数据加密技术在计算机安全中的应用

华中师范大学伍伦贡联合研究院　沈维洋
北京字节跳动科技有限公司　沈维海

【摘要】21世纪是一个信息化的世纪，伴随着经济与科技创新大力发展的脚步，社会所囊括的信息量与日俱增，信息量的增多正面临着诸多安全问题的挑战，各个公司乃至个人在计算机中所存储的重要数据亟待保护。文章阐述了几种主流的数据加密算法，并给出了相关数据加密技术在计算机安全中的具体应用，旨在有相关需求的用户营造安全的计算机使用环境。
【关键词】数据加密；计算机安全；应用

DOI:10.19353/j.cnki.dzsj.2017.09.082

一、计算机安全面临的威胁

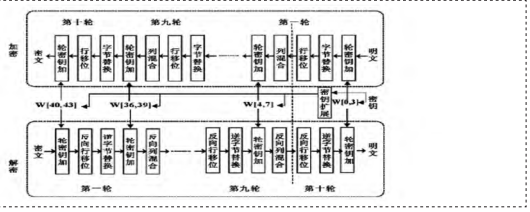
计算机更新换代速度较快，在不断的演变的进化过程中，针对计算机网络通信也随之提出了更高的要求，在计算机快速发展的同时，层出不穷的网络安全事件持续发酵，严重威胁社会各界计算机网络的使用安全。整体来讲，计算机网络信息安全可细分为以下两个方面：第一、用户的计算机信息存储安全；第二、网络中各节点之间的通信安全。

关于威胁计算机安全的诸多因素中，人为因素所占的比例要明显大于非人为因素，人为因素又可以具体细分为主被动攻击两种。在这两种攻击中给计算机数据保密性造成主要威胁的是被动攻击，所采用的手段大体有六种：第一、针对计算机通信线路中所传递信息进行窃取以及监听；第二、对所获取的信息实施分析整理；第三、假冒计算机用户身份；第四、对计算机网络中所传递的信息实施篡改；第五、已发信息不予确认；第六、其他的一些相关手段。

二、新型数据加密技术概述及算法

为了让使用计算机的所有用户，个人的一切信息都能够得到安全的保障，离不开对计算机数据加密技术的良好掌握。文中所说的新型数据加密技术主要包含以下四个部分：密文、明文、密钥以及加密算法。这几部分共同构成了的模型结构图如下：数据加密所涉及的方式方法与技术有很多，以往传统的加密方式，根据在加密处理过程中所使用的密钥，自身所具有的特征区分为对称秘钥以及非对称密钥解码技术两种。对称密钥解码技术又可以继续细分为序列密与和分组密码两种。

下面文章会主要以最新型的加密算法 AES加密算法为例，对其所用的加密算法以及步骤进行阐述。



1.AES 算法结构

AES 算法所应用的是128 位、192 位、256 位，加解密是依靠128 字节实现的。过往传统的密钥这两者应用的都是相同的数据，所得到的回馈数据与输入数据也是一样的。下面使用循环的代码结构进行迭代加密，并在循环中重复替换和置换输入的数据。以下图表就是 AES算法的加密与解密的具体实现。表中的加密算法所应用的就是 128 字节的分组，在此过程中还把方阵复制到了状态数组，AES 算法的加密过程每实现一步，状态数组就会随之做出相应的改变，待到全部结束，生成的状态数组会被复制为输出矩阵。

2.AES 算法步骤

AES 算法的步骤可主要划分为以下四步：

①字节替换。字节替换是AES 算法的第一步，也是最为关键的一步，利用S-盒将所有的分组通通实施字节替换，用盒中的四个高位表示行值，对应的四个低位表示列值，其他的数值元素为对应的输出值。字节替换主要表达的是 AES 加密算法的非线性特征，可以有效避免简单的代数攻击。

②行移位。在此步骤过程中所用到的列表，每一行均按照某个偏移量向左循环移位。比如 S-盒中的首行固定，则第二行可以按照一个字节的偏移量做循环移位。那么在完成全部的循环移位后，分组的每一列表内的各个列，都是由不同列中所含有的元素结合而成的。每次移位，其线性距离均为四字节的整倍数。

③列混合。在完成上述的线性变换后的分组列表，将按列分别进行相对独立的操作。这个操作过程是将，单列的四个元素作为系数，合并为有限域的某一多项式，并用这个多项式与固定多项式做乘运算。该过程也即可认为是在有限域条件下的矩阵加、乘运算。在经过几轮的行移位变换和列混合变换后，分组列表中的所有输入位均与输出位相关。

④轮密钥加。在整个实现过程中，第二步与第三步的程序每执行一次，主密钥就会自动的生成一个对应的密钥组，所产生的密钥组和原字节分组列表相同。

三、计算机安全加密技术的应用

AES加密算法的具体应用以及应用哪种形式，取决于所应用此项技术的行业具体要求，例如我们日常手机所连接的无线网络，其工作原理就是借助将AES嵌入到计算机安全机制中，与此同时，众多的为网络数据传输，提供安全保障的相关技术也是基于AES算法；当下最流行的电子商务交易平台中也随处可见AES加密算法的身影，AES凭借高安全性确保在SSL协议中，能够安全稳定的进行交易中用户各项重要信息的传递；我们日常所用到的大多数硬件，如：公交卡、门禁卡以及所使用的身份证，都应用了AES加密算法嵌在芯片里。从而保障了在使用过程中的安全性。

数据加密的工作原理是，按照预先设定的密码把较容易识别的明文密码，转换成难以识别的数据形式，使用几种不同的加密密钥，以一致的加密算法来实施加密，进而呈现出不同的密文形式来达到保护重要数据的目的。在目前的各种网络电子交易过程中，与电商相连的银行机构几乎所有都是，使用数据加密技术来与所应用的交换设备实施联动，把所涉及的多样化的数据流传输至网络安全设备当中去，系统通过对这些数据的读取来实现安全环境的分析，应用相应的措施来应对已被发现的网络安全隐患。

当下数据加密最主要的实现形式是密钥，这是因为与其他的形式相比，密钥具有较为理想的安全性，密钥形式又可以细分为私人和公用两种。密钥形式的使用十分广泛，尤其是在当下电子商务的交易当中，在我们使用信用卡进行消费时，收费方拥有的是公用密钥，这是为了方便读取消费者的消费信息，在消费的过程中借助个人密钥进行数据加密。进而确保消费者个人的信息安全，同时一定程度的限制了信用卡权限。

数据加密的另一种常用表现形式就是数字签名认证。这种技术依托于加密技术，重要的工作原理是依靠加密解密来提供所需要的安全保障，这项技术和上一种一样也是分为公私两种，通常而言，数字签名技术在税务安全部门的应用相对较多。

四、结束语

综上所述，文章主要就数字加密技术在计算机安全中的应用进行论述，先后主要阐述了当下计算机安全所面临的威胁，进而提出新型的AES加密算法，并给出了相应的算法结构与算法步骤，最后详细的讲解了计算机安全加密技术的具体应用。希望通过全篇的叙述，来为相关的计算机加密技术的研究提供借鉴。

参考文献

[1]王秀翠.数据加密技术在计算机网络通信安全中的应用[J].软件导刊,2011(3).

[2]张金辉,郭晓彪,符鑫.AES 加密算法分析及其在信息安全中的应用[J].信息网络安全,2011(5).

[3]邵雪.数据加密技术在计算机网络安全领域的应用探讨[J].中国市场,2011(45)

[4]孔婵.计算机网络安全中数据加密技术应用探讨[J].科技致富向导,2011(18).