网络安全和IAM中的机器身份

CSA GCR cloud security alliance GREATER CHINA REGION ®

CSA cloud security alliance ®

IAM工作组的官网地址是：

https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management/

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《网络安全和IAM 中的机器身份（Machine Identity in Cybersecurity and IAM）》由CSA IAM工作组家编写，CSA大中华区IAM工作组专家翻译并审校。

中文版翻译专家组（排名不分先后）：

组长：

于继万

翻译组：

伏伟任　　崔鉴　　朱璐　　于振伟

审校组：

戴立伟　　谢琴

研究协调员：

蒋妤希

感谢以下单位的支持与贡献：

北京天融信网络安全技术有限公司　　华为技术有限公司

江苏易安联网络技术有限公司　　上海物盾信息科技有限公司

深圳竹云科技股份有限公司

在此感谢以上专家及单位。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予雅正！ 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

英文版本编写专家

主要作者：

Ravi Erukulla　Ramesh Gupta　Shruti Kulkarni　Ansuman Mishra　Alon Nachmany

贡献者：

Kapil Bareja　Faye Dixon　Jonathan Flack　Paul Mezzera　Michael Raggo

Venkat Raghavan　Heinrich Smit　David Strommer

审校者：

Iain Beveridge　Guillaume Cesbron　Senthilkumar Chandrasekaran　Rajat Dubey

Shraddha Patil　Murali Palanisamy　Chandrasekaran Rajagopalan　Michael Roza

Gaurav Singh

CSA分析师：

Ryan Gifford

CSA全球员工：

Claire Lehnert

编辑：

Larry Hughes

序言

随着信息技术的迅猛发展和企业数字化转型的推动，身份和访问管理（IAM）以及机器身份管理成为了组织安全战略中不可或缺的一部分。在这个数字化时代，管理和保护机器身份、控制访问权限以及确保数据和资源的安全性至关重要。

本文提供机器身份基本概念、安全保护、挑战和最佳实践。围绕机器身份，介绍机器身份的定义和历史背景，对比了机器身份与人类身份的差异，分析了组织在保护机器身份时所面临的挑战， 最后，讨论了机器身份管理的最佳实践，包括生命周期管理、身份认证和持续监控控制。

本文汇集了专业人士、企业领袖和安全专家的观点， 为您提供了全面的信息和见解，以帮助您更好地理解和应对当前和未来的身份和访问管理挑战。这些经验和措施将改变组织的机器身份安全策略和操作方式，以适应不断发展的数字化环境。

我们希望这份白皮书可以为您提供有关 IAM 和机器身份管理的全面了解，帮助您加强组织的安全性，降低风险，实现合规性，并在数字化时代取得成功。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

摘要：

身份管理是信息安全的一个重要方面，因为它能确保只有经过授权的个人和实体才能访问敏感的数据和资源。随着技术在当今组织中的应用日益广泛，身份管理已扩展到包括（但不限于）机器身份（人类以外的任何其他身份），如设备身份、数字身份和工作负载身份。本白皮书旨在定义机器身份，探讨其历史和意义，并提供机器身份管理的最佳实践，以及与其相关风险的治理。本白皮书的目标受众包括信息安全专业人士、风险办公室/责任人、IT/网络安全联络员、技术/站点可靠性工程师（SRE）DevOps 团队、业务流程责任人、应用程序开发人员以及政府和监管机构。

1.介绍

身份管理可确保正确的个体（如人或机器）在正确的时间、正确的时长和以正确的理由访问正确的资源。这对于维护组织资源的安全至关重要。随着新技术的出现，身份管理已发展到不仅包括人类身份，还包括机器身份，如设备、数字工作负载和 RPA 机器人。本文件旨在提供对机器身份及其使用影响的理解。

2.机器身份的定义

通常，身份是由一个或多个属性组成的集合，可在特定上下文环境下唯一描述一个主体，如：个人、组织、设备、硬件、网络、软件、工作负载或服务（来源：NIST SP 800-63）。

