SAC074

SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
03 November 2015

Preface

This is an advisory to the ICANN Board, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) on **Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle**.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this advisory, references to SSAC members' biographies and disclosures of interest, and individual SSAC members' withdrawals and dissents with respect to the findings or recommendations in this advisory are at the end of this document.

Table of Contents

Executive Summary

Attacks that compromise registrant data and/or the Domain Name System (DNS) settings of *domain names*[1] continue to be a significant problem for registrars and registries, as well as for the registrants themselves and the users of their sites. This Security and Stability Advisory Committee (SSAC) advisory provides background about this problem, including numerous examples, and explains the *credential management* lifecycle and related terminology for the Internet Corporation for Assigned Names and Numbers (ICANN) community.

This advisory then provides specific best practice guidelines that will help registrars and registries enhance the security of domain names and the systems that support them. Section 6 of this advisory contains these best practices, addressing the entire credential management lifecycle.

SSAC makes four recommendations to ICANN, which are described fully in Section 7 below:

Recommendation 1: As part of regular reports, the ICANN Compliance Department should publish data about the security breaches that registrars have reported in accordance with the 2013 Registration Accreditation Agreement (RAA), paragraph 3.20. [2]

We do not, at this time, recommend whether registrars' names be published or not. However, we do recommend that statistics about the number of breaches and the number of registrars affected, the aggregated number of registrants affected, and the high-level causes of the breaches, including specifying which breaches could be attributed to a problem in the credential management life cycle would be illuminating to the community and will emphasize the need for good security measures to be followed by registrars. We believe that this data can be appropriately anonymized, and still be a useful way to provide better information to the Registrar community as to the nature of the threat landscape. We observe that the term 'security breach' in the 2013 RAA is defined as 'any unauthorized access to or disclosure of registrant account information or registration data.' It would be helpful in the reported data and any statistical summaries to distinguish between, on the one hand, breaches of registrar systems or unauthorized release of data by the registrar itself, and, on the other hand, unauthorized access or disclosure due to individual registrants losing control over their credentials in a way not attributable to their registrar's systems or controls.

[1] Appendix A provides a Glossary of Terms. Terms defined in the Glossary are italicized the first time they are used in the text of this Report.

[2] See https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#3.20.

Recommendation 2: A provision similar to 2013 RAA paragraph 3.20 should be incorporated into all future registry contracts, with similar statistics published as per Recommendation 1 above.

Recommendation 3: Future RAA deliberations should encourage stronger authentication practices, specifically the use of multi-factor authentication.

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. We would welcome the opportunity to advise training staff in the creation of a curriculum.

This effort should involve measurement and outreach including cooperation with other global training efforts with ICANN partners such as ISOC. ICANN should support this effort with adequate staffing and funding. Such a program should cover at least the following topics:

- Create a training program that follows the structure of the DNSSEC Deployment Initiative but that is focused on hands-on training of operational practices that provide best security practices for the credential management lifecycle.
- Create and maintain an information portal, managed by ICANN staff, supported by community subject-matter expert contributions, and with links to educational material.
- Provide an annual report on the work accomplished.

1 Introduction

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. This advisory augments the previous work done in SAC40,[3] which advised registrars on protecting registrant accounts, and SAC44,[4] which advised registrants on protecting their accounts. Both advisories recommended strong identification and *authentication*, but did not itemize specific methods for doing so. This SSAC advisory fills this gap by defining specific best practice guidelines for preserving security and stability in comprehensive domain-related credential lifecycle management. Since registrants, registrars, and registries all manage some aspects of *credentials* relating to domain names, this advisory targets all three communities, with some emphasis on the registrar community. While these three communities address the contracted parties within the ICANN contractual model, added stakeholders should also make note of their credential uses and lifecycle management practices. This includes: Privacy Proxy Services, Resellers, Hosting Facilities and Independent DNS Providers.

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.

This SSAC report recounts recent attacks to motivate the need for action, examines where credentials are used throughout the complete lifecycle of a domain name, and recommends better practices to create a more secure credential management process.

This advisory specifically addresses credential lifecycle practices for designing, creating, distributing, storing, renewing, transferring, revoking, recovering, and destroying credentials associated with a domain name lifecycle. All methods and schemes used to provide authentication of an identity (registrant or authorized administrator of registrar or registry) and *authorization* for specific actions are in scope. The scope also includes highlighting any relevant policy issues that can support or hinder credential management.

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. 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 *PIN*s generated

[3] See https://www.icann.org/en/system/files/files/sac-040-en.pdf.
[4] See https://www.icann.org/en/system/files/files/sac-044-en.pdf.

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).

Information about recent attacks was acquired through searches of public news reporting. Only very limited information about current credential management practices was publicly available because registrars and registries do not generally make their processes public. Additionally, the ICANN 2013 RAA does not contain any meaningful requirements about credential management. It is important to note that the lack of transparency and lack of requirements in this space prevents any rigorous analysis of the current situation or the effectiveness of any measures undertaken to improve the situation. This assessment of the current state of the practice is based on private conversations with registrars and registry operators and what can be deduced from public reporting about attacks.

This advisory specifically addresses protection of a registrant's domain name at the level delegated by a registrar, not further subdomains the registrant may administer.

2 Recent Attacks

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. Typical attack vectors, and instructive examples of specific attacks that occurred between March 2012 and March 2015, are reviewed below, with further examples contained in Appendix B. While the examples below point to specific publicized events, they are not meant to single out specific registrars or registries, but rather illustrate the importance and immediacy of the problem.

Re-using the Same Username/Password Combination

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: a

single compromise of a user/password combination can be used to attack other sites. One clear example was the attack at the domain registrar Namecheap in January 2014.[5]

Phishing and Spear Phishing Attacks

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. This tactic appears to have succeeded via targeting of GoDaddy registrants in 2012,[6] and other registrars and their customers have also been targeted. A successful detection strategy is for the registrar to identify suspicious access patterns (indicative of credential abuse), as the theft of credentials does not occur on the registrars' systems.

