数据安全

第5章 数据存储安全

计算机与大数据学院 刘延华

福州大学
FUZHOU UNIVERSITY

第5章 数据存储安全

福州大学
FUZHOU UNIVERSITY

5.1 数据存储安全概述

- 存储网络行业协会(SNIA)词典则提供了数据存储安全性的定义：

存储安全：应用物理、技术和管理控制来保护存储系统和基础设施以及存储在其中的数据。存储安全专注于保护数据(及其存储基础设施)，防止未经授权的泄露、修改或破坏，同时确保授权用户的可用性。

这些控制措施可能是预防性的、侦查性的、纠正性的、威慑性的、恢复性的或补偿性的。

5.1 数据存储安全概述

- 必须使**敏感数据**不受未授权用户的影响，他们必须确保系统中的**数据是可靠的**，同时还要确保组织中需要访问数据的每个人都**可以使用这些数据**。

5.1 数据存储安全概述

□ 数据存储安全的关键驱动因素：

数据增长 - 不断增长，作为目标更有价值，更难以保护；

网络攻击增长 – 网络攻击让企业担心自己的安全状况；

数据泄露的成本 -数据泄露恢复成本非常高昂；

提高数据价值 - 大数据的价值，要求确保数据的真实性；

合规要求 - 政府制定了更强大的法律法规，合规性要求高；

需要业务连续性 -突出了灾难恢复能力的需求；

5.1 数据存储安全概述

□ 存储系统的漏洞

•**缺乏加密 -** 许多产品不包含加密功能，需要安装单独的软件或加密设备，以确保敏感数据已加密；

•**云存储 -** 云计算增加了存储环境复杂性，数据安全需要加强；

•**不完整的数据销毁 -** 不能确保从存储中删除的任何数据都被覆盖，可能会被（部分）恢复；

•**缺乏物理安全性 -** 内部人员(例如员工或清洁人员)可能访问物理存储设备，提取数据，绕过所有精心策划的基于网络的安全措施的情况。

5.1 数据存储安全概述

- 数据存储安全是数据中心安全和组织安全的一部分，这是数据安全重要的阶段，也是数据完整性、保密性和可用性三个方面都涉及的过程，所以该阶段的重要性不言而喻。***数据安全能力成熟度模型（DSMM）***
- 该过程包含**三个过程域**，分别为：存储介质安全、逻辑存储安全、数据备份和恢复。
- 数据存储安全其实就是为了保证数据在物理层面和逻辑层面的存储安全，主要的目标就是**实现数据加密、完整性和高可用**，实现数据由动态到静态的存储安全。

5.1 数据存储安全概述

- 存储介质安全

针对组织机构内需要对数据存储介质进行访问和使用的场景，提供有效的技术和管理手段，防止对介质的不当使用而可能引发的数据泄露风险。

数据存储在介质上，比如物理实体介质（磁盘、硬盘），虚拟存储介质（容器、虚拟盘）等，对介质的不当使用及其容易引发数据泄露风险，此安全域更加注重物理安全层面的数据保护。

5.1 数据存储安全概述

◘ 存储介质安全

人员能力：

负责该项工作的人员熟悉介质使用的相关合规要求，熟悉不同存储介质访问和使用的差异性，能够主动根据政策变化更新管理要求。

技术工具：

组织机构采取有效的介质净化工具对存储介质进行净化处理。

对介质访问和使用行为进行记录和审计。

5.1 数据存储安全概述

◘ 存储介质安全

重点关注的内容：

1.明确组织机构对数据存储介质进行访问和使用的场景，建立存储介质安全管理规定/规范，**明确存储介质和分类的定义**，常见存储介质为磁带、磁盘、光盘、内存等，依据数据分类分级内容确定数据存储介质的要求。

