted parties to obtain a background and learn practical operational practices for preserving security and stability of the credential management lifecycle.

This course will outline specific guidelines that will help registrars and registries enhance the security of domain names and the systems that support them, thereby promoting the security, stability and resiliency of the Internet's unique identifiers.

Presentation Agenda

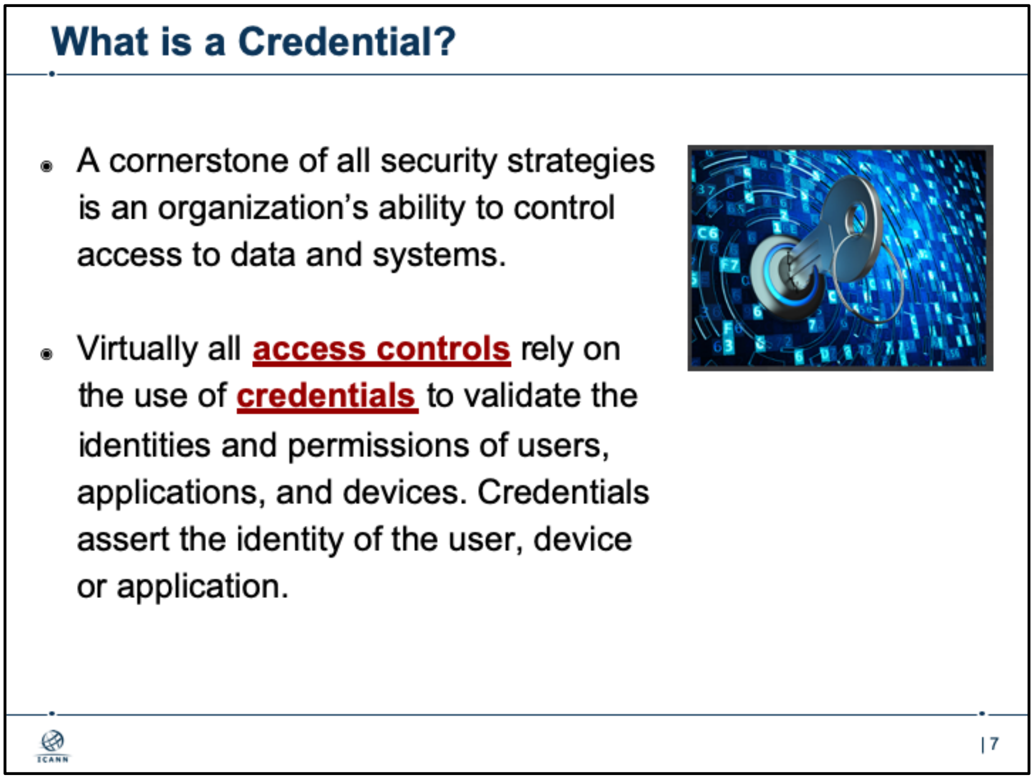
1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action



What is a Credential?

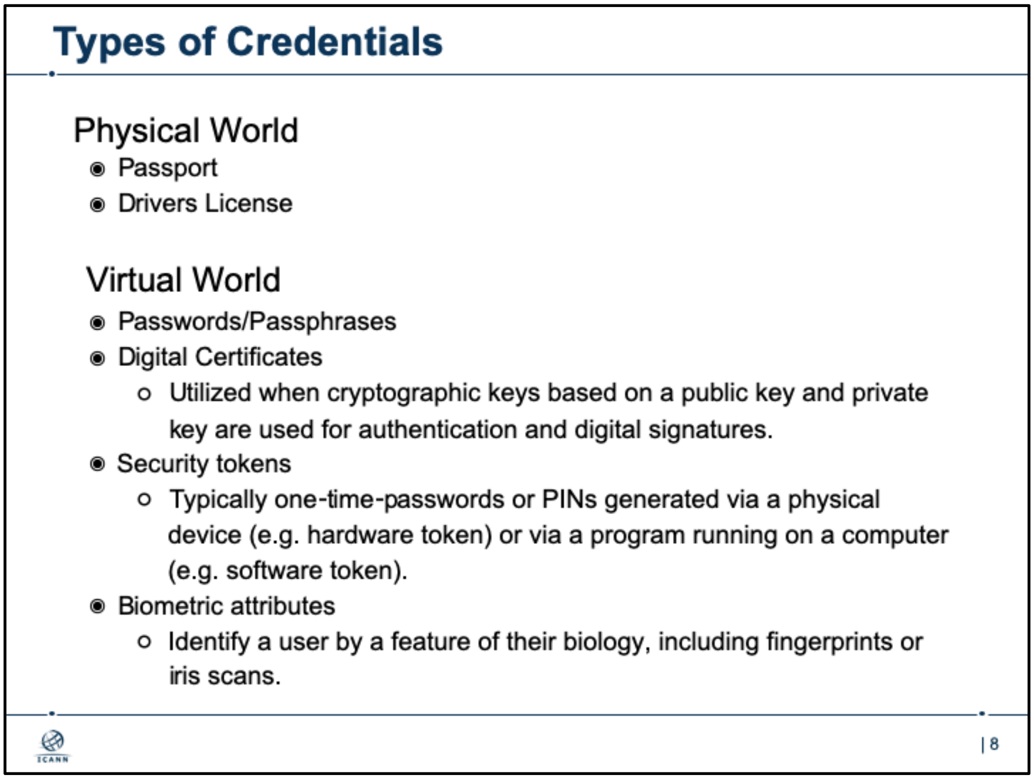
- A cornerstone of all security strategies is an organization's ability to control access to data and systems.
- Virtually all **access controls** rely on the use of **credentials** to validate the identities and permissions of users, applications, and devices. Credentials assert the identity of the user, device or application.

Attacks that compromise registrant data and/or the DNS settings of domain names continue to be a significant problem for registrars and registries, as well as for the registrants themselves and the users of their sites. The issue of credential management has emerged as a serious business challenge that goes far beyond traditional password management. Many compromises have been tied directly with issues relating to credential management.

So what is a credential?

Credentials serve as the cornerstone of all security strategies for an organization to be able to control access to its data and systems. Virtually all access controls rely on the use of credentials. Credentials are based on a user, a device, or an application.

Credentials are required for individual users, devices, and applications and are often used for authentication purposes, access control, integrity checking, and/or providing confidentiality. These credentials typically consist of a public/private key pair, a shared secret, some kind of hardware or software token, an individual password/passphrase, or a digital certificate. These credentials are used to assert the identity of an entity wishing to get authenticated to perform certain functions.



Types of Credentials

Physical World

- Passport
- Drivers License

Virtual World

- Passwords/Passphrases
- Digital Certificates
  - Utilized when cryptographic keys based on a public key and private key 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.

| 8

Pretty much all of us carry credentials in the physical world. We can think about driver's licenses, passports, and other forms of identification we may have on our personal selves. The strength of the these physical credentials depend on how easy is it to forge or impersonate someone’s identity using them. And so when we're looking at the virtual world what's really important to understand what is the strength of a credential that we're using.

Types of security credentials include:

• User Names or IDs, and passwords or passphrases.

• Asymmetric Key Pairs. A public key and private key that enable encryption, authentication and digital signatures.

• Security tokens, which are typically one-time-passwords or PINs generated via a physical device (i.e. hardware token) or via a program running on a computer (i.e. software token).

• Biometric attributes, which identify a user by a feature of their biology, including fingerprints or iris scans. These are not commonly used in domain name registration processes, and are mentioned for completeness.

Multi-factor authentication schemes employ two or more such types of

credentials. Typically they will mix credentials from the categories "something one has" (e.g. a hardware token), "something one knows" (e.g. a password)
and "something one is" (e.g. biometrics).