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. Spear phishing reportedly resulted in the change of DNS settings of several high-profile domains in August 2014.[7] Attackers employed a spear phishing attack against staff at a Melbourne IT reseller to capture administrator-level account credentials, and used them to alter name server delegations for several domain names, including NYTimes.com.[8] The attacker changed the content served by the hijacked domains by serving all Internet lookups for those domains via their DNS servers.[9]

Domain Shadowing

Attacks against registrar accounts using stolen registrant credentials continue to escalate and evolve. Recently, the "Angler" exploit kit has drastically increased the use of a tactic called "Domain Shadowing"[10] in which, by using stolen or phished credentials, the malicious actors create numerous subdomains associated with existing, reputable domains in the registrant's portfolio. This tactic has been used since at least 2011, and is even more prevalent today. 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.

---

[5] See http://www.ecommercetimes.com/story/80979.html.
[6] See https://nakedsecurity.sophos.com/2012/11/23/hacked-go-daddy-ransomware/.
[7] See http://www.reuters.com/article/2013/08/28/media-hacking-melbourne-idUSL2N0GT01K20130828.
[8] See http://www.pcworld.com/article/2047628/spear-phishing-led-to-dns-attack-against-the-new-york-times-others.html.
[9] See http://www.cnet.com/news/melbourne-it-tells-how-hacker-launched-ny-times-cyberattack/.
[10] See http://blogs.cisco.com/security/talos/angler-domain-shadowing.

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. 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. This was one of the factors that made a compromise at Melbourne IT so damaging.[11]

Insecure transmission of credentials includes unencrypted email or browser sessions (*cleartext*) and phone conversations. Sending passwords over the phone to customer service representatives has reportedly been common practice at some registrars as recently as July 2013. [12] Ideally, customer service representatives should not have visibility of the primary account password/passphrase. Additionally, customer service representatives should not ask a registrant for their password to verify their identity because the service representative then learns those passwords. In order to allow for phone verification, many registrars have implemented a phone-specific authentication method. These authentication methods can take similar forms to the additional factors often found in two-factor authentication models. They can be in the form of a pre-determined Personal Identification Number (PIN), or by verifying a temporary access code / phrase sent to a mobile device or alternative email by the registrar.

Hacking Attacks

Successful attacks on registrars and registries have allowed hackers to obtain credentials directly from these authoritative systems. An example is the compromise of registrar Webnic.cc in February 2015. The attackers evidently obtained persistent access into the registrar's systems via a rootkit, granting them access to a variety of credentials.[13] It is not publicly known whether those credentials were stored in cleartext.

On February 23, 2015 attackers briefly hijacked Google's Vietnam domain, google.com.vn. The attackers then updated the domain record of computer manufacturer Lenovo.com, and pointed it to a Cloudflare account that they controlled, where the attackers then intercepted emails sent to the Lenovo.com domain. The main public-facing Lenovo.com website was also disrupted on February 26, 2015, and was unavailable for some time. Neither of the hijacked domains was protected with a registry lock.

During the incident the attackers also claimed that they had obtained the *EPP (Extensible Provisioning Protocol)* AuthInfo codes for domains that the registrar sponsored[14]; however this claim has not been publicly substantiated.

---

[11] See http://www.itnews.com.au/News/374095,melbourneit-storing-domain-passwords-in-cleartext.aspx.
[12] See http://security.stackexchange.com/questions/39621/is-my-domain-registrar-storing-my-password-in-cleartext.
[13] For accounts of the compromise, see: http://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/ and http://www.theverge.com/2015/2/25/8110201/lenovo-com-has-been-hacked-apparently-by-lizard-squad.
[14] See https://twitter.com/LizardCircle/status/570732413971800064 and http://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/.

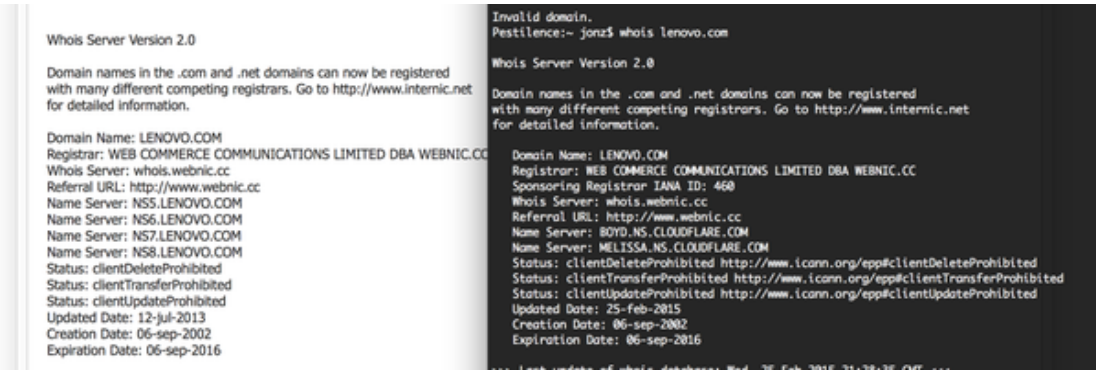

Figure 1: DNS records for Lenovo.com, which was hijacked on 25 February 2015. The record on the left shows the record before the hijack, and the right shows the record while the attack was in progress.

Compromises of Unclear Mechanism

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. For example, in August 2013 many .NL websites were redirected to a handful of IP addresses controlled by a malicious party, which replaced legitimate content with malicious content. This kind of attack is dangerous because the hijacked domains, benign for their lifetime, will bypass domain-based blacklists or domain reputation filters, and end users largely cannot protect themselves.[15] The domains that were redirected all belonged to only three web hosting companies.[16] The distribution and nature of this attack suggests that the attackers compromised credentials at those three companies and used them to make apparently legitimate changes in the .NL registry. Although there is no evidence of a direct relationship, the .NL registry's website was compromised the month before, and it is plausible the credentials used to redirect the websites were compromised in a sort of *watering hole attack*.