通过验证身份的凭证（如口令、密钥、证书）以区别于不同的身份

身份属性可包括姓名、电子邮件地址、IP 地址或其他识别特征。人类身份与个人相关联，而机器身份则与设备、数字工作负载和其他类型的实体相关联。

设备身份与笔记本电脑、智能手机和服务器等物理设备以及物联网等运营技术（OT）设备相关联。这些身份可用于对访问设备的资源和应用程序的行为进行验证和授权。

数字身份与工作负载、服务、应用程序、虚拟机、容器、云、RPA 机器人和 API 等数字实体相关联。通过核实这些身份凭证或证书，可以对访问内部网络或云上的资源和应用程序的行为进行验证和授权。

机器身份是数字身份，可以使用对称或非对称加密密钥、令牌或通行密钥（译者注：FIDO 联盟制定的一种旨在消除口令的技术）。

- 非对称密钥加密又称公钥加密，使用一组公私密钥对。公钥从来都不是秘密，用于锁定或加密有效载荷，而私钥用于解锁或解密密文。私钥必须保持安全，通常存储在硬件或软件的密钥库或密钥存储区中。绝大多数机器都使用类似数字证书的非对称密钥来识别自身和建立信任。例如 WEB 服务器证书、客户端证书、SSH 主机密钥和 SSH 主机证书。

- 对称密钥加密的应用没有非对称加密那样广泛。通常它只用于一些简单的场景。对称密钥加密只使用一个密钥，而不是一个密钥对。机器身份使用对称密钥的例子包括 API 密钥、令牌和共享秘密。

3.历史背景

机器身份的概念起源于早期的计算机网络。随着网络的复杂性和规模不断增大，确保资源和应用程序的访问安全变得越来越重要。确保访问安全的最早方法之一是为设备分配唯一身份，如 IP 或 MAC 地址，并根据这些网络身份限制对设备的访问。随着技术的发展，工作负载变得更加重要。而且随着时间的推移，工作负载瞬息万变，给识别工作负载带来了挑战。机器身份已扩展到包括数字工作负载、服务账户、RPA 机器人、API 等。此外，物联网和智能设备在家庭和企业中的大量使用也给机器身份增加了其他复杂因素。随着联网设备和机器的爆炸式增长，以及机器数量相对于人类的大幅增加，关注机器身份的安全和管理势在必行。

4. 与人类身份的差异

机器身份是由既不能更改口令也不支持多因素身份验证的实体来区分。通常情况下，机

器身份使用不会过期的长口令。为了确保凭证的安全，许多组织都会对口令实施定期轮换或更改的策略。但是，如果机器身份被嵌入到应用程序中或被工具使用，这就会带来问题，因为口令的轮换会破坏应用程序或工具可能具有的依赖性。在云环境中使用托管身份（Azure）/角色（AWS）是解决这些情况的一种方法。在内部环境中，解决这个问题可以使用特权访问管理工具（如 Thycotic、CyberArk），这些工具可以发现机器身份及其依赖关系。

5.保护机器身份：

保护机器身份对于维护组织的信息和资产的安全性和完整性至关重要。与人类身份不同，机器身份在软件中无法嵌入生物特征或其他形式的二次验证。

机器身份可以分配给任何设备，甚至用于模拟一个设备。因此，确保人类不能直接处理或访问这些身份的私有信息至关重要。人类应该专注于创建策略和治理方案，使用自动化方案负责这些身份的验证、发行和管理。

机器身份通常使用非对称密钥对进行认证。不论何种原因，人类都不应该以明文方式访问私钥。

机器身份可能会被恶意用户攻击，攻击者可以隐藏在被控制的机器身份后面。机器身份通常是分配的名称或完整域名（FQDN）。机器日志和事件日志将记录机器的身份名称作为执行恶意活动的行为者。一个常见的例子是，在 Active Directory 环境中服务账户启用了“交互式登录”从而导致服务账户被（攻击者）利用。任何有权访问其口令的用户都可以作为（仿冒）服务账户登录。活动日志记录服务账户的名称，而不是恶意行为者。因此，除非有足够强的业务要求，否则最好禁用服务账户上的“交互式登录”。