2.明确**存储介质的采购和和审批要求**，建立可信任的渠道，保证存储介质的可靠。

3.对**存储介质进行标记**，如分类（可按照类型、材质等分类）、标签（对存储介质进行打标签处理，明确存储数据的内容、归属、大小、存储期限、保密程度等）。

5.1 数据存储安全概述

◘ 存储介质安全

重点关注的内容：

4.明确介质的**存放环境管理要求**，包括存储的区域位置、防尘、防潮、防静电、防盗、分类标识、出入库登记等内容。

5.明确**存储介质的使用规范**，包括申请单、登记表等一系列访问控制要求及数据清理（永久删除、暂时删除等）和销毁报废（销毁方式、销毁记录）要求。

6.明确**存储介质测试和维修规范**，包括测试存储硬件的性能、可靠性和容量等以及如何返厂、操作人、时间和场地等内容。

7.明确**常规和随机审查要求**，定期对存储介质进行检查，以防信息丢失。

5.1 数据存储安全概述

◘ 逻辑存储安全

基于机构内部的**业务特性和数据存储安全要求**，建立针对数据逻辑存储、存储容器和架构的有效安全控制。

针对存储容器和存储架构的安全要求，比如认证鉴权、访问控制、日志管理、通信举证、文件防病毒等安全配置，以及安全配置策略，以保证数据存储安全。

5.1 数据存储安全概述

□ 逻辑存储安全

技术工具：

提供数据存储系统配置扫描工具，定期对主要数据存储系统的安全配置进行扫描，以保证符合安全基线要求。

利用技术工具监测逻辑存储系统的数据使用规范性，确保数据存储符合组织机构的相关安全策略要求。

具备对个人信息、重要数据等敏感数据的**加密存储能力**。

5.1 数据存储安全概述

□ 逻辑存储安全

人员能力：

负责该项工作的人员熟悉数据存储系统架构，并能够分析出数据存储面临的安全风险，从而能欧保证对各类存储系统的有效安全防护。

5.1 数据存储安全概述

□ 逻辑存储

重点关注的内容：

有专人专岗统一负责逻辑存储安全管理，同时要熟悉了解逻辑存储安全架构和相关运维工作。建立数据逻辑存储安全管理规范，包含认证授权、账号和权限管理、日志管理、加密存储管理、版本升级、上线前统一安全配置、数据隔离等方面的要求。提供相关工具进行配置扫描和漏洞扫描、监测数据使用规范性，对重要数据进行加密的工具或技术。

5.1 数据存储安全概述

□ 数据备份和恢复

通过执行定期的数据备份和恢复，实现对存储数据的冗余管理，**保护数据的可用性**。

备份和恢复是为了提高信息系统的高可用行和灾难可恢复性，在数据库系统崩溃的时候，没有数据库备份就没法找到数据，保证数据可用性是数据安全的基础。

5.1 数据存储安全概述

□ 数据备份和恢复

重点关注的内容：

专人专岗负责数据备份与恢复，同时具备了解数据备份操作业务流程和满足相关合规性要求的能力。制定数据备份与恢复的安全管理制度和操作规范，包含备份范围、频率、工具、过程、日志记录、保存时长、恢复测试流程、访问权限设定、有效期保护、异地容灾等各项内容。提供数据备份和恢复的自动化工具和数据加密、完整性校验的工具及技术手段。

5.1 数据存储安全概述

□ 数据安全最佳实践

1.数据存储安全策略 - 企业应该制定书面策略，为其拥有的不同类型的数据指定适当的安全级别。显然，公共数据所需要的安全性远远低于限制或机密数据，组织需要有适当的安全模型、过程和工具来实施适当的保护措施。这些策略还包括应该在组织的存储设备上部署的安全措施的详细信息。

2.访问控制 - 基于角色的访问控制是安全数据存储系统的必备条件，在某些情况下，多因素认证可能是合适的。管理员还应确保更改其存储设备上的任何默认密码，并强制用户使用强密码。

3.加密 - 数据在传输过程中以及在存储系统中静止时都应该加密。存储管理员还需要有一个安全的密钥管理系统来跟踪他们的加密密钥。

5.1 数据存储安全概述

□ 数据安全最佳实践

4.数据丢失预防 - 许多专家认为仅靠加密不足以提供全面的数据安全。他们建议组织还部署数据丢失防护(DLP)解决方案，以帮助查找和阻止正在进行的任何攻击。

5.强大的网络安全性 - 存储系统并不存在于真空中，它们应该被强大的网络安全系统所包围，例如防火墙、反恶意软件防护、安全网关、入侵检测系统，以及可能的高级分析和基于机器学习的安全解决方案。这些措施应该可以防止大多数网络攻击者获得对存储设备的访问权限。

6.强大的端点安全性 - 同样，组织也需要确保他们在个人电脑、智能手机和其他访问存储数据的设备上拥有适当的安全措施。这些端点(尤其是移动设备)可能会成为组织网络攻击的薄弱环节。

5.1 数据存储安全概述

□ 数据安全最佳实践

7.冗余性 -包括RAID技术在内的冗余存储不仅有助于提高可用性和性能，在某些情况下还可以帮助组织缓解安全事件。

8.备份和恢复 - 一些成功的恶意软件或勒索软件攻击如此完全地破坏企业网络，唯一的恢复方法是从备份恢复。存储管理人员需要确保他们的备份系统和流程适合这些类型的事件以及灾难恢复的目的。另外，他们需要确保备份系统与主系统具有相同的数据安全级别。