Similar attacks have occurred against the Uganda,[17] Guadeloupe,[18] Romania,[19] Ireland, Tajikistan,[20] and Pakistan Topic Level Domain (TLD) registries, through a variety of attack methods. Some of the attacks appear to have bypassed a TLD's credential management system altogether, but in the Uganda case the registry statement indicated the likely cause was compromised registrar credentials. In 2013 Markmonitor counted twenty-three registry breaches, noting that "popular ccTLD [country code Top Level Domains] registries such as .CN (China), .BE (Belgium) and .MY (Malaysia) were all impacted by issues arising from Distributed Denial of Service (DDoS), Social

[15] See http://blogs.cisco.com/security/dns-compromise-distributing-malware/.
[16] See http://blog.fox-it.com/2013/08/05/dns-takeover-redirects-thousands-of-websites-to-malware/.
[17] See http://news.softpedia.com/news/Sony-PayPal-Gmail-Intel-Yahoo-Uganda-Domains-Hacked-via-DNS-Poisoning-362340.shtml.
[18] See http://thehackernews.com/2012/11/guadeloupe-national-domain-registrar.html.
[19] See http://arstechnica.com/security/2012/11/google-microsoft-paypal-other-romanian-sites-hijacked-by-dns-hackers/.
[20] See http://thehackernews.com/2014/01/Tajikistan-Google-Twitter-hacked-Domain-Registrar.html.

Engineering and Brute Force attacks."[21] Please see Appendix B: "TLD Registry Breaches" for more details.

Registrars also come under attack from sophisticated actors whose goal is to modify Internet architecture to achieve further objectives. For example, Enom.com detected a highly targeted redirection of domains in May 2015.[22] and coordinated the response to the hijacking with the assistance of U.S. Federal law enforcement.

Credential Management Incident Response Errors

Important lessons can be learned not just from recent attacks, but from responses to them. Attacks cannot be completely prevented, so it is critical to have an incident response plan for when attacks occur.[23] ICANN's 2013 RAA requires that registrars notify ICANN of security breaches that result in unauthorized access to registrant information.[24] Further, it is best practice for a registrar or registry to notify its customers of a breach once detected, and if the credentials or credential management system may have been compromised, to recommend that customers change their password.[25]

However, *it is important that customers know the format of such notifications ahead of time, and to make sure that the notification email comes from a trusted and recognizable domain name, Pretty Good Privacy (PGP) signed, and the password change service is on a known site*. Lessons for how not to format such password breach notification emails can be gleaned from Moniker's handling of a 2013 compromise. The process Moniker followed was sound, but customers often discarded the email that notified them of the breach as a suspected phish, which cost valuable time during the incident response.[26]

3 Credential Types

There are a variety of mechanisms, generically *credentials*, for users to prove their identity and authenticate to registrars. Once authenticated, users can register new domains, transfer ownership, remove existing domains, or modify DNS records. When a malicious entity undertakes these actions it causes significant problems or financial harm to individuals, organizations and companies. Credential types used in the domain name industry include:

---

[21] See https://www.markmonitor.com/mmblog/2013-domain-name-year-in-review/.
[22] See http://www.thedomains.com/2015/05/20/enom-com-informs-customers-of-very-sophisticated-attack-but-no-domains-were-stolen/.
[23] See http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?.
[24] ICANN 2013 RAA, paragraph 3.20: "Registrar will give ICANN notice within seven (7) days of... any unauthorized access to or disclosure of registrant account information or registration data. The notice required pursuant to Subsection (iii) shall include a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response."
[25] See SAC-040; https://www.icann.org/en/system/files/files/sac-040-en.pdf.
[26] See http://news.softpedia.com/news/Domain-Name-Registrar-Moniker-Hacked-Users-Forced-to-Change-Passwords-362278.shtml.

Digital Certificates: A *public key infrastructure (PKI)* provides the components and services that enable practical deployment and operation of a system that uses *digital certificates*. Digital certificates are data structures that bind (associate) a public key with the identity of a process or system as verified and signed by a trusted entity. Usually the trusted entity is an independent third-party whose primary function is to certify certificates, called a Certificate Authority (CA). Because these certificates are signed by another trusted signing entity (the CA), it is imperative to create an appropriate trust relationship with the CA and to ensure appropriate procedures and policies exist to avoid any breach of trust. 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 that is issued. An entity validating a digital certificate must be able to check the digital signature by using the public key of the trusted signing entity, many of which are pre-installed in modern web browsers and operating systems. In the Internet Engineering Task Force (IETF) there is work ongoing to sign certificates with the help of DNS Security Extensions (DNSSEC), which would imply a different chain of trust be built for Digital Certificates than the traditional use of CAs that is described here.

Domain AuthInfo Code. The *Domain AuthInfo Code* is a secret code shared between a registrar and a registrant. The registrar relies on the code to initiate the transfer of a domain name from another registrar. This is a measure designed to prevent unauthorized domain transfers. The EPP <domain: authInfo> element is defined in RFC5731,[27] and EPP AuthInfo codes are stored in registry databases.

In generic Top Level Domains (gTLDs), every registrar is required by ICANN's Inter-Registrar Transfer Policy[28] to give the AuthInfo code to the registrant, who can give it to any other registrar to initiate a valid transfer request. The policy requires registrar-generated AuthInfo codes to be unique on a per-domain basis (noting that this does not mean it can or should be used to identify a Registered Name Holder).[29]

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), and something "that you are" (something about you that is unlikely to change over time, such as a biometric attribute).

One Time Password (OTP): A password that is valid for only one login session or transaction on a computer system or other 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, for example a text message to a pre-registered mobile phone number.

---

[27] See RFC5731: https://tools.ietf.org/html/rfc5731.
[28] See https://www.icann.org/resources/pages/registrars/transfers-en.
[29] See ICANN Inter-Registrar Transfer Policy, section 5: https://www.icann.org/resources/pages/policy-2012-03-07-en.

Password/Passphrase: A string of characters from a set of acceptable characters that is a secret shared between a user (or client) and the systems (servers) to which that user authenticates. The length and complexity of the string affect the strength of the password in resisting a brute force attack.

Public/Private Keys: An encryption and authentication scheme based on a pair of cryptographic keys that is owned by each party. The Public Key is made publicly known and is used to encrypt data intended *for* that party or to authenticate (verify the signature of) data coming *from* that party. A party's Private Key is kept secret and used to authenticate ("sign") data sent by that party, and to decipher encrypted data sent *to* that party.