我们无法保护我们不知道的资产，因此发现机器身份并为他们它们创建准确的清单是保护它们的基本第一步。包括服务账户、托管身份和 API。

可信根（RoT）是组织中的信任基础。对于任何组织来说，利用安全且高度可靠的硬件和软件保护机器身份的安全至关重要。理想情况下，机器身份的私钥存储在硬件可信根中，但这会增加管理和维护身份方面的成本和复杂度。由于软件密钥库的灵活性，被广泛用于保

护私钥。每个组织都应该利用软件密钥库保护机器身份或私钥，并将整个过程完全自动化，以便消除人类访问或管理软件密钥库的可能性。

6. 机器身份的挑战

由于机器身份的特性及其管理方式，它们给组织带来了若干挑战。其中包括：

可发现性和机器身份后门：

并非所有组织都遵循一致的方法来发现和编制机器身份。与人类身份不同，机器身份可能在组织内的任何地方出现。不安全的编码可能引入机器身份后门，例如无论是有意或无意出现在应用程序/服务/脚本中的硬编码凭据。注意，此类机器身份与设备管理员账户的默认身份不同。那些（指设备管理员账户身份容易管理，但后门身份难以发现，可能需要专用工具。

遗留机器身份：

因为可能缺乏文档，使用易受攻击的密码学算法或过时的安全控制，或拥有不确定的所有权，传统（遗留）机器身份可能给组织带来重大挑战。传统（遗留）身份的例子包括但不限于打印机、闭路电视、投影仪、无线路由器等。处理传统（遗留）身份时，必须采取基于风险的方法，并应根据每个身份的风险水平考虑其优先级。这可能涉及停用未使用的身份、轮换密钥或更新安全控制。

此外，当已知的传统（遗留）身份正在使用时，组织可以采取一些补救措施，以防止凭据被窃取。

一个补救措施的例子是确保具有这种身份的设备位于独立的网络中，与处理敏感数据的网络之间进行物理隔离或逻辑分段。

另一个例子是确保这类设备位于内部分段的网络中，而不在面向公众的网络上。

机器身份的生命周期管理：

管理机器身份的一个重要方面是确保它们在整个生命周期中保持最新。这些工作包括了启用新的身份、撤销或停用旧身份、以及确保现有身份仍然活跃并正在使用。为每个机器身份分配一个明确的标识符，并记录其依赖项，将有助于实现访问配置和策略执行。

为管理机器身份的生命周期定义一个明确的流程有助于确保身份被正确创建并使用，并在不再需要时撤销或停用。

永久所有权：

管理机器身份的另一个挑战是处理永久所有权的问题。人类身份与特定个体关联，但机器身份并不一样。随着时间的推移，机器身份可能被多个个体、设备或实体拥有。例如，一个 RPA 机器人可能归负责其开发和运营的个人或组织所有，但它也可能被多个组织或团队使用。恰当的管理方式应该是能确保管理所有权和重用机器身份的过程清晰明确。

通过合适的控制措施确保这些机器身份的所有者不会有意或无意滥用他们的特权，并通过一系列有害的操作进行欺诈。这一点很重要。通常这些操作不会被注意到，并且在事后很难进行关联分析，所以最好通过事前主动控制进行预防。将凭证存放于在安全存储中并对凭证进行定期轮换等控制措施可以防止欺诈。

机器身份的治理：

确保机器身份得到有效治理对于维护组织的信息和资产安全至关重要。这包括确保身份被创建并被正确使用，并在不再需要时被撤销或停用，以及被正确的个人或实体拥有和管理。制定和实施全生命周期的身份管理策略有助于确保身份得到有效管理，并将相关风险降至最低。

机器身份的集中管理：

由于组织的各个部门对不当管理带来的影响认识不足，经常对机器身份处理不当。跨团队协作（如应用程序开发、IT、安全、IAM、DevOps、身份治理和云基础设施）是实现这些身份集中管理的关键。集中管理不仅增强了可见性和控制力，还有助于应用和执行标准化的策略和流程。这能确保安全实践的统一性，提高流程的效率和有效性，并有助于风险、审计、