5.1 数据存储安全

目前，大数据主要是分布式地存储在大数据平台（Hadoop）中，采用云存储技术，以多副本、多节点、分布式的形式存储各类数据。数据的集中存储和滥用增加了被非法入侵和数据被泄露的风险。因此，如何保障大数据存储安全一直是重点研究的问题。

5.2 数据(库)加密

- 数据加密

数据加密是保障大数据存储安全的主流方法之一。

可以使用的国家商用密码局制定的应用标准包括SSF33、SM1、SM2、SM3、SM4、SM7、SM9等加密标准。

使用的技术包括**基于属性的加密**、**同态加密**等。

对于海量数据来说，加解密操作不可避免会带来无法忽略的**额外开销**，这限制了数据加密技术在数据存储安全中的应用范围。

5.2 数据(库)加密

□ 数据库加密的粒度

数据库加密的粒度可以有4种，即表、属性、记录和数据元素。

加密粒度越小，则灵活性越好且安全性越高，但实现技术也更为复杂，对系统的运行效率影响也越大。

5.2 数据(库)加密

□ 数据库加密的粒度

（1）表加密

表级加密的对象是整个表，类似于操作系统中文件加密的方法。这种方式最为简单，但因为对表中任何记录或数据项的访问都需要将其所在表的所有数据快速解密，因而执行效率很低，浪费了大量的系统资源。在目前的实际应用中，这种方法基本已被放弃。

5.2 数据(库)加密

- 数据库加密的粒度

（2）属性加密

属性加密又称为“域加密”或“字段加密”，即以表中的列为单位进行加密。

如果只有少数属性需要加密，属性加密是可选的方法。密钥管理的复杂度增加，同时系统效率也受到影响。

5.2 数据(库)加密

- 数据库加密的粒度

（3）记录加密

记录加密是把表中的一条记录作为加密的单位，当数据库中需要加密的记录数比较少时，采用这种方法是比较好的。

（4）数据元素加密

数据元素加密是以记录中每个字段的值为单位进行加密，数据元素是数据库中最小的加密粒度。

采用这种加密粒度，系统的安全性与灵活性最高，同时实现技术也最为复杂。

5.2 数据(库)加密

- 数据加密方式

（1）库内加密

库内加密在DBMS内核层实现加密，其优点是加密功能强，加密功能与DBMS之间无缝耦合。对于用户和数据库应用来说，库内加密方式是完全透明的。但这种方式对系统性能影响比较大，DBMS要进行加、解密运算，加重了数据库服务器的负载。密钥管理也存在一定问题。

5.2 数据(库)加密

- 数据加密方式

（2）库外加密

库外加密指在DBMS之外进行加密，加解密过程大多在客户端实现，或由专门加密服务器或硬件完成。

库外加密减少了数据库服务器负担；可以分开存储密钥与加密数据，安全性更高；更适合实现端到端的网上密文传输。

但库外加密可能导致加密后的数据无法正常索引、检索等，会给数据库管理系统和数据应用带来影响。

5.2 数据(库)加密

◘ 磁盘存储安全

数据平台或数据中心存储数据集中，其安全性异常重要。

针对传统磁盘存储数据的安全性一直是研究热点，主要工作集中在防磁盘数据篡改、防数据泄露失窃等方面，还包括自存储安全解决方案、网络安全硬盘、安全云盘以及分布式存储系统安全等研究工作。

5.2 数据(库)加密

◘ 磁盘存储安全

固态硬盘因其延迟低、吞吐量大、能耗低等优点，正逐渐替代传统机械硬盘。新出现的可信固态硬盘技术依靠提供安全存储接口和协议，保证数据的机密性，并细粒度控制用户访问存储的数据，使得数据存储是可以信任的，从而保护了数据的存储安全以及机密性。

因此，对于数据密集型应用的数据存储安全需求而言，**可信固态硬盘**有望成为保障大数据平台存储安全的新基础。

5.3 数据数据备份与恢复

- 安全的数据库系统必须能在发生故障后利用已有的数据备份，恢复数据库到原来的状态，并保持数据的完整性和一致性。
- 数据库系统所采用的备份与恢复技术，对系统的安全性与可靠性起着重要作用。
- 备份是必需的数据库日常维护工作，是数据库恢复的前提；恢复则是数据库安全的最后一道屏障。