Symmetric Keys: An encryption or decryption key that is known only by authorized parties. Typically a *secret key* is used in symmetric key encryption technologies where two parties share the same secret key.

User ID: A *User ID* is a unique character string (often an email address) or numeric value used by a system to identify a specific user.

4 Credential Use

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.

At a high level, the domain industry has three general distribution models:

1. The registry operator interacts solely with registrars, who offer domain names to registrants. In this model each registrar is responsible for all interactions with its registrants.
2. The registry operator has registrars, but the registry operator also acts as a registrar. In this model each registrar is responsible for all interactions with its registrants.
3. The registry operator acts as the sole registrar for the TLD. The registry operator interacts directly with all registrants.

In addition, some registrars have resellers, which access the registrar's system in order to create and manipulate domains in the registry on behalf of their registrants. Some companies that sell domain names to the public are fully accredited registrars for some TLDs and have direct access into those registries, and offer additional TLDs by acting as a reseller of another registrar that has direct access to those other TLDs. As a result, the access credentials that are used depend upon the role that an entity is fulfilling at a given time or for a given interaction.

This table lists the most common credentials used in the domain name industry, the purposes for which they are used, and the parties who use them.

Table 1: Various Credential Types, Their Purpose, and Who Uses Them

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
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

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

All credentials need to have a secure process for credential management regardless of their purpose. Compromise of any of the abovementioned credentials by someone with malicious intent could cause severe damage to the resources controlled by that entity. Attack vectors can include modifications to domain holder registration, DNS entries, transfer options and renewals, responsible contact information as well as billing information for credit card fraud or identity theft. Successful attack consequences include significant damage to brand reputation, financial implications as well as time costs required to investigate and rectify the damage.

5 The Credential Management Lifecycle Today

Credentials have a lifecycle for their initiation, maintenance and associated support.[31] 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.

Recently, some registries have allowed registrars to fund their accounts with the registry using credit cards, while others have created direct debit access methods. In these cases, registry operators must take special care regarding the holding and management of credentials associated with credit cards and banking information. In situations where Cardholder Data is involved, there are controls specifically prescribed by the Payment Card Industry Data Security Standards (PCI DSS) that must be met. PCI DSS provides a comprehensive baseline of credential management and security measures, and are updated by the major credit transaction networks (Visa, Mastercard, etc.) periodically in

[30] For more about privacy and proxy services, see the work of the PDP Privacy & Proxy Services Accreditation Issues Working Group, at: http://gnso.icann.org/en/group-activities/active/ppsa

[31] See http://www.idmanagement.gov/glossary/letter_c.

an attempt to compensate for changing attack methods and complexity.[32] Many companies who regularly handle transactions involving credit cards go through extensive audits annually to attest that they are meeting these standards.

Some registries have switched from a "deposit" account model (pre-pay) to a "credit" account model (post-pay). The post-pay model sometimes reduces the number of transactions that the registry has to account for from a security and credential management point of view, and also reduces some real-time dependencies of domain registrations on finance functions.

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. As demonstrated in **Table 1** above, most registrants are identified by e-mail addresses or account IDs and are validated only through the use of passwords/passphrases. Registries validate registrar identities with a wider variety of credential types. In many cases one credential provides all access with no further checks. How long the user remains authenticated varies, but at some registrars the user can remain logged in for days. Human-generated and human-input passwords are being phased out as single factor authentication because, in general, they are no longer considered sufficient protection for a resource of even moderate value – they are either too easy to break or too hard to remember.[33] A variety of programs for automated password generation and management[34] are available, and already in use. These programs and applications are designed for use by end users and can help registrants keep track of and improve the security of their own credentials, but cannot be directly required by a registrar or registry.

Based on the anecdotal information available, some registrars and registries have implemented stronger validation measures, such as two-factor authentication, source-IP-address validation, or manually verified keys. Two-factor authentication may be in the form of a short-lived one-time password (OTP). The OTP is either generated by a hardware token or software application, or sent to an enrolled mobile device. Allowing log-ins only from a pre-arranged set of IP addresses is a useful second factor. However, this relies on the integrity of global routing and IP-address delegation, which are not foolproof. Thus address validation by itself is not sufficient. Manually distributed and

[32] See https://www.pcisecuritystandards.org/security_standards/.
[33] See Shimeall, T., & Spring, J. (2013). *Introduction to Information Security: A Strategic-based Approach*. Newnes. pg 130.
[34] See http://lifehacker.com/5529133/five-best-password-managers.

verified (i.e. carried by human courier rather than over the network) cryptographic keys provide a very high degree of assurance in the validation process.

A special case to consider is how to authenticate an interaction that is not over the Internet, but still remote. Registrars and registries usually have a telephone number for serving users. On telephone conversations, cryptographic integrity is not readily possible, and passphrases must be used with requirements different from typed passwords ("choose a verbal passphrase with a number and a symbol in it" doesn't really make sense). A pre-authorized list of contacts and their phone numbers is a technique some registries add when validating registrar personnel. Callback to a number on the list increases the strength of the authentication. Modification of names on the pre-authorized list is a tightly controlled process at some registries, while informal at others.

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. Some registries require only that the registrant pass a "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part" (*CAPTCHA*) as evidence of human creation. Other registries require the registrant to appear in person with certain government-issued identification. Registry authentication of a new registrar, or vice versa, is a process bound by international contract law, and thus rather rigorous. However, requesting a new account for an employee of a registrar or registry at another organization (e.g. a registrar employee account at a registry) may be as simple as a phone call or help-desk email with little formal authentication.

Distributing

Credential distribution means getting the credential to every person or process that needs to use it. 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. A third party may create the credential, such as hardware OTP generators, and distribute relevant elements to each party. Each of these situations has unique considerations, but the most common tacit user expectation is that during distribution the credentials are protected by strong cryptography,[35] including verification of message integrity, and that credentials are exposed as little as possible.

