Responsibilities and Considerations in Secrets Management

Adam Yarborough

ICTN 6823: East Carolina University

Abstract

Secrets management is an aspect of information security management needed for organizations of all sizes. Small organizations may leave all the important passwords in the control of the owner, where larger organizations may have multiple teams dedicated to different facets of information security. This paper will inspect the creation and adoption of specialized roles in information security management with a focus on secrets management. There are commonalities shared between the carefully guarded recipes of a family restaurant, the intellectual property holdings of startups looking for acquisition, and classified credentials protected by nation states. Associated with those commonalities are roles and their positions in the organization structure that were created to protect confidentiality, integrity, and availability. A person may be able to easily remember a single password, like for a website, but maintaining multiple unique passwords across many sites will soon lead to either password re-use or lost credentials. The same happens with organizations of all sizes.

Keywords: Secrets management, Identity management

Introduction

The need for secrets management exists across organizations large and small. There is a misconception that only technical resources are involved in the security and life cycle management of secrets, or that some companies are too small to be engaging in secrets management. While the scopes will certainly change, as do the tools, there are commonalities. As organizations grow, blended responsibilities can become individual roles, particularly when deciding who does what.

The issuing of roles is thought to be establishing a division of work that makes the best use of the skills of employees to efficiently fulfill the tasks and responsibilities needed (Georg & Tryggestad, 2009). It is also worth noting that small and medium sized organizations often find themselves unable to fully implement existing frameworks such as NIST 800-53, ISO/IEC 27001, OCTAVE, or ITIL. This can be due to cost, relative effort, lack of expertise or many other reasons. Alshboul and Streff (2015) write "While these standards are marketed for all sized organizations, the reality is that these frameworks are simply too large and complex for small organizations to understand and operationalize." (Alshboul & Streff, 2015, p. 2).

Key Terms

When discussing the emergence of these secrets management roles in organizations, it is useful to have some clear definitions of terms that are commonly used.

Authoritative is usually used in the context of describing a trusted source of digital identity.

Data are considered "facts" under U.S. law and are not directly protected until intellectual property law, because they are discovered, as opposed to created, by individual works (Kent State University , 2020).

Secrets are defined as digital credentials. Secrets are an umbrella term for passwords, tokens, encryption keys, and so on that are used for access to information. Examples of these include user passwords, temporary access credentials, application keys and APIs, private TLS and SSL certificates, system passwords, and credentials stored in databases (Ekran System, 2019).

Look-up Secrets are computer generated records with a group of secrets shared between and endpoint and a verifier. During authentication, the verifier may ask to provide a specific

record or records based on current conditions (Grassi, et al., 2017). This is most often associated with recovery keys in the case of authentication problems.

Memorized Secret, (password) is *something you know*. This is a secret value that needs to be complex enough that it would be hard for a third party to guess or obtain, that is created and memorized by the user (Grassi, et al., 2017).

Identity Management (IdM), also known as Identity and Access Management (IAM), is a group of technologies and policies that work to ensure that entities are given appropriate access to resources. They are involved in the authentication and authorization of various identities, and control access to resources, usually through role-based access control (RBAC) or attribute-based access control (ABAC). This is plays the role of the verifier of digital identity.

Identity Provider (IdP) is a computer system that holds a set of digital identity attributes (Chadwick & Inman, 2009). It is what stores the representations of roles, attributes, and permissions used by Identity Management system.

Public Key Cryptography is a cryptographic system based on two keys, a public key and a private key. As the names imply, the **public key** is meant to be shared and accessed in the open, whereas **private keys** are usually kept secret by the owner (Lopez, Oppliger, & Pernul, 2005).

Public Key Infrastructure (PKI) is a framework under which public key cryptography that takes public key cryptography from small trusted exchanges to widespread use. This is done via a series of trusts and communications that binds public keys to known identities through a process of registration with a certificate authority (Lopez, Oppliger, & Pernul, 2005). Organizations can have their own certificate authorities as well as go through trusted third parties called validation authorities.

Revocation is the act of retiring or invalidating a secret, most often used upon certificates.

Single Sign On (SSO) is the implementation of protocols integrated with identity providers that allow a single authorization to work with multiple services (Indu, Anand, & Bhaskar, 2017).

Shared Secret is data known only between certain entities.

Transport Layer Security (TLS) is a cryptographic protocol built on public key cryptography for authentication. TLS has additional cryptographic benefits such as forward secrecy which means that future encryption keys cannot be used to decrypt past communications.

Token is a form of secret, or digital credential, that is single use and usually encrypted.