Presentation Agenda

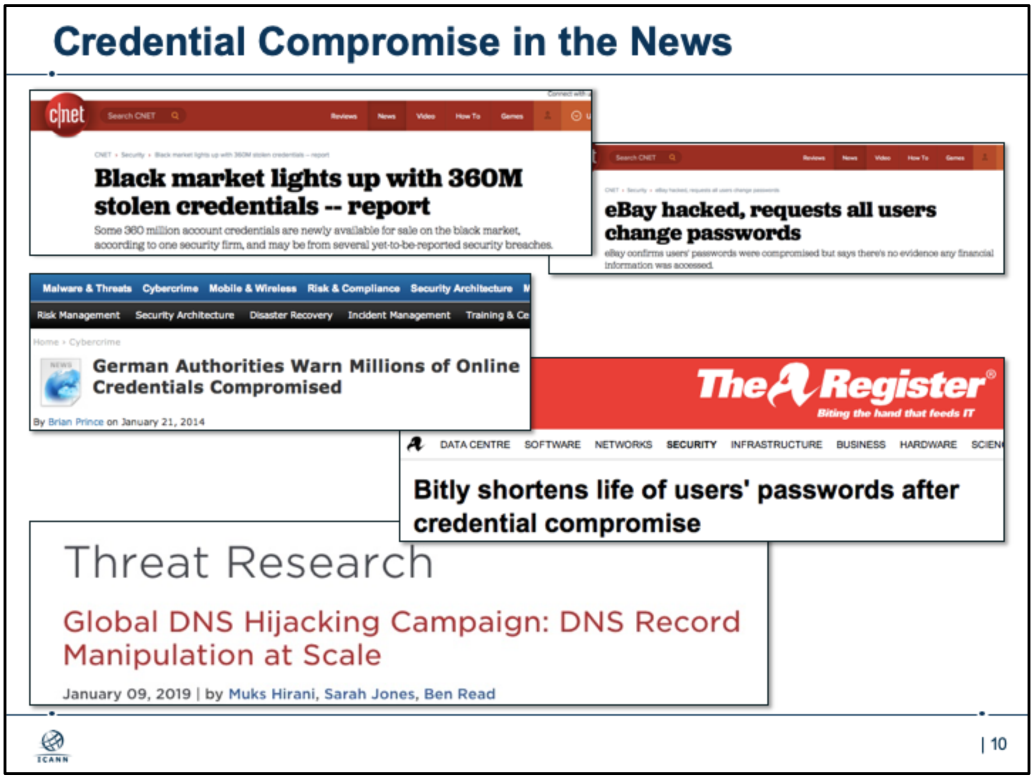
1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action



Credential Compromise in the News

c|net
Search CNET
Reviews
News
Video
How To
Games
CNET › Security › Black market lights up with 360M stolen credentials -- report

Black market lights up with 360M stolen credentials -- report

Some 360 million account credentials are newly available for sale on the black market, according to one security firm, and may be from several yet-to-be-reported security breaches.

Search CNET
Reviews
News
Video
How To
Games
CNET › Security › eBay hacked, requests all users change passwords

eBay hacked, requests all users change passwords

eBay confirms users' passwords were compromised but says there's no evidence any financial information was accessed.

German Authorities Warn Millions of Online Credentials Compromised

By Brian Prince on January 21, 2014

Bitly shortens life of users' passwords after credential compromise

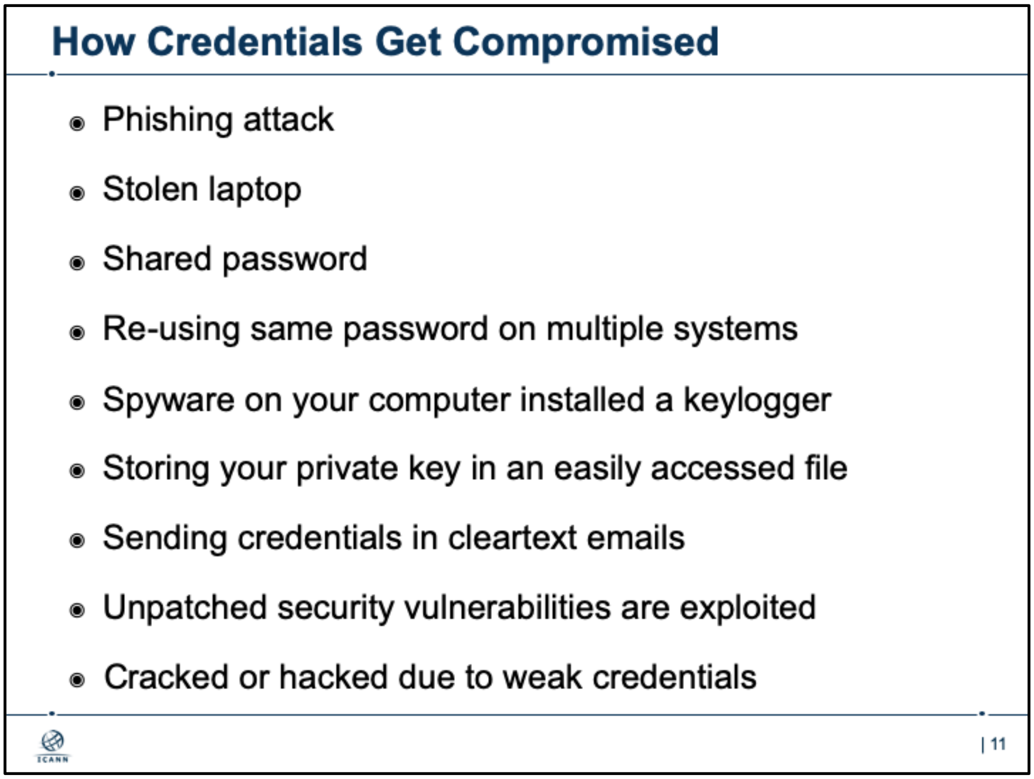
Threat Research

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

January 09, 2019 | by Muks Hirani, Sarah Jones, Ben Read

Malicious access to and potential reconfiguration of registrant data can severely disrupt business operations and can cause significant financial and reputational harm. Damage from changes to registrant data is not limited to the registrant alone, but can also affect registrars, registries, users of the registrant’s domain(s), and other DNS service providers.

In the last few years, there have been numerous publicized events where the compromises were attributable to deficiencies in credential management. These examples illustrate the importance and immediacy of the problem.



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

| 11

How do credentials get compromised? A wide number of possible ways…

Here are some common scenarios. In many instances, users employ the same username/password combination across different accounts or on different websites. Password reuse stems from a user’s need for convenience and the limited human capacity to remember random strings of characters. Either registrants or authorized personnel for a registrar or registry may make this mistake. Such reuse is poor practice because it makes the authentication system brittle.

Credential data is sensitive and needs protection both in transit and at rest to minimize the chance of disclosure. Even if the information is encoded in a way that is not human readable, techniques exist to determine which encoding is being used, and then to decode the information. Insecure transmission of credentials includes unencrypted email or browser sessions (cleartext) and phone conversations.

Successful attacks on registrars and registries have allowed hackers to obtain credentials directly from these authoritative systems. The true mechanism used for an attack or compromise is often indeterminable. However, sometimes analysts can reasonably conclude that weak or stolen credentials were involved.

Phishing is an illicit attempt to compromise credentials by luring Internet users to a page that imitates a trusted site such as a bank or e-commerce site. A spear phishing attack uses phishing techniques to target high-value credentials that allow access to critical systems or data such as those held by the staff members of a registrar or registry. The compromise of an entire registrar is highly critical as all customer data and systems can be exposed. Attackers therefore spend time specifically crafting a targeted approach and a resultant spear phish email.

Domain Shadowing, in which, by using stolen or phished credentials, the malicious actors create numerous subdomains associated with existing, reputable domains in the registrant's portfolio. With credentials, the attackers gain full access to DNS and domain resources. The new subdomains are pointed to Internet Protocol (IP) addresses that further serve up malicious content such as malware and ransomware. Because registrants often do 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. Improved monitoring and notifications by registrars confirming DNS changes to zones they are hosting for registrants, and an increased awareness of DNS activity by registrants would go a long way towards reducing or eliminating domain shadowing

It is important to note that the 2013 Registrar Accreditation Agreement requires registrars to notify ICANN should there be a security breach

- Do you have the capability to detect a breach?
- Do you have a process for incident response?
- Do you test it periodically?

