From Security to Assurance in the Cloud: A Survey

论文学习笔记

author:Damon

该论文全文页数：48

全文简单概括：

论文背景：

如今，云计算的技术和应用都得到了广泛的普及。相较于传统的本地资源，云租户可以以更低的价格，更高的性能和灵活性使用云资源，且不用担心基础设施的管理。在过去纪念，研究界一直关注云范式的非功能方面，尤其是在云安全这一块。

本文的论述的方法和研究目标：

- 首先介绍云安全的最新技术，
- 并在云安全技术的一般调查总结这些方法，
- 分析它们对云安全的影响
- 针对下一代云安全和云安全保障的开发提供了一些意见

本文文章目录结构：

第一节：引出论文的研究意义

（为什么云服务怎么少人用就是最大的原因就是云安全没有得到很多人的认可）

第二节：描述了在调查的基础上的云安全分类法

主要基于（when, where, what，how）

作者希望通过分析指定了安全和保障解决方案何时、何地、什么属性以及如何加强云计算环境。

第三节：介绍了特定的云的漏洞，威胁和攻击

作者介绍了，针对用户和服务之间交互的攻击与传统分布式通信中著名的攻击类似(例如，拒绝服务-DoS、SQL注入、跨站点脚本-XSS)。但是，云环境的适当攻击也涉及由云提供商管理的接口。然后作者描述了对示例云环境的一些成功的攻击。在后面的小结中，作者采用类似的威胁建模方法，分类关于漏洞、威胁和攻击的论文。

第四节：概述了现有的安全解决方案

作者第二节讨论的安全技术分类法对云安全方法进行了分类：加密、签名、访问控制、IDS/IPS、身份验证、受信任计算。

第五节：讨论了用于安全验证、测试、和认证的保证技术

通常，在云中测试的技术可以分为两大类：测试云基础设施的解决方案和使用云资源测试任何类型的软件应用程序（包括云服务）的解决方案。

第六节：

根据提出的方法总结了调查结果，强调了我们对下一代安全和保证问题的建议，并得出了我们的结论。

最后，为了提供关于云安全和保证问题、挑战、要求和完整的解决方案，最新的调查。可以去附录查看。

作者的结论

如果我们考虑安全技术，则有34.8%的目标机密性属性（最高），而只有8%的目标可用性属性（最低）。其余的技术几乎同样针对完整性、真实性和隐私属性（在17.9%到21%之间）。如果我们考虑保证技术，它们在属性类别之间的分布更加均匀，可能是因为它们最近才应用于云环境：完整性（最高）为29.8%，隐私（最低）为15.8%。

作者的建议

对下一代云安全和保障的建议 云计算的广泛采用需要安全和保障解决方案来增加云用户对云本身和云提供商的信任。

许多研究人员针对云安全问题的不同角度提出了细粒度的安全解决方案，该解决方案可能会帮助专家用户保护他们在云中的应用程序和数据，但它们使大多数客户的云安全方案变得繁琐。

我们声称内省是云提供商检查和观察其内部流程的能力，并不是考虑云安全时唯一重要的概念。事实上，外省的概念，即赋予客户和服务提供商检查和观察影响其活动/应用程序/数据（安全性）的云内部流程的能力，也至关重要。一个适当的云安全解决方案应该包括云提供商的自省和云客户（一般租户）的自省，平衡提供商和客户之间的安全和保证控制，并在关键环境中促进云范式的全面采用。

我们声称，提高云透明度可以帮助解决安全管理问题，支持自省和自省。透明度可以通过独立于云堆栈的标准化接口来实现，这为云后端中发生的事件和活动提供了一个公共访问点。例如，可以通过收集有关给定安全机制（例如，用于授权的访问控制机制）的功能的数据来证明、监视和测试对给定安全属性的支持。

云后端数据代表了一个隐藏的宝藏，人们可以利用它构建新服务，并改进云功能、安全性和保障。