Physical Responsibilities

While most of this exploration of secrets management is more technically or organization geared, it is important to address the first layer of protection. Physical protection makes sure that the way secrets are physically stored are secure. This means usually means the maintenance and protection of barriers separating non authorized individuals from physically obtaining the media in which the secrets are stored on. These barriers come in many forms from locked doors, guarded entryways, and physical safes but also include making sure that the media on which the secrets are located is encrypted. It is useful to note that simply because an individual is trusted to physically secure a secret, that does not mean that the same individual has access to the contents of that secret itself.

Usually, the primary focus of physical perimeter security is on preventing an unknown or malicious actor from taking hard drives or putting a malicious device on the network by blocking them from being able to get access in the first place. There are other benefits and functions to

the organization. Perimeter security can often function as a method of accounting and reporting on access attempts, as well as loss prevention. Physical security guards may log all attempts to access a facility, make note of invalid badge attempts or other suspicious activity and investigate further. In higher security areas, there may be searches that make sure that your secrets do not walk out on an unapproved USB drive hidden in someone's pocket. By controlling physical access to the secrets, you can potentially avoid impersonation attacks with stolen credentials, as well as other methods of compromise. The proper retirement of media also prevents secrets exfiltration though more clandestine methods such as dumpster diving. A form of perimeter security often overlooked is also in the design of office layout to limit activities such as shoulder surfing, or the placement of a physical fence to limit wireless or electromagnetic wave transmissions originating from the organization (Stankovic, 2020).

Finally, physical security also ensures a physical preservation of the secrets as well. This is evident in maintaining physical backups in secure locations, having distributed copies of secrets in the event of failure, and other contingency planning operations. This mirrors many asset management protocols as well.

Each of these aspects and responsibilities of physical protections also require regular maintenance and evaluation from both technical and non-technical resources. They also require a certain level of oversight and trust. A small business owner may write down their website logins in a notebook they keep in their office safe just as a government entity may only let approved individuals access systems after they have been checked for no recording devices in a safe room, but both might regularly sweep areas to make sure no post-it notes with passwords are left on monitors (Templeton, 2014).

Compliance Responsibilities

It is important to decide what the organization's stance is on secrets and their management. Often this comes in the management of the lifecycles of policies and risk management frameworks. There can be legal repercussions for not maintaining compliance, so first and foremost it is important to understand what relevant laws, regulations, and guidelines your organization must adhere to. This includes not only the operational standards for secrets that your organization uses to conduct business, but also any external operational standards that might be imposed.

For instance, an organization might be legally required to comply with NIST 800-63B, which indicates how secrets are to be stored, transmitted, generated, encrypted, and how it can exist in memory (Grassi, et al., 2017). In this document, they state that lookup secrets can be shared between organizations via postal mail or securely in person, but that they must have been generated with at least 20 bits of entropy. It is also defined what complexity rules are enforced in the generation of memorized passwords like maximum password length, susceptibility to dictionary attacks, and use of SMS as a two-factor authentication method (Grassi, et al., 2017). If the organization does not know what obligations it is under, it may not to be able to continue to operate in the manners it desires.

It may be that the organization chooses only certain accounts to be under such restrictions on secret generation, based on context. Like identity and access management, there can be many conditional aspects to secrets management, especially with the rise of infrastructure as code. This will allow for separation of duties as well as the ability to implement a least privilege model for secrets access. The organization may need to maintain internal policies that dictate that hard-coded secrets and default passwords are not allowed in any configuration file, or even take it a

step further to make sure that no secrets are logged even as a part of the debugging process. This is especially important for organizations to determine which type of secret can be used by which entity, in what context, for what purpose (To, 2019).

There also exists cases where secrets need to be shared, especially among teams. Instead of emailing credentials, certs, and application keys, using a centrally managed collaborative and auditable system, a large organization may mandate that only trusted users from trusted computers can access these resources, much like a small company might only let the boss handle certain tasks. As organizations scale, the need to manage secrets does as well. These changes were ushered in with the adoption of complex computer services and cloud technologies, as AWS offers more than 100 services and various teams may all have their own unique instances (Burshteyn, 2018). It should be noted that there are many ways that an attacker will go after secrets, passwords especially, and there are arguments against ever providing shared secrets, and to instead employ federated services that use individual tokens whose revocation is far easier (Corum, 2017).

Defining internal standards of communication and storage of secrets also means that internal compliance can be enforced and measured. There may be the need for regular review and auditing as the company grows or serve as solid guidelines that smaller companies strive for as they implement new policies and procedures. This usually is where the establishment of system-specific security policies occurs, with a split into two groups, managerial guidance and technical specifications (Whitman & Mattord, 2019). It may be that the technical evaluation of a secrets management platform reveals that features of secret versioning and rolling was available, which the management guidance then uses to state that secrets are to be regenerated as opposed to exposing a user to cleartext of the credentials.