Presentation Agenda

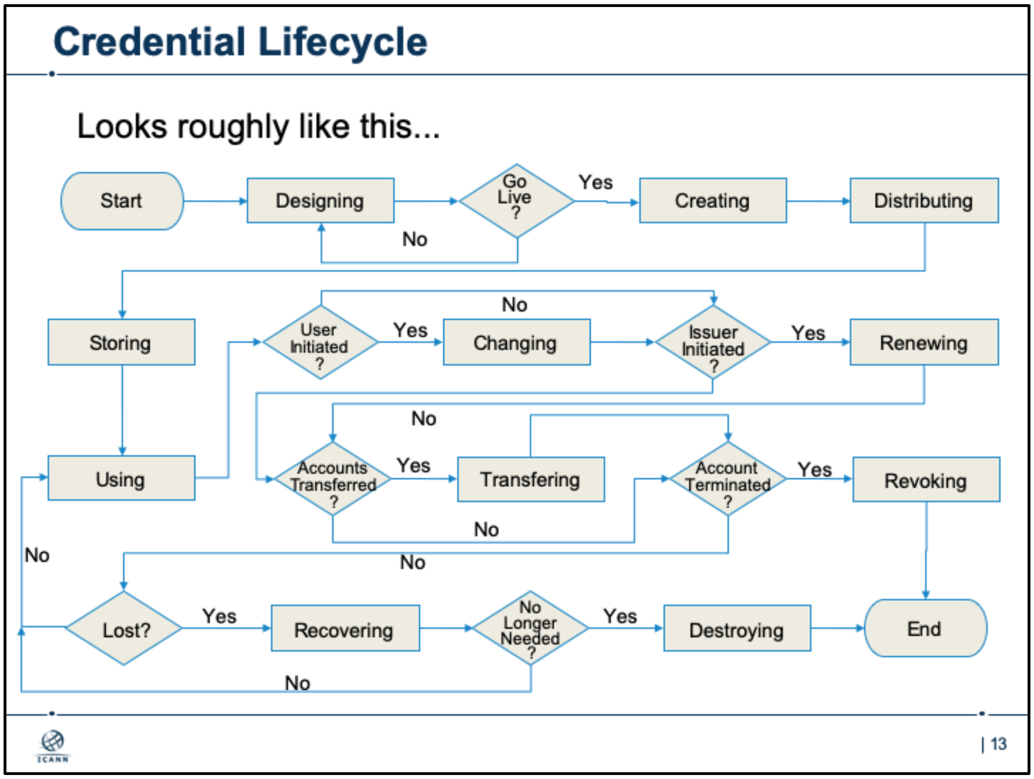
1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action



Credential Lifecycle

Looks roughly like this…

Credentials have a lifecycle 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. We discuss each phase as it is practiced by registrars and registries today: designing, creating, distributing, storing, changing, renewing, transferring, revoking, recovering, and destroying.

Designing Credential design is the decision about how the registrar or registry will validate an identity including requirements and constraints on the validation mechanism. The design choices embody policy and risk decisions, sometimes based on assumptions rather than carefully considered choices. Choices made at the design stage directly impact possibilities at all other stages of the credential management cycle, so it is important to choose wisely. A wide variety of credential design practices are in use today. Important factors in credential design decisions include the expertise of the staff, the operational budget, usability requirements, threats to the credential confidentiality, and costs incurred if threat actors succeed. However, no standard exists for password management. While most registries have basic security implemented, there are not regular audits of password management practices to update the practices as threats evolve.

Creating Creating credentials is a complex process that involves more than just generating a shared secret. Other steps currently in use by some organizations include validating the authenticity of the creation request, assigning the credential to the appropriate user, and initiating the distribution and storage procedures that take integrity and confidentiality mechanisms into account. Registries and registrars enforce several policies at creation time. Creation time is when requirements on the shared secret are enforced. Policies for who or what may request a credential are also enforced, though the policies vary widely.

Distributing Credential distribution means getting the credential to every person or process that needs to use it and protections are in place ensuring confidentiality and integrity (encryption in place) of the credential. The owner of the credential often is its creator, such as when a user selects a password or generates a public key certificate. Sometimes (part of) the credential is something about the user, such as their personal or organizational name, phone number or IP address.

Storing Users expect registrars and registries to store a protected version of the credential that does not reveal the credential if the file is read. For passwords, this means a one-way function that is unique to each user (formally, a salted hash function). There are no confirmed public cases of registries or registrars storing passwords incorrectly, although there are several confirmed instances of web content companies doing so. Computer generated private keys can be stored by encrypting them with a key derived from a password/passphrase for extra protection, as in Pretty Good Privacy (PGP).

Changing Changes to credentials are important events. Many registrars and registries have advised that they log when the user changes their password, and many send change notification messages. However, the credential change phase contains many opportunities for attack. Some controls implemented by some registrars and registries include: automated and manual processes that monitor change logs for suspicious patterns as indicators of problems, credential reuse policies, multiple credential change mechanisms, and the protection of information that can be used to change a credential at the same level of protection given to the credential itself.

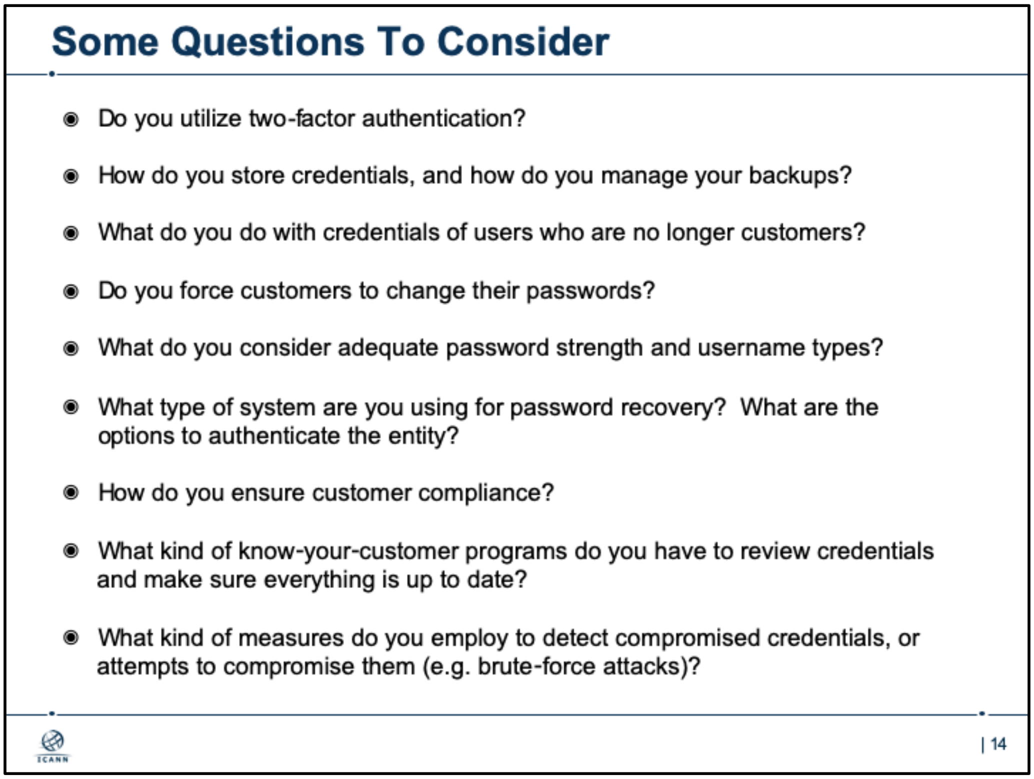
Renewing Renewing credentials is similar to the changing phase, except that a credential renewal is a change required by the service provider after a certain amount of time. The amount of time specified by the service provider policy varies widely. Some registrars never require a credential renewal. Some registrars and registries require credentials to change as often as every 90 days. 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.

Transferring Registrars and registries in gTLDs and many ccTLDs have policies that registrars must transfer sponsorship of a domain at the request of the registrant. This requirement presents credential management challenges. Therefore the Extensible]Provisioning Protocol (EPP) registry-registrar protocol offers a means by which one party can pass identity validation information to another. As prescribed by 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. Many registrars change a domain's AuthInfo code after the domain has been transferred.

Revoking There are multiple scenarios in which a registry or registrar revokes a credential. Revoking is not the same as destroying – a revoked credential is actively removed from credential caches, active sessions terminated, and the use of the credential blocked as quickly as possible. Revocation commonly occurs when credentials are determined to have been compromised, are changed (the old credential may be revoked after the new one is installed), or personnel leave the organization.

Recovering Credential recovery occurs when a user has forgotten their user ID, password, or other credential material. These recovery processes vary among different registrars, but often they are simply 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. Additionally, registrars who provide telephone support may also have a mechanism that allows someone to access the account with a combination of passwords, call-in personal identification numbers (PIN), or by providing the last few digits of the credit card or payment method on file for the account.

