云计算安全

严春伟

2013 年 1 月 14 日

1 前言

云计算是一种以网络为载体，整合大规模可扩展的服务形式。云计算能够将包括计算、存储、数据、应用等可扩展的，分布式资源高效分配和协同工作，从而实现一种超级计算模式。

通过整合相关的资源提供更加由弹性的服务，以及集中式的，更加可靠中央服务，云计算可以说是一种相当成功的商业运行模式，在当今信息时代大行其道。但最着云计算的快速发展，云计算领域也面临着各种潜在的风险和安全隐患。

本文将会阐述云计算安全方面的一些技术。

2 云计算安全的挑战

2.1 云安全的一些事故

云计算发展的这几年，已经发生了一些事故，这里总结了 2012 年前的大的事故

- 2008 年 2 月 15 日 Amazon 出现了网络服务宕机事件，使得几千个依赖亚马逊的 EC2 云计算和 s3 云存储的网站受到影响
- 2009 年 2 月 24 日，Google Gmail 邮箱爆发全球性故障，服务中断时间长达 4h，起因其一个数据中心例行维护，使得另外一个数据中心过载
- 2009 年 3 月 7 日，Google 发生大批用户文件外泄事件
- 2009 年 3 月 15 日，Microsoft 的云计算平台 Azure 停止运行长达 22h
- 2009 年 6 月 11 日，Amazon 的 EC2 中断了几个小时，起因是雷击损坏了公司数据中心的电力设施
- 2010 年 1 月，几乎 6 万 8 千名的 Salesforce.com 用户经历了至少 1 个小时的宕机。
- 2010 年 3 月，VMware 的合作伙伴 Terremark 就发生了七小时的停机事件
- 2011 年 3 月，gmail 再次爆发大规模的用户数据泄漏事件，大约有 15 万 Gmail 用户在周日早上发现自己的所有邮件和聊天记录被删除
- 2011 年 4 月 22 日，亚马逊云数据中心服务器大面积宕机，这一事件被认为是亚马逊史上最为严重的云计算安全事件

总结这些事故，可以得到一些结论：

与传统的网络安全多针对软件漏洞不同，云计算安全事故涉及到软件和硬件两个方面。硬件方面，如停电、停机等事故，或者负荷超载等造成的宕机；软件方面，由于一些常规的软件安全方面的漏洞，造成用户的信息外泄，比如 Gmail 或者 Microsoft 的用户信息外泄

云计算框架把更多的计算资源整合成一个整体，但其中一个部分出现问题也会使整体的服务发生很大的影响。比如 Gmail 全球性的服务中断，仅因为欧洲的一个数据中心超载。

由于云计算厂商同时服务着众多的用户，云计算服务短暂的事故也影响非常广泛。2010 年 1 月著名的云计算厂商 Salesforce.com 1 个小时的宕机，影响了几乎 6 万 8 千名云计算的用户。

2.1.1 云计算五大问题

1. 虚拟化安全问题
2. 数据集中后的安全问题
3. 云平台可用性问题
4. 云平台遭受攻击问题
5. 法律问题

3 云计算安全的关键技术

3.1 数据安全

3.1.1 数据传输安全

在使用公共云时，数据加密至关重要。一般云计算服务商会对存储的数据进行加密，在数据传输的时候，采用 SSL，SSH 等安全协议保证安全访问。但是，还是有一个隐患，那就是在内存中的数据，依旧是明文，这为使得利用操作系统漏洞攻击载入内存中的数据成为可能。

3.1.2 数据隔离

采用安全独立的云区域提供虚拟机来实现数据资源的高度隔离，除此以外，云服务商与组织内部的通信采用加密的 VPN 专用通道。

3.1.3 数据残留

由于公共云中，共享资源高度重用，并被用户共享。当一个用户的数据空间被废弃，但是由于内存或者硬盘的物理特性可以被恢复数据，这就客观上残留了用户敏感数据泄露的可能。因此，云计算服务商需要保证一个用户的数据空间在回收后，必须进行彻底的擦除后再分配给其他用户使用。在应用中，相关技术已经比较成熟。

3.2 应用安全

云计算安全的实质是安全责任的转移，云计算时代之前，由单个用户自己负责服务器的安全及维护，而如今，用户将自己的服务架设在云计算框架上，将一部分安全责任转嫁到自己信任的云计算服务提供商身上。

将分散的小应用部署到“云”上，可以降低单个用户的运营维护的压力。例如：最近沸沸扬扬的 12306 订票网站（12 月 16 日和 9 日，此网站因为空调故障两度瘫痪，影响的用户应该是千万级），如果架构在 SAE（sina 云计算平台）上，那么应该就不必要有这么多宕机事件（如果出问题，那么大部分责任是 SAE 的，远不是单纯 12306 本身的问题了）。另外，如果当初开发的时候就考虑到要部署到“云”上，那么此前的沸沸扬扬的 9 亿元升级其实只需要在 SAE 那边扩容而已，而且还可以在重要时段进行暂时性的扩容，以应对春节或者国庆长假时候的压力。但是是否足够信任“云”上的运行安全，是一个考察决策者智慧和勇气的，在作者看来，如今的 12306，除非从底层进行重构，或者部署到“云”上，否则所谓的升级只能是一条不归路。