5.3 数据数据备份与恢复

- **数据库备份技术**

常用的数据库备份的方法有如下3种。

（1）冷备份

冷备份是在没有终端用户访问数据库的情况下关闭数据库并将其备份，又称为“脱机备份”。这种方法在保持数据完整性方面显然最有保障，但是对于那些必须保持每天24小时、每周7天全天候运行的数据库服务器来说，较长时间地关闭数据库进行备份是不现实的。

5.3 数据数据备份与恢复

□ 数据库备份技术

（2）热备份

热备份是指当数据库正在运行时进行的备份，又称为“联机备份”。在数据备份期间发生的数据更新不能被及时执行，有可能使备份的数据不能保持数据完整性。采用数据库运行时日志可以解决上述数据不一致问题。热备份还对系统运行效率产生负面影响。

5.3 数据数据备份与恢复

□ 数据库备份技术

（3）逻辑备份

逻辑备份是保存原数据库中数据内容的一个映像，而不是直接备份数据内容。

逻辑备份一般用于增量备份，即备份那些在上次备份以后改变的数据，对数据库系统效率影响较小。

5.3 数据数据备份与恢复

◘ 数据库恢复技术

数据库恢复技术一般有3种：

（1）基于备份的恢复

基于备份的恢复是指周期性地备份数据库。当数据库失效时，可取最近一次的数据库备份来恢复数据库，即把备份的数据拷贝到原数据库所在的位置上。

备份的周期越长，丢失的更新数据越多。

5.3 数据数据备份与恢复

◘ 数据库恢复技术

（2）基于运行时日志的恢复

运行时日志文件是用来记录对数据库每一次更新的文件。对日志的操作优先于对数据库的操作，以确保记录数据库的更改。

这种恢复回复机制类似于热备份机制，当系统突然失效而导致事务中断时，可重新装入数据库副本，把数据库恢复到上一次备份时的状态。

然后根据日志文件，可把数据库恢复到故障前某一时刻的数据一致性状态。

5.3 数据数据备份与恢复

- 数据库恢复技术

（3）基于镜像数据库的恢复

数据库镜像就是在另一个磁盘上复制数据库作为实时副本。

这种恢复方式能够最大限度恢复到故障前的状态。

但实时的数据库镜像将大大影响数据库系统的效率。

5.4 数据安全销毁

- 大数据的安全销毁或删除是近年大数据安全的一个重要研究热点。如果其存储在云端或云平台的数据删除不彻底，极有可能使其敏感数据被违规恢复，导致用户数据或隐私信息面临泄露的风险。
- 传统的数据物理删除的方法是采用物理介质全覆盖的方法，然而针对云计算环境下的数据删除问题，这一手段并不可信。在云环境下，用户失去了对数据的物理存储介质的控制权，无法保证数据存储的副本同时也被删除，导致传统删除方法无法满足大数据安全的要求。
- 因此，如何保证被删除的数据确实被删除，即保证数据可信删除，是一个重要挑战。

5.4 数据安全销毁

- 一种支持两种类型的**数据可信删除**方法，该方法基于文件的创建时间，使过期文件无法被恢复访问，并支持按需删除个别文件，从而确保了文件被安全删除的可信性。
- 一个针对密文数据可信删除的方法，设计了一个验证的“**消失原型**”，能够确保在用户指定的时间期限之后，所有特定数据副本都变得不可读，而不需要对用户进行任何特定的操作，即使攻击者同时获得了该数据的缓存副本和用户的密码和密钥。
- 提出了**基于数据加密标准的数据安全删除策略**，使被删除的文件无法被任何人恢复，即使是云存储平台的管理人员。

5.4 数据安全销毁

- **基于图论和密码学技术**，提出了基于无环图删除策略的安全删除数据存储系统模型，该策略通过删除属性和保护类来说明数据销毁，当删除指定的数据属性时，同时也必须相应地删除该属性链接的保护类，从而最终达到数据安全删除的目标。
- 一种带有时间指定属性的**安全数据自毁**方案，只有在允许的时间间隔内且与密文关联的属性满足密钥的访问结构时，才可以读取数据。在用户指定的过期时间之后，敏感数据将被安全地自毁。

5.4 数据安全销毁

- 在云计算环境下，个人数据被第三方（云数据存储平台）缓存、复制和存档，而这些数据往往没有真正被用户控制，在网络和云存储系统中，正确删除数据并清除所有痕迹的操作通常是无法预见的，因此，数据的可信删除技术仍然是未来数据安全技术研究的热点。

谢谢大家，一起交流学习！

QQ：10068 0 2383