Destroying Destroying a credential is the end of its lifecycle. Registrars and registries have different processes for credential destruction that approximately follow these steps. The credential file and any information associated with the account or account validation is delinked, i.e. deleted. Many registrars 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. Some organizations treat hard drives that have stored credential information as sensitive and physically shred or degauss the drives when they are retired. Registrars and registries try to be careful to remove all copies of credential information from their systems during destruction. Not all registrars and registries agree as to which information is sensitive enough to warrant destruction, but some agree that anything used in any phase of the credential lifecycle, including information used in recovering, transferring, or renewing, should be destroyed carefully.



Some Questions To Consider

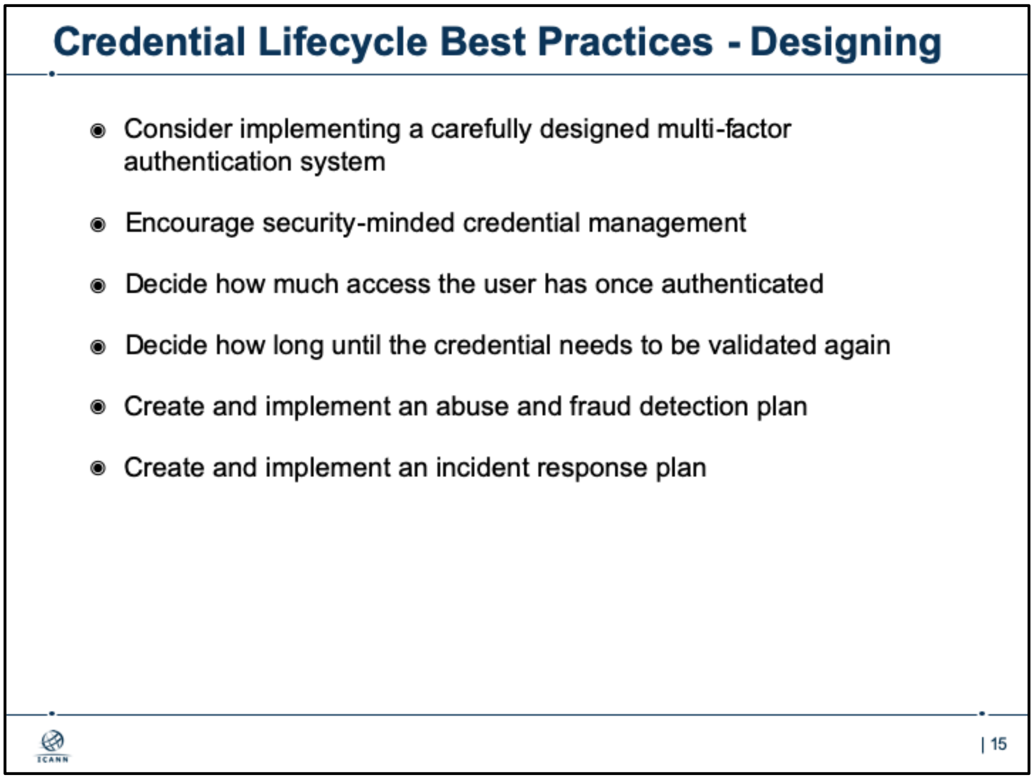
- Do you utilize two-factor authentication?
- How do you store credentials, and how do you manage your backups?
- What do you do with credentials of users who are no longer customers?
- Do you force customers to change their passwords?
- What do you consider adequate password strength and username types?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

Here are some key questions to try to answer as you consider the entire Credential Management lifecycle.

- Do you utilize two-factor authentication?
- How do you store credentials, and how do you manage your backups?
- What do you do with credential 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?
- 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)?

There are practical improvements that can be made to all stages of the credential management lifecycle. We present these overall considerations for implementing good best current practices for each stage in the lifecycle in the same order the stages were presented in the prior slide.



Credential Lifecycle Best Practices - Designing

- Consider implementing a carefully designed multi-factor authentication system
- Encourage security-minded credential management
- Decide how much access the user has once authenticated
- Decide how long until the credential needs to be validated again
- Create and implement an abuse and fraud detection plan
- Create and implement an incident response plan

Attacks cannot be completely prevented, so design should include risk assessment and incident response plans

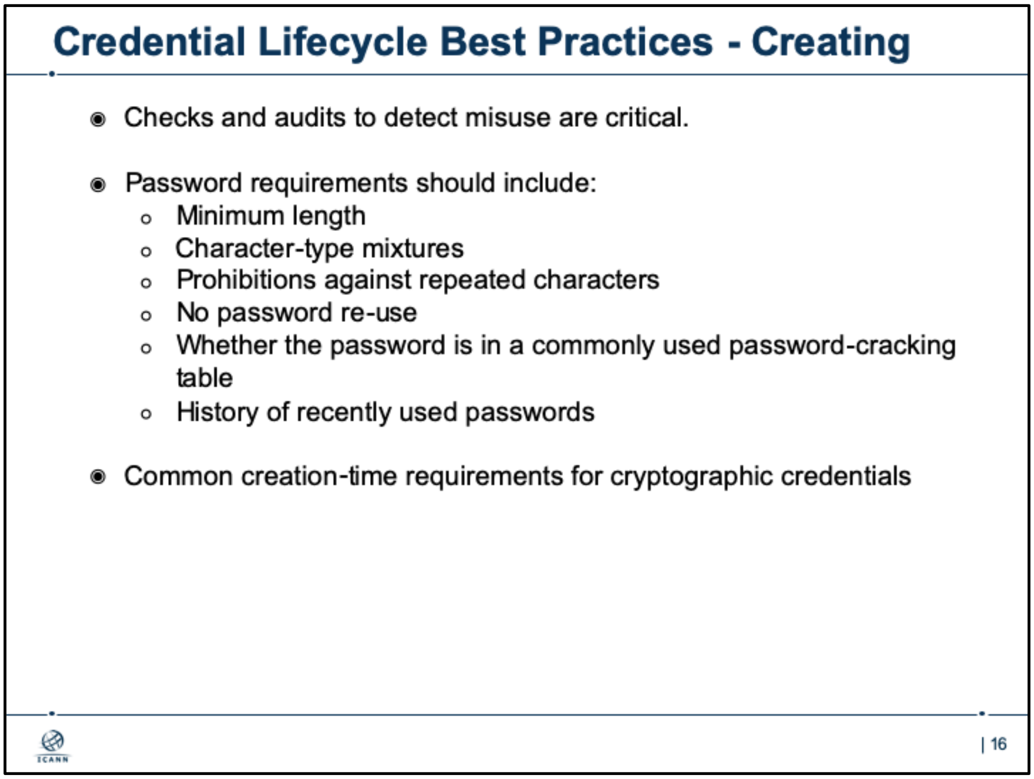
• Consider implementing a carefully designed multi-factor authentication system. One option is to send text messages containing a PIN to a customer-authorized mobile phone number.

• Encourage security-minded credential management, including adequate requirements for: password length and strength, password expiration, and password recovery.

• Decide how much access the user has once authenticated, and how long until the credential needs to be validated again. These design decisions should follow basic security principles of providing the least access and least privilege while still permitting the user to perform the task. This includes requiring a user to re-authenticate to do important tasks and having a relatively short inactivity timeout once logged in (15 to 120 minutes). Such a design makes abuse and compromise harder for an adversary and easier for the registrar or registry to detect.

• Create and implement an abuse and fraud detection plan. For example, registrars can monitor DNS activity in order to reduce current attacks such as domain shadowing. Monitor for unauthenticated access attempts and monitor DNS changes to help determine potential compromise

- Create and implement an incident response plan.
    - Maintain current and accurate contact details
    - Determine who needs to be notified and under which criteria
    - Determine chain of authority for decisions
    - Determine who is responsible for internal and/or external communications.