Registrants, registrars, or even registries do not always meet this expectation. Passwords are often written down to distribute them to coworkers who share the same account (this is in itself bad practice – *each person should have their own account for the role or relevant function*). Paper and pencil distribution is not ideal, but it is far better than unsecured electronic distribution, over email or chat for example. As at creation time, each of the individuals receiving the credentials must somehow have their need for access validated. Shared credentials make this process harder to track, make auditing access/security events less effective and make revoking credentials for an individual intractable.

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.[36] Computer-generated private keys can be stored by encrypting them with a key derived from a password/passphrase for extra protection (as in PGP [Pretty Good Privacy]).

Problems arise when those who authenticate credentials cache valid credentials and/or a cookie representing the fact that the credential has been validated so users don't need to constantly type in their passwords. Caching creates a time window during which an attacker can obtain the cached credential and use it.

This vulnerability is particularly severe on Windows machines, where a family of attacks called "pass the hash" is prevalent. Multiple features of a networked Windows environment combine in such a way that the adversary can bypass the need to crack the password hash at all and just use the cached or stored hashed credential as a validation mechanism, bypassing legitimate authentication.[37] Any credential storage scheme is vulnerable to credential caching attacks, however the attacks on Windows are particularly easy, well known, and exploitation code is freely available.[38] Many registrants, registrars, and registries have vulnerable Windows machines being utilized for important management functions, increasing the risk of credential compromise. Regardless of the Operating System used for storing credentials, registries and registrars should be aware of

[35] See Section 5.6. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.
[36] See http://www.dirmgr.com/blog/2012/6/12/how-linkedin-missed-out.html.
[37] See http://passing-the-hash.blogspot.com/2014/03/guest-post-lets-talk-about-pass-hash-by.html.
[38] See https://community.rapid7.com/Rapid7_BlogPostDetail?id=a111400000AajbcAAB.

these kinds of issues and have mitigation plans in place to deal with a breach or compromise to these systems.

Backing up key material is a special case of storage that is handled quite differently from usual storage. Backups of passwords/passphrases, private keys and secret keys need to be readable in an emergency. Therefore backups need to be stored offline or otherwise physically separated to minimize compromise. Not all registrars and registries separate backups in this way.

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.
- Protection of information that can be used to change a credential at the same level of protection given to the credential itself.

Credential reuse prevents users from selecting the same password as their last password, or last 5 passwords, for example. There are anecdotal stories of users not understanding that "change" password meant switching to a different password, the user thought the act of password change somehow fixed compromised passwords by itself. Reuse limitations overcome this particular user education issue.

Users change credentials with a variety of mechanisms, such as via a web session, via encrypted email, in person, or via the help desk. Each mechanism has challenges. For example help desk requests are sometimes hard to authenticate. Encrypted email can be hard to acknowledge in a different message channel, though text messages may work.

Important information includes more than just the credential itself – it includes any information that may be used to validate an identity. Names, phone numbers, IP addresses, physical addresses, email addresses, security questions, and fax are used by registrars and registries in some combination to validate identities at least in some workflows, including recovery of credentials. These information items, or some subset of them, can be used to gain control of an identity.

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 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,[39] all gTLD registries use EPP.[40] A valid EPP AuthInfo code[41] is required to initiate a registrar-to-registrar transfer (see Section 3 for more about AuthInfo codes). Many registrars change a domain's AuthInfo code after the domain has been transferred.

ICANN policy also contains provisions for revoking improperly requested transfers. Registrars can use revocation procedures to recover from situations in which an AuthInfo code was obtained or used improperly and leads to a domain hijacking. In order to deter hijacking some registrars also have an optional process of domain locking. If a domain is locked transfer requests are rejected unless the registrant provides out-of-band instruction to unlock the domain.[42]

However, these policies may not always be implemented, and some registrars have reportedly used registrant account passwords as AuthInfo codes. Additionally, registrars must protect the AuthInfo codes they assign and receive. There are unconfirmed reports of hackers using AuthInfo codes for domain hijacking.

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. Common structures in use for revoking credentials include revocation lists such as certificate revocation lists (CRL).[43] The authentication system Kerberos (Microsoft Active Directory and many open source solutions use Kerberos[44]) has an account lockout function, but no explicit credential

[39] See https://www.icann.org/resources/pages/policy-transfers-2014-07-02-en.
[40] See http://icannwiki.com/EPP.
[41] See RFC 5731 at https://tools.ietf.org/html/rfc5731.
[42] See http://icannwiki.com/Domain_Locking.
[43] See http://tools.ietf.org/html/rfc5280.
[44] See http://www.kerberos.org/software/whykerberos.pdf.

revocation function besides destroying an account,[45] which makes this function difficult for some organizations to execute in short time frames.

When personnel turn over at registrars, registries, or corporate registrants the departing person sometimes provides all access information to their successor. The successor rarely changes the credentials, which allows for the former employee to potentially still have access to the registrar account.

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.

While such a process is necessary, this process is a likely target for attacks attempting to gain unauthorized access. In particular, there does not appear to be wide awareness of the dangers of using email (which relies on proper functioning of the DNS) to verify elements of DNS functionality. If attacks are successful, as described above, the attacker gains the ability to change nearly anything relating to the domains and the domain management account. This might include the registrant name, contact information, password, PIN, payment profile or billing information, and even the two-factor authentication elements.

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.

[45] See http://web.mit.edu/kerberos/krb5-1.13/doc/admin/lockout.html.

6 Practical Checklist / Credential Management Best Common Practices

There are practical improvements that can be made to all stages of the credential management lifecycle. We present these overall considerations for implementing best current practices for each stage in the lifecycle in the same order the stages were presented in the prior section. Familiarity with SAC40's and SAC44's recommendations will help the reader contextualize this report, however reading them is not necessary to make use of the recommendations presented here.

Refer to Established Best Practices

First, SSAC recommends that registries and registrars refer to community vetted and standards-based documents since these are well defined and continuously evolving to what the information security community believes to be best current practices. These documents address security controls in a methodical and holistic approach and cover much more than just credential management. The specific sections that pertain to credential management are highlighted.

