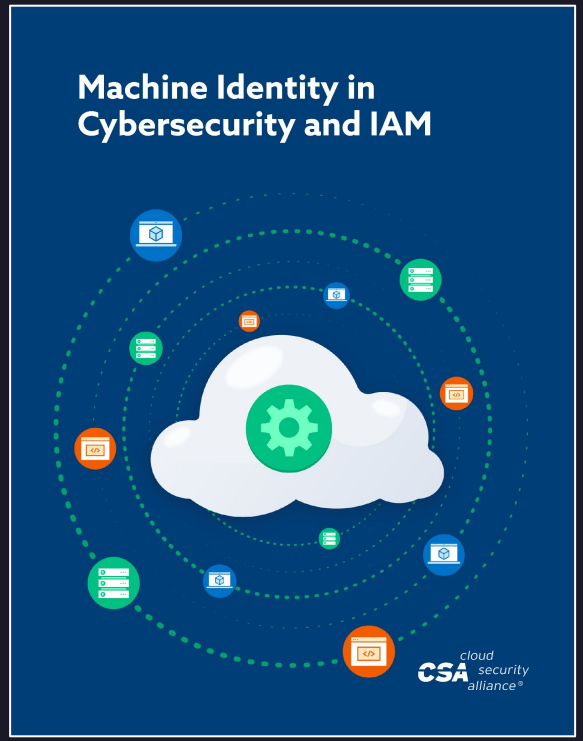
cloud security alliance®

Machine Identity in Cybersecurity and IAM



Release Date: September 20, 2023

Identity and Access Management Working Group

Agenda

1. Introduction
2. Definition of Machine Identities
3. Background History
4. Differences from Human Identities
5. Protecting Machine Identities
6. Challenges with Machine Identities
7. Best Practices
8. Conclusion

Introduction

- Identity management ensures that the right individuals, such as people or machines, have access to the right resources, at the right time, for the right length of time, and for the right reasons.

- Identity management has evolved to include not only human identities, but also machine identities, such as:
    - Devices
    - Digital Workloads
    - Robotic Process Automation (RPA) bots

- This document aims to provide an understanding of machine identities and the implications of their use.

Definitions

- An identity, in general, is a set of one or more attributes that uniquely describe a subject within a given context – a person, organization, device, hardware, network, software, workload, or service; and are distinct from the credentials used to authenticate them.
- The attributes may include a name, email address, IP address, or other identifying characteristics. Human identities are associated with individuals, whereas machine identities are associated with devices, digital workloads, and other types of entities.
- Device identities are associated with physical devices such as laptops, smartphones, servers, and operational technology (OT) devices such as Internet of Things (IoT). These identities are used to authenticate and authorize access to resources and applications on a device.
- Digital identities are associated with digital entities such as workloads, services, applications, virtual machines, containers, clouds, RPA bots, and APIs. These identities are used to authenticate and authorize access to resources and applications on an on-prem network or in the cloud, either by verifying credentials or certificates.

Definition of Machine Identities

Machine Identity:

- A machine identity is a digital identity associated with a device or machine, such as a server, a computer, or a mobile device. Machine identities are used to authenticate and authorize devices and systems that access network resources
- Digital identities that use symmetric or asymmetric cryptographic keys, tokens, or passkeys.

Asymmetric (Public Key) Encryption:

- Uses a public-private key pair.
- Public key: Used to encrypt, never a secret.
- Private key: Decrypts, kept secure in a key vault or store.
- Predominantly for machine identification: e.g., web server certificates, SSH host keys.

Symmetric Encryption:

- Not as widely used as asymmetric.
- Uses one key, not a pair.
- Typical for simplistic use cases.
- Examples: API keys, tokens, shared secrets.

Background History

Origins:

- Rooted in early computer networks.
- Securing access became vital with growing network complexity.

Early Methods:

- Unique device identities: IP or MAC addresses.
- Restricted access based on network identities.

Evolution with Technology:

- Emergence and ephemerality of workloads.
- Expansion to include digital workloads, service accounts, RPA bots, APIs, etc.

Modern Challenges:

- Proliferation of IoT and smart devices in homes and businesses.
- Explosive growth of connected devices.
- Significant increase in machine vs. human count.

Current Need:

- Strong focus on securing and managing machine identities.

Differences from Human Identities

Characteristics of Machine Identities:

- Used by entities that can't change passwords or support multi-factor authentication.
- Often possess long, non-expiring passwords.

Security Challenges & Measures:

- Many organizations rotate/change passwords regularly for security.
- Risk: Password rotation can break dependencies if the identity is embedded in applications or tools.