Credential Lifecycle Best Practices - Creating

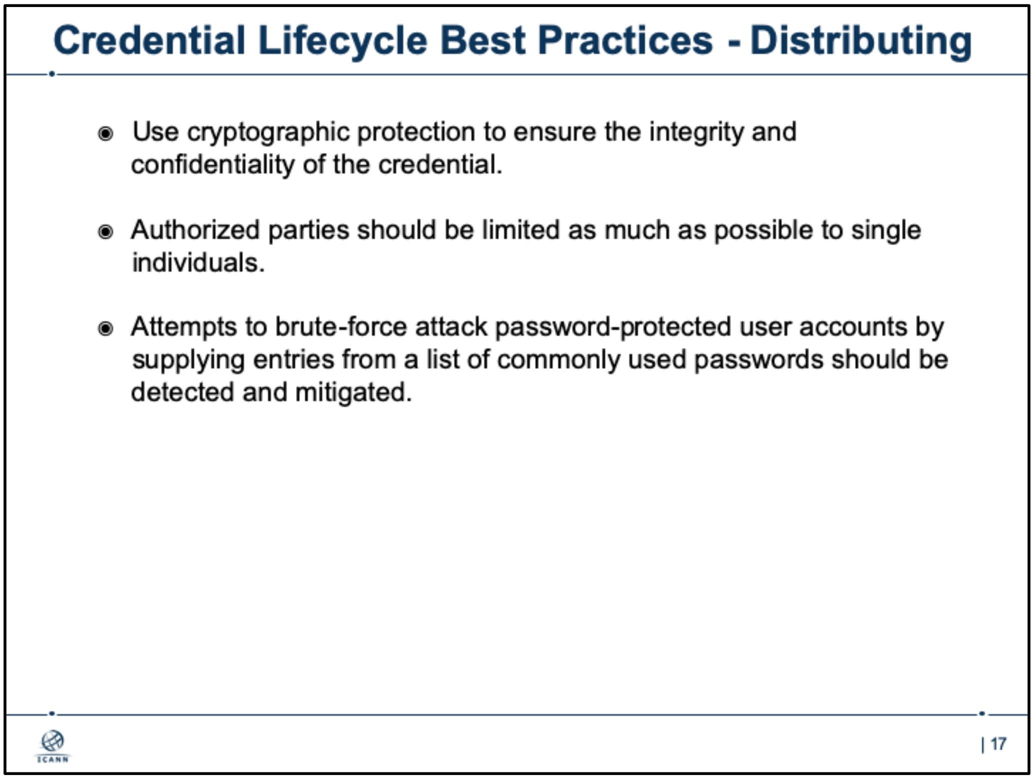
- Checks and audits to detect misuse are critical.
- Password requirements should include:
  - Minimum length
  - Character-type mixtures
  - Prohibitions against repeated characters
  - No password re-use
  - Whether the password is in a commonly used password-cracking table
  - History of recently used passwords
- Common creation-time requirements for cryptographic credentials

| 16

Credential creation involves trust in policies and procedures that cannot be completely tamper-proof. The risk must be managed, as it cannot be eliminated. Checks and audits to detect misuse are critical. Creation time is when requirements on the shared secret are enforced.

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), and • history of recently used passwords.

There are common creation-time requirements for cryptographic credentials as well, such as their intended lifetime, how large (in bits), and key protocol.



Credential Lifecycle Best Practices - Distributing

- Use cryptographic protection to ensure the integrity and confidentiality of the credential.
- Authorized parties should be limited as much as possible to single individuals.
- Attempts to brute-force attack password-protected user accounts by supplying entries from a list of commonly used passwords should be detected and mitigated.

ICANN

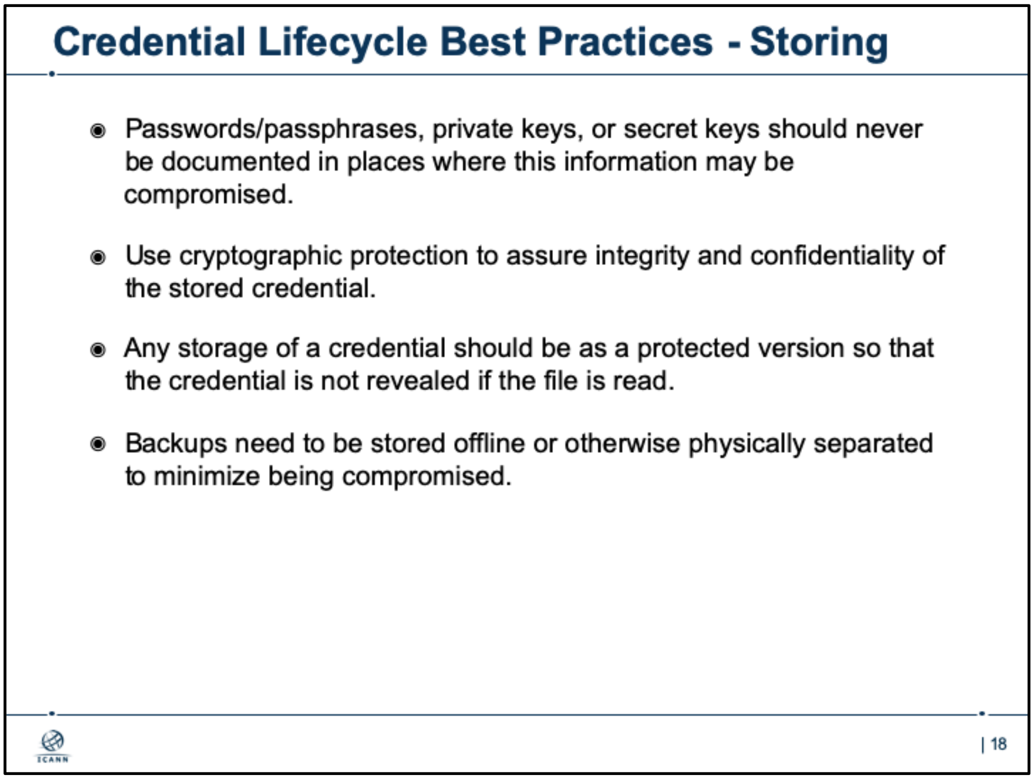
| 17

Credentials must be protected while they are distributed to or used by the authorized parties. Protections include:

• Transmitting only over an encrypted channel such as Hypertext Transfer Protocol Secure (HTTPS) or Secure Shell (SSH) between any pair of machines that handle the credentials.

• Authorized parties should be limited as much as possible to single individuals. Where multiple individuals share a role, they should still obtain unique credentials in order to better track abuse or misuse, and to 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 Lifecycle Best Practices - Storing

- Passwords/passphrases, private keys, or secret keys should never be documented in places where this information may be compromised.
- Use cryptographic protection to assure integrity and confidentiality of the stored credential.
- Any storage of a credential should be as a protected version so that the credential is not revealed if the file is read.
- Backups need to be stored offline or otherwise physically separated to minimize being compromised.

| 18

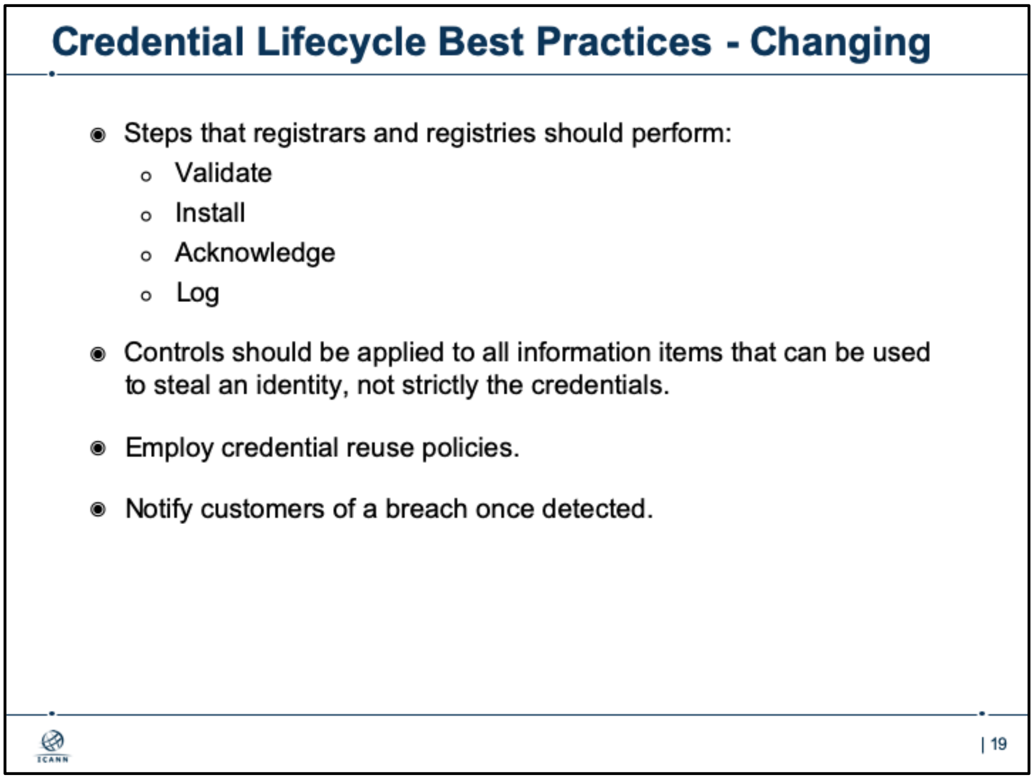
Registrars and registries should have clear policies and procedures for storing or backing up credentials. Credentials need to be stored in a way that minimizes the risk of revealing them to adversaries during the credential’s lifetime.