- The Critical Controls[46] are a recommended set of actions for information security defense that provide specific and immediate high-value actionable ways to stop today's most pervasive attacks. They were developed, vetted and are maintained by a consortium of hundreds of security experts from across the public and private sectors.
- Registrars and registries should refer to the ISO 27000 family of standards, which help organizations keep information assets secure.
- ISO/IEC 27001 specifies requirements for an information security management system (ISMS). This standard includes risk assessment and a list of security controls and their objectives.
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining ISMS. This standard includes access control, operational security, and communications security.
- Registrars and registries that take credit card information from users should refer to the controls specifically prescribed by the PCI DSS. PCI DSS[47] provides a comprehensive baseline of relevant credential management and security measures.

The following sections of the PCI DSS specifically pertain to aspects of credential management and cover in detail aspects of password length, strength, rotation, session timeouts, incorrect login attempts, minimum necessary access, etc.

[46] See http://www.counciloncybersecurity.org/critical-controls/.
[47] See https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

- Requirement 8: Identify and authenticate access to system components
- Requirement 3.2: Credential Storage
- Requirements 3.5 – 3.7: Cryptographic Key Management

Multi-Factor authentication remains a key element in efforts to establish a more secure environment. There are many variations on how and when a multi-factor model could be implemented, but many web application environments could benefit from the proper implementation of such a methodology.

- The World Wide Web Consortium (W3C)[48] group is publishing a guide to help implement strong multi-factor authentication.

Designing

Attacks cannot be completely prevented, so design should include risk assessment and incident response plans.[49]

- 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.
- Create and implement an incident response plan.

[48] See http://www.w3.org/Security/.
[49] See http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?.

Creating

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.

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 such as Hypertext Transfer Protocol Secure (HTTPS) or Secure Shell (SSH)[50] 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.

[50] See NIST SP [[need to look up pub number]] for specifications on what is considered a strong algorithm and key size for a safe encrypted channel.

Storing (including 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, 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.
- Registries and registrars should have clear policies and procedures for storing or backing up credentials.

Changing

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.

Renewing

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.

Transferring

Registrars and registries are required to follow ICANN's Inter-Registrar Transfer Policy for handling AuthInfo codes (see Section 5 of the policy).

Revoking

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. Personnel turnover should result in automatic credential termination by use of individual logins, along with hardware tokens retrieved on employee termination or, where appropriate, OTPs sent in text messages as a second factor.

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. (One way to handle session termination is to routinely check whether a password change has happened during an active session.)

Recovering

Registrars and registries should increase internal awareness that credential recovery processes are common targets for adversaries.

a. 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.

b. 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.

c. Registrars should pay attention to non-delivery notices for email sent to email accounts.

Destroying

Destroying credentials is the last stage in the credential management lifecycle.

a. Credentials, and any information that can be used to recover or create credentials, should be destroyed when no longer needed.

b. 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.

c. 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.

d. Registrars and registries should have well-formed processes to ensure that all copies of a credential are destroyed during this phase, including any backups.

7 Recommendations

SSAC makes the following recommendations to ICANN:

Recommendation 1: As part of regular reports, the ICANN Compliance Department should publish data about the security breaches that registrars have reported in accordance with the 2013 RAA, paragraph 3.20. [51]

[51] See https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#3.20.

We do not, at this time, recommend whether registrars' names be published or not. However, we do recommend that statistics about the number of breaches and the number of registrars affected, the aggregated number of registrants affected, and the high-level causes of the breaches, including specifying which breaches could be attributed to a problem in the credential management life cycle would be illuminating to the community and will emphasize the need for good security measures to be followed by registrars. We believe that this data can be appropriately anonymized, and still be a useful way to provide better information to the Registrar community as to the nature of the threat landscape. We observe that the term 'security breach' in the 2013 RAA is defined as 'any unauthorized access to or disclosure of registrant account information or registration data.' It would be helpful in the reported data and any statistical summaries to distinguish between, on the one hand, breaches of registrar systems or unauthorized release of data by the registrar itself, and, on the other hand, unauthorized access or disclosure due to individual registrants losing control over their credentials in a way not attributable to their registrar's systems or controls.

Recommendation 2: A provision similar to 2013 RAA paragraph 3.20 should be incorporated into all future registry contracts, with similar statistics to be published as per Recommendation 1 above.

Recommendation 3: Future RAA deliberations should encourage stronger authentication practices, specifically the use of multi-factor authentication.

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. We would welcome the opportunity to advise training staff in the creation of a curriculum.

This effort should involve measurement and outreach including cooperation with other global training efforts with ICANN partners such as ISOC. ICANN should support this effort with adequate staffing and funding. Such a program should cover at least the following topics:

- Create a training program that follows the structure of the DNSSEC Deployment Initiative but that is focused on hands-on training of operational practices that provide best security practices for the credential management lifecycle.
- Create and maintain an information portal, managed by ICANN staff, supported by community subject-matter expert contributions, and with links to educational material.
- Provide an annual report on the work accomplished.

8 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

8.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this Advisory.

SSAC Members

Greg Aaron
Jeff Bedser
Don Blumenthal
Ben Butler
KC Claffy
Merike Kaeo
Mark Seiden
Doron Shikmoni
Julie Hammer
Ram Mohan
Rod Rasmussen

ICANN staff

Julie Hedlund
Kathy Schnitt

8.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2015-06-15-en

8.3 Dissents

Mark Seiden has provided this dissent:

As an active member of this work party, I regret dissenting with this report's recommendations. As a whole they fall short of recommending that the ICANN Board require any basic technical protection for parties whose credentials have been breached.

The current recommendations do little harm, but miss the opportunity to go far enough to be useful in addressing actual breaches.

A credential holder needs to find out about (e.g.) the loss of a password (the best known example of a static credential) so they can manage their own risk after the breach, usually by changing the password. The same breached password might be used, for example, by a reseller or a registrant at a multiplicity of registrars, or by a registrar at a multiplicity of registries. So the password may need to be changed in lots of places. If not informed of a breach, there is significant risk of loss of valuable assets, direct operational impairment, and consequential damage.

Two practical mechanisms for finding out about such breached credentials are - direct notification by the party who became aware of the breach and - publication of the details of the breach with adequate specificity.