Solutions to Challenges:

- Cloud Environments: Use of managed identities roles.
- On-Premises: Utilize privileged access management tools (e.g., Thycotic, CyberArk) for discovery and management.

Protecting Machine Identities

The Importance of Protecting Machine Identities:

- Vital for security and integrity of organizational assets.
- Unlike humans, lack secondary verification like biometrics.

Handling Machine Identities:

- Can mimic or be allocated to any device.
- Crucial to prevent human access to private components.
- Humans should focus on policy and governance and automate verification, issuance and management.

Authentication & Potential Threats:

- Authenticated via asymmetric key pairs; clear text access to private keys by humans should not be allowed.
- Compromised identities: malicious actors can operate behind them, e.g., service account compromises in Active Directory.

Protecting by Knowing:

- Essential to discover and inventory machine identities: service accounts, managed identities, APIs, etc.

Root of Trust (RoT):

- Foundation of organizational trust.
- Private keys ideally stored in Hardware Root of Trust, though costly and complex.
- Software key stores offer flexibility and are widely used. Automate to minimize human intervention in software store management.

Challenges with Machine Identities

Discoverability and Backdoor Identities:

- Machine identities can manifest anywhere.
- Insecure coding might introduce backdoor machine identities like hard-coded credentials.
- Backdoor identities are difficult to discover compared to default identities.

Legacy Machine Identities:

- May lack documentation or use vulnerable algorithms.
- Examples: printers, CCTVs, routers.
- Risk-based approach: retiring, rotating keys, updating controls.
- Compensating controls: air-gapped networks, internal segmented networks.

Lifecycle Management:

- Provisioning, revoking, ensuring active use.
- Distinct identifier for each identity.
- Create and revoke appropriately.

Challenges with Machine Identities Continued

Perpetual Ownership:

- Machine identities owned by multiple entities over time.
- Clear process for managing ownership.
- Controls to prevent abuse: vault storage, regular rotations.

Governance:

- Essential for organizational security.
- Comprehensive lifecycle for effective management.

Centralized Management:

- Frequent mishandling across departments.
- Collaboration among diverse teams crucial.
- Centralized system enhances visibility, control, and ensures security practices.

Best Practices

Life-cycle Management:

- Formal process: provisioning, de-provisioning, key rotation.
- Define ownership, accountability.
- Relationship between identity and role.
- Implement “crypto-modularity” in application development.
- Apply principles of least privilege and JIT Access.
- Use managed identities in cloud environments.
- Reduce manual compliance; automate issuance, renewal, revocation.
- Implement a centralized system for complete visibility.
- Differentiate between devices and workloads.
- Continuous monitoring for access reviews; decommission inactive identities.
- Right-size permissions for machine identities.
- Guide development, I&O, DevOps, and security teams.
- Implement a secure key orchestration mechanism.

Best Practices Continued

Vaulting and Authentication:

- Centralize and store keys in HSMs or key vaults.
- Restrict access to privileged users with strong passwords or RBAC.
- Use identity-centric approaches with tools like gateways and encryption.

Continuous Controls and Monitoring:

- Monitor and audit continuously.
- Apply anomaly detection for unusual machine identity actions.
- Periodically detect and disable compromised identities.
- Integrate machine identity management into overall security strategy.
- Document machine identity-related outages.
- Ensure regulatory compliance.
- Enforce separation of duties; prevent toxic transactions.
- Avoid admin-level permissions for machine identities.
- Monitor privilege escalation, track malicious behaviors.

Conclusion

- Machine Identities are an essential aspect of identity management.

- Understanding the unique characteristics and risks associated with these identities, and developing best practices for managing and governing them, is crucial for maintaining the security of information and assets.

- By implementing effective identity management strategies, organizations can ensure that the right machine identities, as with individuals, have the right access to the right resources, at the right time, for the right intention, thereby minimizing the risk of unauthorized access.

Acknowledgements

Lead Authors

- Ravi Erukulla
- Alon Nachmany
- Ramesh Gupta
- Shruti Kulkarni
- Ansuman Mishra

Contributors

- Heinrich Smit
- Jonathan Flack
- David Strommer
- Venkat Raghavan
- Faye Dixon
- Paul Mezzera
- Michael Raggo
- Kapil Bareja

Reviewers

- Michael Roza
- Murali Palanisamy
- Rajat Dubey
- Shraddha Patil
- Senthilkumar Chandrasekaran
- Chandrasekaran Rajagopalan
- Iain Beveridge
- Guillaume Cesbron
- Gaurav Singh

CSA Analyst

- Ryan Gifford

Editor

- Larry Hughes