• Passwords/passphrases, private keys, or secret keys should never be documented in places where this information may be compromised, such as in debug logs, wikis or trouble tickets.

• Any storage of a credential should be as a protected version so that the credential is not revealed if the file is read. Proper protection methods include encrypting the data, employing proper authentication protocols, and using one-way functions (salted hashes or bcrypt) when possible so the cleartext cannot be easily recovered. Storing hashes on disk properly is not enough; the 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 themselves be encrypted with one master backup key. This master key needs to be physically protected and highly guarded when in use.



Credential Lifecycle Best Practices - Changing

- Steps that registrars and registries should perform:
  - Validate
  - Install
  - Acknowledge
  - Log
- Controls should be applied to all information items that can be used to steal an identity, not strictly the credentials.
- Employ credential reuse policies.
- Notify customers of a breach once detected.

| 19

No matter where a credential is changed, there are four steps that registrars and registries should perform: validate, install, acknowledge, log.

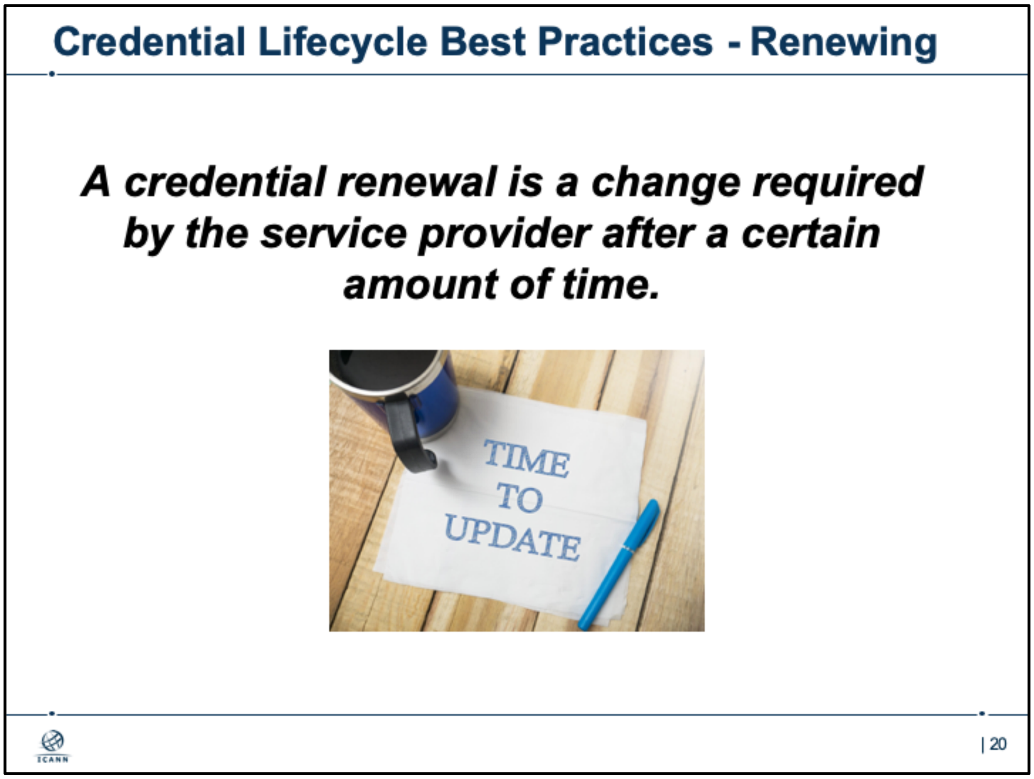
> • Any change request must be validated. The user requesting the change must be a validated, authentic user who is allowed to request the change. The new credential is installed, following all the good practices used during the credential creation phase. The change is acknowledged via a message to the user in a medium different from that used to change the credential and not relying on the credential just changed; this step is important in the case where the genuine user did not in fact make the change request as well as in general customer relations to confirm the change succeeded. Finally the change (but not the value of the new credential) is logged.

• Such controls should be applied to all information items that can be used to steal an identity, not just strictly the credentials. Other important information items include names, phone numbers, IP addresses, physical addresses, email addresses, security questions, and fax numbers.

• Registrars and registries should employ credential reuse restrictions. Reuse restrictions strengthen credentials, especially passwords, because a credential weakens significantly if used in multiple places or over a long time.

- 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 notices should also be placed on the registry's or registrar's web site, and on social media, so that customers can obtain confirmation of the incident in an independently verifiable way.

- Breach notification emails should be sent from a trusted and recognizable domain name, should be PGP-signed, and the password change service should be on a known site.

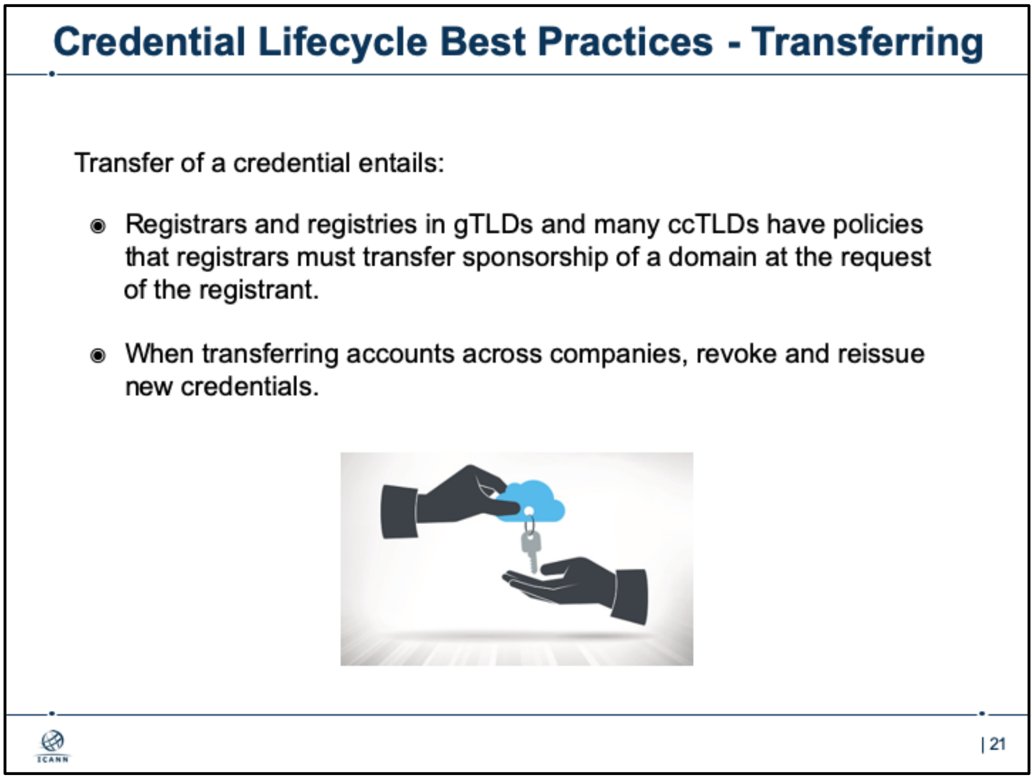


Credential Lifecycle Best Practices - Renewing

A credential renewal is a change required by the service provider after a certain amount of time.

TIME
TO
UPDATE

During the design phase, select 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.