Though noting that notification to credential holders of loss of their credentials is a best practice, this report does not go so far as to recommend that ICANN require prompt notification to credential holders by all Contracted Parties who become aware of such a loss, and, further, to require that business associates of Contracted Parties (such as resellers, vendors, subcontractors, privacy protection services) be similarly contractually required to take action of a sort resulting in prompt notification to the holder of the breached credential.

Paradoxically, many data breach laws already require notification and (in many cases) publication of applicable breaches, so an ICANN contractual requirement for breach notification (unless inconsistent with applicable law) would likely not be surprising to many. It would beneficially clarify the need in cases where certain kinds of valuable breached credentials are not covered by particular data breach laws (cryptographic keys, and other shared secrets, for example, may not be mentioned in laws which typically have focused on Cardholder Data, and Personal Information breach which can result in identity theft).

The recommended aggregated statistical information should be of use to analysts, but does not inform credential holders whose accounts are compromised. Absent a contractual requirement to promptly notify, the prompt publication of breach details could serve a similar purpose if specific enough so cardholders could identify that they are among the affected group.

- The Work Party has not determined what use ICANN makes of the breach reports they receive under section 3.20 of the RAA, but has been told that when past reports were supplied by registrars there might be an expectation that data reported would be kept in confidence by ICANN. My opinion is that an excess of sensitivity to this mere possibility has weakened Recommendation 1.

My additional recommendation to the Board is that ICANN publish full breach details starting as soon as this becomes possible, and if needed to notify contracted parties to adjust their expectations that this will soon occur, thus eliminating any future expectation of privacy in the interests of transparency about misfeasance or operational failure.

- Due to lack of time, this report is incomplete in some areas which, in my opinion, would have been better included than omitted in a document intended to be definitive. While these omissions are not worthy of a dissent on their own, I will mention them now in passing as possible future work areas:

The report does not currently cover in enough detail the use and flow of credentials in contexts beyond the expected Registrant, Registrar and Registry (including addressing critical parties such as resellers, privacy proxies, operators of DNS and DNSSEC services), and there is no recommendation addressing the possibility of those parties mishandling credentials.

The report does not discuss any requirements for Contracted parties to provide transparency in credential management or other security practices (of the sort one would find in a Certificate Authority's Certificate Practice Statement.)

To summarize: We start out, and are left with a lamentable situation where a registrant (for example) may not be reliably able to determine how their credentials are handled and, even worse, even after a breach, may not reliably find out that their credentials are compromised.

8.4 Withdrawals

There were no withdrawals.

Appendix A: Glossary of Terms

A quick reference guide for terms used in the documents. Where possible, definitions from authoritative sources are used.

- *Access Control* – The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
- *Asymmetric Key Pair* – A cryptographic key pair that is utilized in asymmetric algorithms.
- *Authentication* – The process of verifying a claim that a system entity or system resource has a certain attribute value.
- *Authorization* – An approval that is granted to a system entity to access a system resource.
- *Biometric Authentication* – A method of generating authentication information for a person by digitizing measurements of a physical or behavioral characteristic, such as a fingerprint, hand shape, retina pattern, voiceprint, handwriting style, or face.
- *CAPTCHA* – a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot (http://www.captcha.net/); stands for "Completely Automated Public Turing test to tell Computers and Humans Apart."
- *Cleartext* – Any information that is not encrypted.
- *Credential* – Data that is transferred to establish the claimed identity of an entity.
- *Credential Management* – Refers to maintenance of a credential from the time it is created to the time it is destroyed.
- *Digital Certificates* – Data structures that bind a public key to the identity of a process or system as verified and signed by a trusted entity.
- *Domain AuthInfo Code* – The AuthInfo code is a secret code shared between a registrar and a registrant with which a registrar initiates the transfer of a domain name to another registrar while preventing unauthorized domain transfers. Use is required by ICANN's Inter-Registrar Transfer Policy. (See also EPP.)
- *Domain Name* – Officially, the list of the labels on the path from a node to the root of the domain name space tree (RFC 1034, p. 6). For the purposes of registrant protection the domain name is the label under the stewardship of a registrant that is acquired from a registrar. Determining this transition label programmatically in a fully-qualified domain name currently has challenges (see SAC-070).
- *EPP (Extensible Provisioning Protocol)* – A protocol that provides

communication between domain name registries and domain name registrars whenever a domain name is registered or renewed. See RFCs 5730-5734. All registries under ICANN contract use EPP.

- *Encryption* – A method of scrambling information in such a way that it is not readable by anyone except the intended recipient(s), who must decrypt it to read it (synonymous with Encoding).
- *Hash Function* – A mathematical computation that results in a fixed-length string of bits from an arbitrary size input; a one-way hash function is not reversible to produce the original input.
- *Integrity* – Assurance that the data has not been altered except by people who are explicitly intended to modify it.
- *Multi-factor authentication* – An authentication method using more than one factor, where factors are classes of authentication tests such as "a thing one knows," "a thing one has," or "a thing one is" (see also password, crypto token, biometrics, authentication).
- *OTP (One Time Password)* – an authentication technique in which each password is used only once as authentication information that verifies an identity. This technique counters the threat of a replay attack that uses passwords captured by wiretapping.
- *Passphrase* – A sequence of words or other text used to control access to a computer system, program or data.
- *Password* – A protected, private character string used to authenticate an identity.
- *Phishing attack* – A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person.
- *PIN (Personal Identification Number)* – A numeric password shared between a user and a system, which can be used to authenticate the user to the system.
- *Private key* – A digital code used to decrypt information and provide digital signatures. This key should be kept secret by its owner; it has a corresponding public key.
- *Public key* – A digital code used to encrypt information and verify digital signatures. This key can be made widely available; it has a corresponding private key.
- *PKI (Public key infrastructure)* – The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.
- *Secret Key* – A digital code that is shared by two parties; it is used to encrypt and decrypt data.

- *Spear Phishing* – A phishing attack that is specifically targets an organization, department or individual.
- *User ID* – A unique character string or numeric value used by a system to identify a specific user.
- *Watering hole attack* – An attack against targeted businesses and organizations. In a watering hole attack scenario, threat actors compromise a carefully selected website, known to be used by the business or organization, by inserting code resulting in malware infection of those accessing the website.

Appendix B: TLD Registry Breaches

.EDU

In early 2013, an initial breach was discovered via the discovery of email redirection of all MIT.edu email to a RIPE IP address. The alleged target of the redirection was email traffic related to government research projects. The registry database was compromised, and the registry operator sent breach notifications to all registrants, asking them to change their passwords. [52] Due to the compromise of the registrant database, it was alleged that attackers had the ability to modify all DNS and account details to all .EDU domains for an undisclosed period.

.RO

Attackers hijacked the .RO domains of Google, Microsoft, Yahoo, and others. Allegedly the DNS records for the affected domain names were modified as a result of a security breach at the RoTLD domain registry, which manages the authoritative DNS servers for the entire .RO domain space. A compromise of the RoTLD Web system used by .RO domain name owners to administer their domains, or the registry's DNS servers, is one of the possibilities. This incident was also alleged to be a possible DNS poisoning attack. A Microsoft report by Cynthia Kern and Nick Whitworth in April of 2013 indicated that twelve TLDs were successfully hacked since November 2012. [53]

.PY

The .PY (Paraguay) registry was compromised on February 20th, 2014. Hackers allegedly from Iran accessed and modified the www.NIC.py database, redirecting www.google.com.py to another site. The hackers posted the entire NIC.py database[54] containing contact names, national ID numbers, street addresses, phone numbers, and more registrant details. In this instance, the hack was done by exploiting a simple remote code execution[55] vulnerability. This is not the first time[56] that NIC.py, managed by the two most respected Computer Science Universities of Paraguay, was hacked.

.PK

---

[52] See: http://www.educause.edu/educause-security-breach-and-password-change-information.
[53] See: http://ccnso.icann.org/files/38133/presentation-cctld-security-assessments-kern-whitworth-08apr13-en.pdf.
[54] See: http://cker.ir/leak/nic-py/.
[55] See: http://ha.cker.ir/2014/02/www-nic-py-py-registrar-rce-vulnerablity/.
[56] See: http://www.abc.com.py/nacionales/confusion-con-antiguo-hackeo-1217054.html

The .PK (Pakistan) registry was allegedly compromised by the same group that allegedly compromised .RO. A PKNIC SQL vulnerability (PKNIC is the Pakistani (.PK) domain name registry) may have allowed hackers from Turkey to hack into .PK domains registered by Google, Yahoo, and MSN, plus nearly 300 other sites. The Turkish hackers also defaced the Google Pakistan homepage.

.TC, .GD, .VG

The "Adamsnames incident" in 2013 allegedly arose out of a business dispute between parties administering services for the .TC, .GD, and .VG registries. See: "KSRegistry has been appointed the new registry operator for Grenada's ccTLD after bad management at the previous operator led to the whole TLD being hijacked."[57]

A hasty switch-over followed the alleged wholesale hijacking of the ccTLDs[58] by a disgruntled former employee of AdamsNames, who temporarily relocated it from the UK to Turkey. The TLDs went offline in March after the former employee apparently took over the domain AdamsNames.net, the web site which was used by registrants to manage their names.

Registry Security Vulnerabilities Exposed

With 23 registry security breaches in this last year, the number of incidents reached an all-time high. Popular ccTLD registries such as .CN (China), .BE (Belgium) and .MY (Malaysia) were all impacted by issues arising from Distributed Denial of Service (DDoS), Social Engineering and Brute Force attacks (source Mark Monitor).

[57] See: http://domainincite.com/12916-ksregistry-takes-over-gd-but-questions-remain-about-two-other-hijacked-cctlds.
[58] See: http://domainincite.com/12238-confusion-reigns-over-three-hijacked-cctlds

Appendix C: Previous SSAC Report References

A number of previous SSAC Reports have examined issues related to the protection of registrant data and offered recommendations for better practices by registrants, registrars and resellers.

SAC040 "Measures to Protect Domain Name Registration Services Against Exploitation or Misuse"[59] (19 August 2009) examined a number of high profile incidents involving domain name registration accounts to determine if there were common causes among the events that might reveal measures to reduce or mitigate certain threats and vulnerabilities. The report examined the incidents in sufficient detail to identify how accounts were compromised, the actions attackers performed once they had gained control of the account, and the consequences.

The report presented security measures used in other Internet business segments (e.g., financials, durable goods merchants) to protect customers from similar vulnerabilities. It identified practices registrars can share with customers so that registrar and customer can jointly protect registered domains against exploitation or misuse, and discussed methods of raising awareness among registrants of the risks relating to even a temporary loss of control over domain names and associated DNS configurations.

It also identified vulnerabilities as well as policies and practices (business and operational) that were exploited to see whether a common thread might emerge.

SAC044 "A Registrant's Guide to Protecting Domain Name Registration Accounts" (5 November 2010)[60] attempted to catalog measures that registrants should consider to protect their domain name registration accounts and the domain names managed through these accounts. The report described the threat landscape for domain names, and identified a set of measures for organizations to consider. It also considered risk management in the context of domain names so that an organization can assess its own risk and choose appropriate measures.

The problems identified in these reports can be summarized as follows:

> **Passwords.** Enforcement of strong passwords and regular password rotation is not widely undertaken by registrants or enforced by registrars. Additionally, password reset and recovery procedures are frequently vulnerable to exploitation.

[59] See: https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf.
[60] See: https://www.icann.org/en/groups/ssac/documents/sac-044-en.pdf.

Predictable Processes. Simple and predictable processes governing the registrar-registrant interactions can provide opportunities for attackers to intervene and exploit those processes to deceive both registrar and registrant.

Authentication. Not all registrars offer strong two factor authentication (2FA) and in some cases where they do, it is not implemented correctly. Similarly, device verification is not widely deployed.

Contact Email Accounts. Simple and singular approaches to the use of contact email accounts provide opportunities for exploitation by attackers.

Responsible Contacts. Identification of one or more individuals as 'responsible contacts' can cause problems when those individuals are absent, or no longer associated with the domain.

3rd Party Access. Registrants can on occasion allow 3rd party access to registration data or to the account itself thereby increasing the risk of compromise or exploitation, especially should a dispute arise.