管控和合规活动。此外，集中管理有还助于事件调查、漏洞识别和修补。

7.最佳实践：

对于机器身份（非人员身份）的有效管理需要技术和组织控制的结合。下面给出了管理机器身份的一些最佳实践。

生命周期管理

- 实施规范流程管理机器身份生命周期，包括对密钥和证书的配置、撤销以及轮转。
- 确立机器身份的所有权和责任，包括为每个机器身份指定负责人并确保此信息有据可查。
- 定义身份和角色授予之间的明确关系，并确保这种关系的可见性。
- 将“加密模块化设计”作为应用程序开发中的最佳设计实践，以便可以更改或重新轮转应用程序（身份），而无需重新编码整个应用程序。
- 通过实施最小特权和即时 (JIT) 访问原则，以类似于人类身份的方式对待机器身份，确保机器身份仅在有限时间内拥有必要的访问权限，从而有效限制特权和利用的范围。
- 在云环境中使用托管身份(Azure)/角色(AWS)，以降低身份泄露的可能性。这是因为凭证由云提供商管理。
- 减少跨机器身份的手工合规任务。访问请求、发布、续订和撤销的任务应由应用自动化完成。
- 实施集中式系统来管理机器身份，以提供对组织拥有的所有机器身份的完整可见性。
- 将设备的成熟度和工作负载视为不同的因素，因为改进设备的基础设施可能需

要不同于上线（应用）工具所需的方法。

- 建立持续监控（每月、每季度等），审查设备身份或应用身份的访问情况，以确定是否有任何身份不再活跃。
- 作为正常维护工作的一部分，将不再活跃的机器身份或应用身份停用。
- 通过对比已经授予的权限与正在使用的权限，识别过度授权的机器身份并调整其范围。
- 明确应当如何使用（或避免使用）技术堆栈中的工具以及在何种情况下部署它们，为开发人员、基础设施、DevOps 和安全团队提供量身定制的指导。
- 实施安全密钥编排机制，基于信任的继承，自动化的确认、验证和发布身份，从而防止人类访问机器身份。

存储和认证

- 将数字证书、SSH 密钥和密文集中并存储在安全位置，最好是在硬件安全模块 (HSM) 或密钥保管库中。此外，对这些设备的访问应仅限于具有强口令的特权用户或者应用 RBAC 访问控制机制。
- 尽可能在网关、加密或密钥管理等通用工具上采用以身份为中心的策略

持续控制与监控

- 确保持续监控和审核机器身份以发现可疑活动。
- 如果可能，使用异常检测以发现异常机器身份活动。
- 定期检测被渗透的机器身份，并将其禁用或停用。
- 将机器身份管理纳入整体安全和风险管理流程，并在无法降低风险的情况下实施补救措施。

- 识别并记录与身份相关的设备中断，并创建应急计划以防止进一步发生。
- 确保遵守相关的政府和行业法规。
- 强制执行职责分离，不仅针对机器身份，还包括身份和所有者的组合。控制机器身份的人员不应该具有进行有害的组合操作的能力，例如，一部分恶意操作以机器身份执行，另一部分则以自己的身份执行。
- 确保机器身份不拥有能够更改角色权限、创建其他用户等的管理员级交互式权限。在没有业务正当性的情况下，不应将人员权限分配给机器身份。
- 通过跟踪与已知 TTP（策略、技术和应用）相关的任务或与权限更改、横向移动（例如跨账户访问）和敏感基础架构组件（例如虚拟防火墙）相关的行为，对机器身份执行的权限升级行为进行警报和监控。

8.结论

总之，机器身份是身份管理的一个重要方面。 了解与这些身份相关的独特特征和风险，并定制管理和治理的最佳实践，对于信息和资产的安全至关重要。 通过实施有效的身份管理策略，组织可以确保正确的机器身份（就像个人身份一样）能够在正确的时间、出于正确的意图，对正确的资源拥有正确的权限，从而最大限度地降低未经授权访问的风险。 本文档为理解组织内的机器身份及其管理提供了有益的参考。

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905