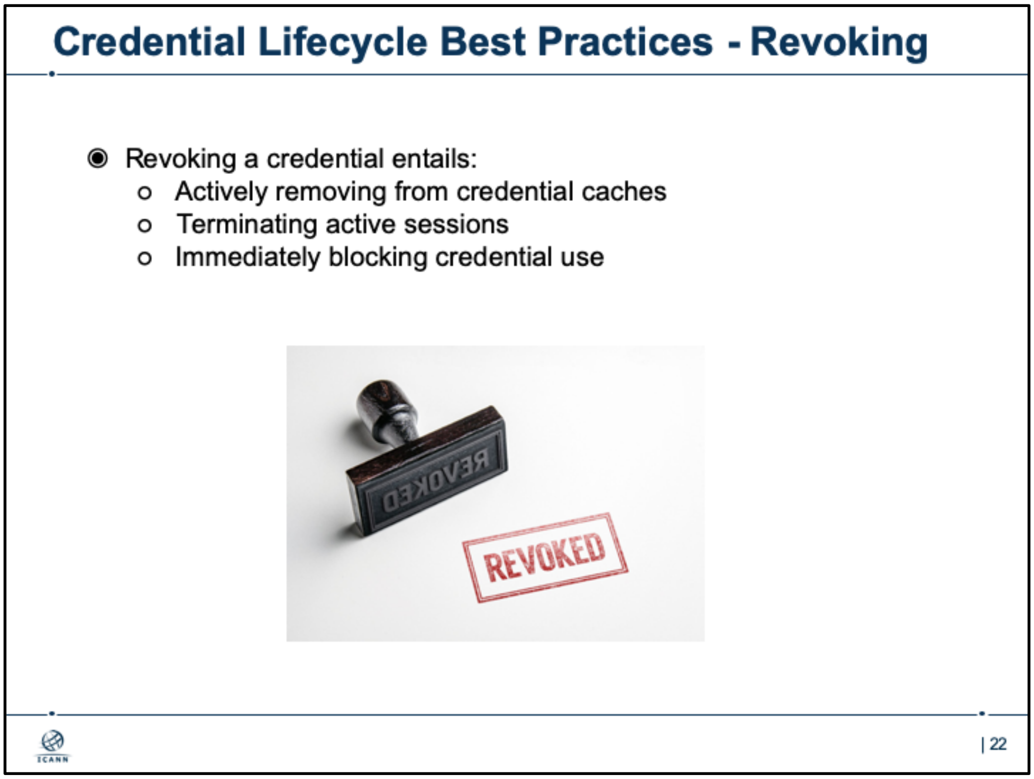
Credential Lifecycle Best Practices - Transferring

Transfer of a credential entails:

- Registrars and registries in gTLDs and many ccTLDs have policies that registrars must transfer sponsorship of a domain at the request of the registrant.
- When transferring accounts across companies, revoke and reissue new credentials.

Registrars and registries are required to follow ICANN's Inter-Registrar Transfer Policy to transfer sponsorship of a domain at the request of the registrant

As it is common to see mergers and acquisitions in the DNS industry, it is sensible to consider how credentials are managed when the transfer of service happens. When transferring accounts across companies, revoke and reissue new credentials.



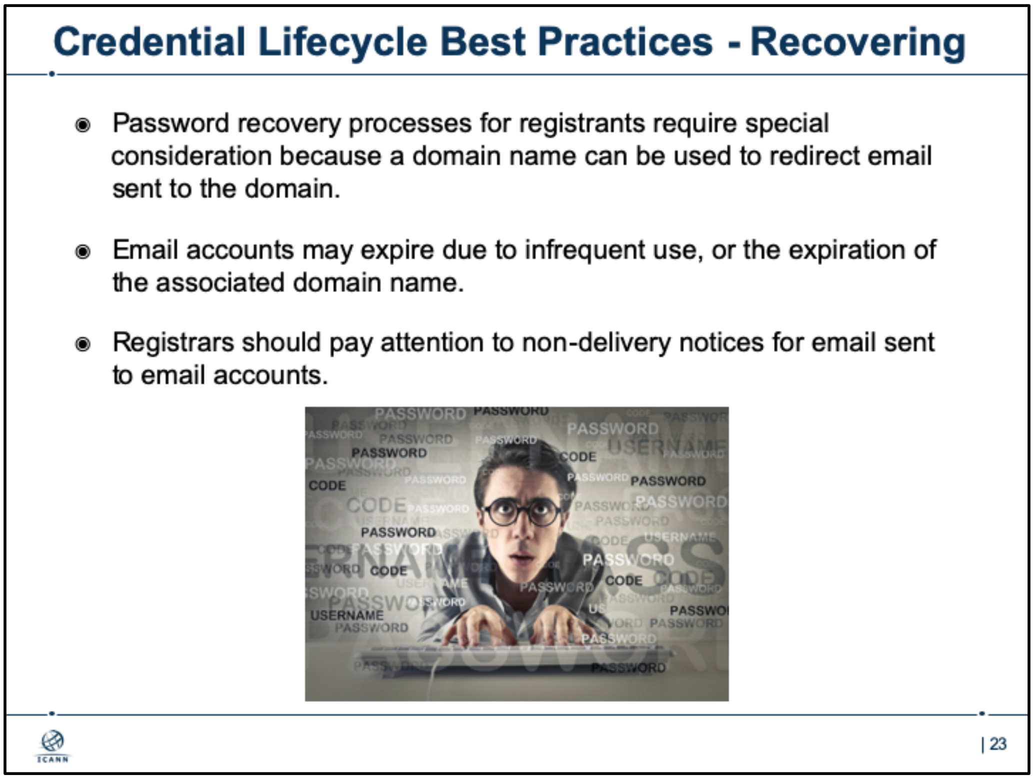
Credential Lifecycle Best Practices - Revoking

- Revoking a credential entails:
  - Actively removing from credential caches
  - Terminating active sessions
  - Immediately blocking credential use

REVOKED
REVOKED
ICANN

- Registrars or registries should revoke credentials under three circumstances:
  - when credentials are compromised;
  - when credentials must be renewed (old credential is revoked); and
  - when personnel change roles or depart the organization.

- Since cached credentials cannot be revoked, registrars and registries should set short cache times. Web sessions or other interactive log-ins should be actively terminated, and credential revocation should propagate quickly through any distributed authentication system.

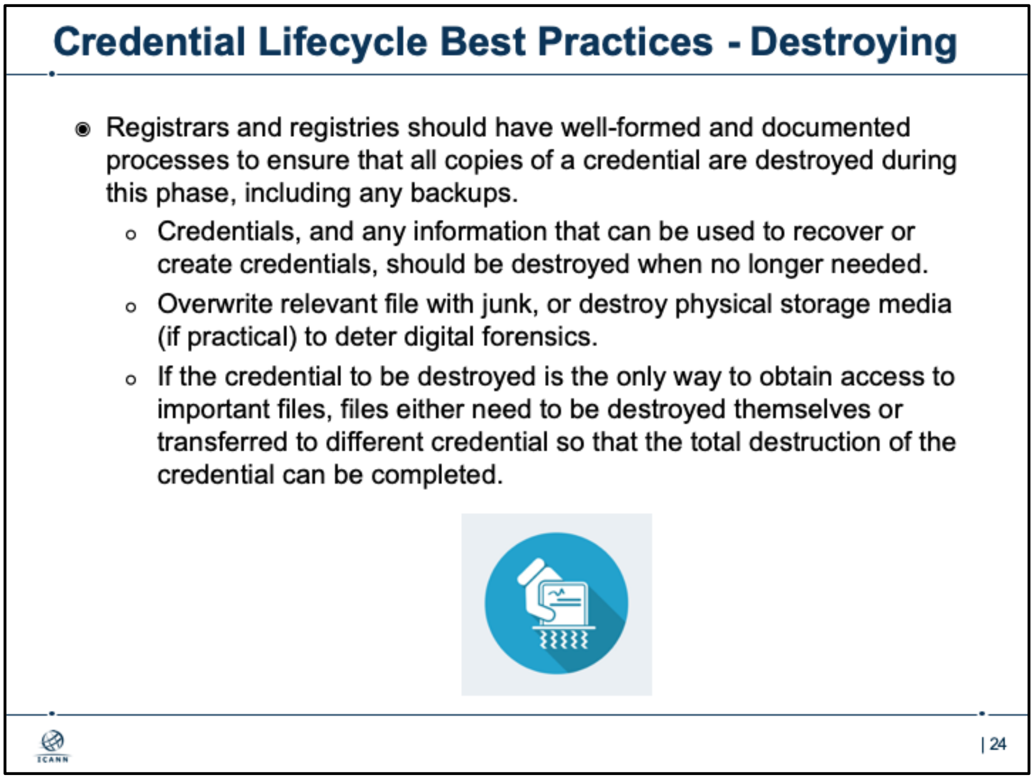


Credential Lifecycle Best Practices - Recovering

- Password recovery processes for registrants require special consideration because a domain name can be used to redirect email sent to the domain.
- Email accounts may expire due to infrequent use, or the expiration of the associated domain name.
- Registrars should pay attention to non-delivery notices for email sent to email accounts.