The life cycle of secrets is also something that needs to be considered and managed as a policy. If the organization says that passwords must be changed every 90 days, or that TSL certs can only have a maximum lifespan of a year, those definitions are part of the lifecycle policy. Also, making sure to define who can create secrets and under what conditions works within the principles of least privilege.

As such, having company compliance standards does not just mean that the organization is staying within legal boundaries. There can also be internal compliance policies defining behaviors referenced using an older standard, so regular review from teams with both legal and technical expertise is needed.

Technical Responsibilities

Secrets management only works with a functional identity management solution.

Central to the idea of managing secrets is that trusted encryption is used to make sure that as secrets are stored, transmitted, and processed in a secure manner. When evaluating the merits of one secrets management platform over another, careful consideration should be given to how well a platform integrates with the organization's public key infrastructure. While small companies may only use the trusted certificate chains included in their operating systems, larger companies utilize internal PKI implementations in many ways.

One of these ways is machine identity validation. With the rise of automation in infrastructure, there can be rapid creation and destruction of resources that must be able to securely bootstrap a service, server, or container. That resources instantiations need to be able to identify itself as trusted. Secrets management platforms that can issue machine certificates or tokens that increase the ability to trust them (Securosis, 2018). Built into certificates are also validation date ranges, which specify a window in which a certificate could be considered valid.

Another way in which an internal PKI can be used is through key management that handle secure distribution of keys and tokens that would be inherently trusted and decryptable only to internally trusted entities. This differs from machine identity validation, because a service or application may need to unlock or access encrypted data on in limited contexts as opposed to full trusted access all the time. These functionalities can be integrated into applications and services via APIs to allow seamless access to secure resources, which allows for the logging and auditing of such requests without having to save those credentials in a hardcoded values that could be compromised (Securosis, 2018). This is all to exert finer control over what sources the organization's networked resources can trust, and how they operate in transit.

After evaluation of different secrets management frameworks, products, and techniques, there is still the implementation whatever design was deemed best for the organization. For smaller companies, this is usually done in a simplistic manner, such as the discovery of all company passwords and throwing them into an encrypted excel file that only certain individuals have access to. As the size of the organization grows, the need for discovery may still exist, but active collaboration becomes harder. Some teams may implement a self-hosted password management server, such as Bitwarden or other vault solutions, that include directory services synchronizations and API access (Bitwarden, 2020). The larger the organization implementing secrets management systems, the more features and security and complexity gets introduced.

Engineers that have been tasked with implementation might also be tasked with its integrations with other services as well. For instance, the secrets management framework might be able to revoke and update new secrets dynamically, but the users, services, applications, and servers that depend on those credentials aren't able to react as fast as the secrets management

can facilitate yet. Not that this is all setting up a software system, directly. Part of implementing an organization's secrets management framework might be creating policies applied by directory services to ensure that password complexity requirements are met, or working with an individual or team that manages data loss prevention. It could be in scope that the public key infrastructure the organization has in place is also used to encrypt the hard drives of workstations and laptops, as well as store the recovery keys for use in Hardware Security Modules (To, 2019). This is all under the umbrella of working within the defined compliance policies on data governance and availability. As these systems deal with some of the most important organization resources or their access, making sure that the audit logs remain secure, unaltered, and highly available is equally important.

There may be cases in where there are existing secrets management systems, such as used on specific cloud providers. The organization will have to choose if they want to store secrets in multiple locations or a single centralized location (Ruth, 2019). There may be the case in which interoperability or functionality was lost through consolidation, so federations may be an option. Federations of trusts can be set up between various systems and identity providers, whether they are internal or external to the organization. An easy example of external federation could be a website that uses a "Sign in with Facebook" or "Sign in with Google" button for authentication, or webservices that tie back in to AzureAD.

During implementation and maintenance, there are the traditional security concerns associated with these systems. The systems that will be storing, transmitting, processing, and managing the secrets themselves need to be secured, with even more stringent restrictions on the nature of access. They will also need to be configured in a way congruent with the organization's defined operations continuity plan, as well as maintained. It is also important that

where possible, secrets are only transmitted on a network in secure ways to known entities. In an active directory system this may present itself as the usage of Group Managed Service Accounts on specific endpoints to run a service. Group Managed Service Accounts are a password-less account whose credentials and security tokens are managed as a function of the directory services (Microsoft, 2016). Further traditional security practices such as vulnerability assessments, configuration review, and regular review of audit logs will all apply as well.

Organizational Responsibilities

Organizations, regardless of size, need to make sure that its workforce has access to the prerequisite skills to implement whatever secret management policy and framework they have chosen. This can be achieved by employee training, outsourcing, or bringing in resources from various internal teams. This is beyond just technical ability, but also making sure that all employees are trained in the continued use of the system of secrets management. For example: If their passwords have to reach a certain complexity requirement, they will need to know. Organizations will also need to ensure that appropriate resources are available.

Companies will use various forms of secret management because it protects the organization's ability to function and enables safe operations. A main responsibility of the organization is to make sure that the high-level view of the secrets management implementation, as well as how it relates to other aspects of the infrastructure is key. Without an organization level understanding, there could be multiple implementations of the same systems, as well as other forms of shadow-it emerging (Diver, 2020). Maintaining the big picture and enforcing the policies is only possible if the organization is committed to acting on violations in a serious manner (Diver, 2020).

Finally, the organization has the responsibility of assessing, negotiating, and approving federations with external entities. This can be a function of HR for managing contractor relations, as well as the establishment of business agreements. By defining the nature of interactions with third parties, including customers, they establish the vision under which the compliance can be sought, and technologies can align.

Works Cited

Alshboul, Y., & Streff, K. (2015). *Analyzing Information Security Model for Small-Medium Sized Businesses.* Retrieved from https://pdfs.semanticscholar.org/c8f1/f0626a50a64962de125847fb373c91749c98.pdf

Bitwarden. (2020). *Bitwarden for Business*. Retrieved from Bitwarden: https://bitwarden.com/#organizations

Burshteyn, M. (2018, October 6). *Secrets management guide — approaches, open source tools, commercial products, challenges and questions*. Retrieved from CryptoMove Blog: https://blog.cryptomove.com/secrets-management-guide-approaches-open-source-tools-commercial-products-challenges-db560fd0584d

Chadwick, D. W., & Inman, G. (2009, May). Attribute Aggregation in Federated Identity Management. *Computer, 42*(5), 33-40. doi:10.1109/MC.2009.143

Corum, C. (2017, February 28). *Avoid shared secrets-based approaches to authentication*. Retrieved from SecureIDNews: https://www.secureidnews.com/news-item/avoid-shared-secrets-based-approaches-to-authentication/

Diver, S. (2020). *Information Security Policy - A Development Guide for Large and Small Companeis.* Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331

Ekran System. (2019, November 26). *Secrets Management: Importance, Challenges, Best Practices*. Retrieved from Ekran System: https://www.ekransystem.com/en/blog/secrets-management

Georg, S., & Tryggestad, K. (2009, 10 01). On the emergence of roles in construction: the qualculative role of project management. *Construction Management and Economics, 27*(10), 969-981. doi:10.1080/01446190903181096

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenshcied, A. R., Burr, W. E., & Richer, J. P. (2017, June). *NIST Special Publication 800-63B.* doi:doi.org/10.6028/NIST.SP.800-63b

Indu, I., Anand, R., & Bhaskar, V. (2017, December). ncrypted token based authentication with adapted SAML technology for cloud web services. *Journal of Network and Computer Applications, 99*, 131-145. doi:10.1016/j.jnca.2017.10.001

Kent State University . (2020, April 24). *Data Management: Intellectual Property and Copyright*. Retrieved from Kent State University Libraries: https://libguides.library.kent.edu/data-management/copyright

Lopez, J., Oppliger, R., & Pernul, G. (2005, December 1). Why have public key infrastructures failed so far? *Internet Research, 15*(5), 544-556. doi:10.1108/10662240510629475

Microsoft. (2016, 10 12). *Group Managed Service Accounts Overview*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

Poticha, D., & Duncan, M. W. (2019, 03 01). Intellectual property—The Foundation of Innovation: A scientist's guide to intellectual property. *Journal of Mass Spectrometry, 54*(3), 288-300. doi:10.1002/jms.4331

Ruth, M. (2019, August 1). *Secrets Management in a Cloud Agnostic World*. Retrieved from Medium: https://medium.com/cruise/secrets-management-3a7c47fe81b

Securosis. (2018, January). *Understanding and Selecting a Secrets Management Platform.* Retrieved from Securosis Library: https://cdn.securosis.com/assets/library/reports/Securosis_Secrets_Management_JAN2018_FINAL.pdf

Stankovic, S. (2020, July 17). *13 Physical Penetration Testing Methods (That Actually Work)*. Retrieved from Purple Sec: https://purplesec.us/physical-penetration-testing

Templeton, M. (2014, April 22). *How to Deal with the Risks of Shadow IT*. Retrieved from Sandhill: https://sandhill.com/article/how-to-deal-with-the-risks-of-shadow-it/

To, N. (2019, March 8). *Secret Management - Part 1: What it is and why it's important*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/secret-management-part-1-what-why-its-important-ngoc-tu/

Whitman, M. E., & Mattord, H. J. (2019). *Management of Information Security* (6 ed.). Boston, Maryland, United States of America: Cengage Learning.