就像能量守恒定律一样，安全责任不可能消失，只能通过转移的方式得到最优的效果。

3.3 终端用户的安全

对于管理远程“云”上应用的用户，自己所用计算机就像钥匙，钥匙丢了，那就算有最坚固的防盗门也是形同虚设。用户的账户信息的安全也需要用户自己多加保密，同时，用户所用终端机器上也需要有完善的安全软件的保护。用户需要注意自己所用终端软件的安全，比如浏览器的安全漏洞问题等，定期做好打补丁以及杀毒软件的更新，从终端角度确保云安全。

3.4 应用运维的安全

应用在云平台的安全运行，当然，需要云计算服务提供端的高度配合。如 PaaS 云提供商能够为用户提供相对安全的应用运行环境，也就是云计算服务提供商承担了运行安全相关的责任，通过一定的措施如虚拟化或者沙箱，保证应用运行时不会受到云架构内部或者外部的侵犯。

但应用本身的安全责任也需要考虑。如果应用是用户自行开发，那么用户自己需要承担应用本身的安全责任，如果应用当中用到了第三方的程序，那么第三方需要承担自己程序部分的安全责任。

目前 PaaS 服务提供商为了安全，会提供自行维护安全的平台 API，比如很多安全特性被封装成了平台相关的安全对象和 Web 服务，用户的应用需要注意调用这些“云”上高效集成和安全的接口，能够更加高效地保证其运行的安全。

而 IaaS 云提供商的服务利用虚拟机来分隔应用，每个虚拟机相当于一个相对独立和部分完整功能的操作系统。把虚拟机当做为一个沙箱，IaaS 提供商的服务并不能够穿透沙箱，因此虚拟机中运行的应用对于云提供商是完全透明的，用户需要自行负责自己应用的大部分安全维护以及其他责任。

用户自己需要有一定的安全运维的实力，这一方面 IaaS 云提供商并不会有太大的协助。

3.5 虚拟化安全

基于虚拟化技术的云计算的安全主要有两方面：一是虚拟化软件的安全；另外一个是使用虚拟化技术的虚拟服务器的安全。

3.5.1 虚拟软件安全

该软件层直接部署在裸机之上，虚拟的主要是服务器。IaaS 云平台上，该软件层对于用户是透明的，管理方面完全是云提供商的义务。

由于虚拟化软件层运行在多租户的环境下，一台主机也许被多个用户多个虚拟机分享。云计算提供商会采取一定的措施，严格限制未授权的用户访问虚拟化软件层，限制对于 Hypervisor 和其

他形式的虚拟化层次的物理和逻辑访问控制。

3.5.2 虚拟服务器安全

应该选择具有 TPM 安全模块的物理服务器，TPM 安全模块可以再虚拟服务器启动时，监测用户密码，如果发现密码及用户名的 Hash 序列不对，就不会启动此虚拟服务器。尽可能使用新的带有多核的处理器，并支持虚拟技术的 CPU，这就能保证 CPU 之间的物理隔离，提高安全性。

另外，为了实现各虚拟服务器间物理隔离的目的，应该在创建虚拟服务器的时候，为每一台虚拟机分配一个独立的分区，以实现磁盘页表的分隔。每台虚拟机系统还需要安全自己独立的完整的安全防护系统，如防火墙、杀毒软件等。另外，对于虚拟机的备份也非常重要，如数据、配置需要定期备份，以提供完整的增量或差量备份方式。

3.6 物理及其他方面的安全

云计算是一种大量消耗硬件的服务方式，底层硬件的稳固以及各方面客观条件的支持对其稳定运行至关重要。

3.6.1 电力及其他设施

对于云计算系统的稳固运行，电力系统首当其冲。可以看到，亚马逊的前几次故障均与电力有关。电力的备份非常重要，因此，google 的工程师甚至为每台主机配备了单独的蓄电池。

3.6.2 人员安全

完整的商业道德以及职业操守对于在关键领域的公司员工非常重要，企业应该主动培养员工的责任意识。

同时，相关的安保措施也需要加强。在网络虚拟的安全，也需要现实中的严格安保措施去保障。

3.6.3 冗余度和扩展性

除了部分大企业会使用大型机和非常昂贵的高可用性解决方案来保证核心应用能达到 5 个 9 个的可用性, 普通企业数据中心的冗余度还是有所欠缺的, 就连非常专业的互联网企业也很难独善其生. 比如,2010 年上半年国内某大型视频网站接连出现各种待机现象. 虽然现在也经常出现小事故, 但是和一两年前相比, 无聊从影响规模还是持续时间上, 都得到了极大的改善.[?]

参考文献

[1] 吴朱华, 云计算核心技术剖析. 人民邮电出版社.2011

<++>