| 23

- Registrars and registries should increase internal awareness that credential recovery processes are common targets for adversaries.
  - Password recovery processes for registrants require special consideration because a domain name can be used to redirect email sent to the domain. It is not safe to send credential recovery instructions for a domain to an email address within that domain. This special problem requires extra attention to the credential recovery process at registrars and registries.
  - 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 Lifecycle Best Practices - Destroying

- Registrars and registries should have well-formed and documented processes to ensure that all copies of a credential are destroyed during this phase, including any backups.
  - Credentials, and any information that can be used to recover or create credentials, should be destroyed when no longer needed.
  - Overwrite relevant file with junk, or destroy physical storage media (if practical) to deter digital forensics.
  - If the credential to be destroyed is the only way to obtain access to important files, files either need to be destroyed themselves or transferred to different credential so that the total destruction of the credential can be completed.

- Destroying credentials is the last stage in the credential management lifecycle. Registrars and registries should have well-formed and documented processes to ensure that all copies of a credential are destroyed during this phase, including any backups.

- 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, or destroying the physical storage media (if practical) to deter digital forensics. Hardware used to store and process credentials should also be shredded or degaussed when it is time for disposal.

- If the credential to be destroyed is the only way to obtain access to important files, either live or backed-up, those files either need to be destroyed themselves or transferred to a different credential so that the total destruction of the credential can be completed.

Presentation Agenda

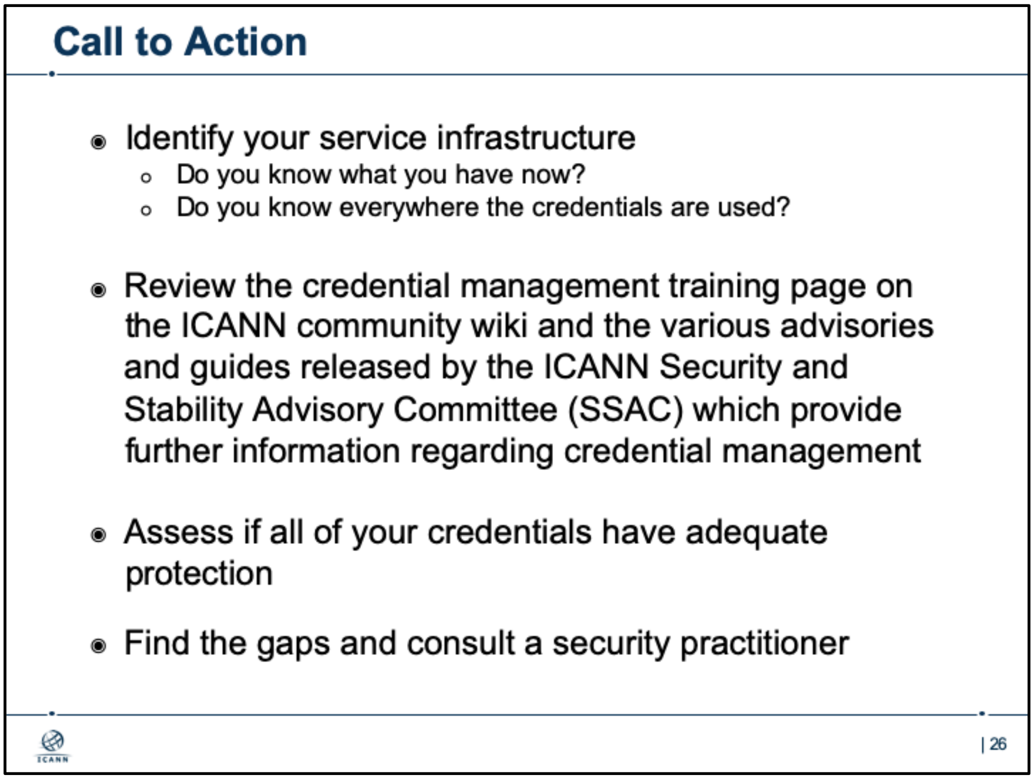
1 Objective

2 Background

3 Risks

4 Lifecycle & Best Practices

5 Call to Action



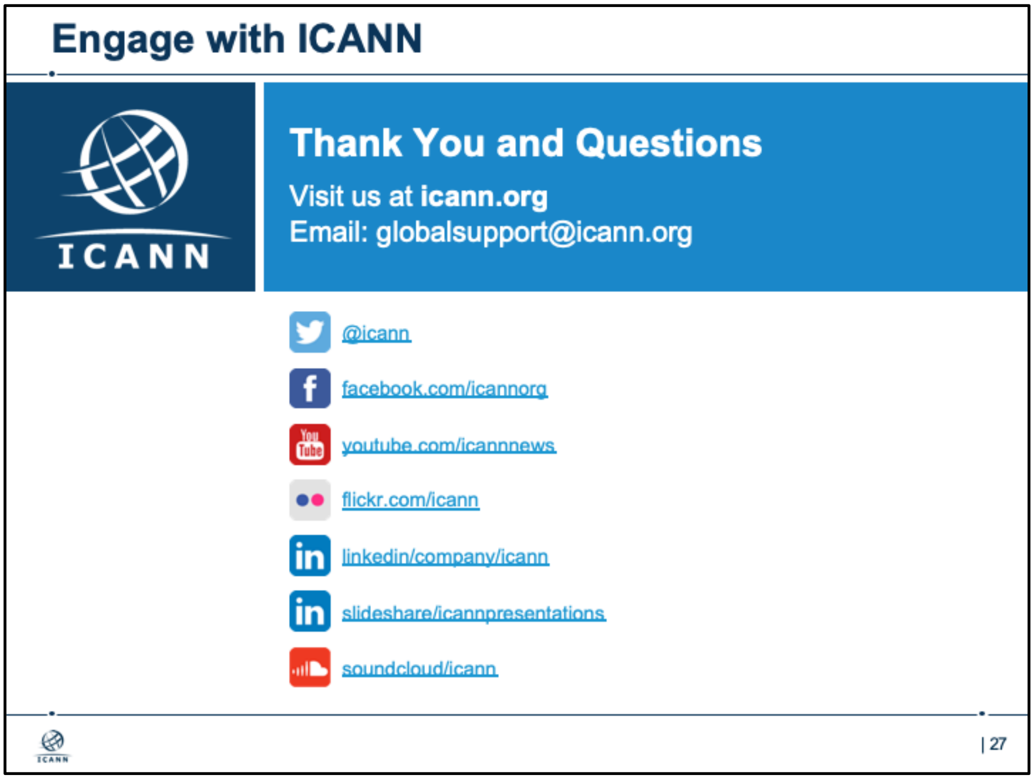
Call to Action

- Identify your service infrastructure
  - Do you know what you have now?
  - Do you know everywhere the credentials are used?
- Review the credential management training page on the ICANN community wiki and the various advisories and guides released by the ICANN Security and Stability Advisory Committee (SSAC) which provide further information regarding credential management
- Assess if all of your credentials have adequate protection
- Find the gaps and consult a security practitioner

Based on this course, it is important that you have better information for your service infrastructure. Do you know what you have now? Where the credentials are used? Review the credential management training page on the ICANN community wiki that provides further information regarding credential management

Know what security controls you have in place. Conduct a detailed assessment to evaluate if your credentials have adequate protection.

If something does not look right or if you're not sure if it looks right, ask a practitioner. You won't regret it when and if something happens.



Engage with ICANN

Thank You and Questions

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

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann