计算机网络信息安全中数据加密技术的研究

李剑
（贵阳职业技术学院　贵州　贵阳　550081）

[摘　要]随着计算机网络应用技术越来越发达并渗透到人们工作生活的各个方面，人们越来越倾向于通过网络系统传输各种信息和数据，但计算机的信息安全依旧存在漏洞。如果在这个过程中出现信息损坏、泄漏等问题，会对用户造成极大的损失，影响用户体验。所以，如何有效地保证计算机信息的安全是技术领域的一个重要挑战。信息加密技术可以减少数据泄漏，从而减少危害，保证数据的安全，有一个好的储存环境，保证用户在便利使用网络的同时，免受数据泄漏的危害。

[关键词]计算机；网络信息；数据加密；技术研究
【DOI】10.12252/j.issn.2096-6288.2021.07.057

引言

现代世纪时科技高速发展的世纪，越来越多的高科技取代劳动力，其中计算机技术发挥很大的作用，而计算机使用中也存在风险，对人们的工作和生活造成了很大的影响。数据加密在信息时代发展，尤其是受到企业方面的特别关注，从加密技术研发出来至今，加密技术不断的更新迭代，不断升级，这些不断出现的新加密方式都证明：技术正在不断完善和优化用户体验。

一、加密技术的概念和根本原理

密码学是数据加密技术中重要的一部分，有很长的使用史，加密主要的步骤就是把文件数据通过密钥、加密算法转变成密文，解密主要是：通过密钥、算法把密文变成文件数据[1]。加密算法是总所周知的，但是密钥则仅使用者知道，对外保密，只有网络运转时数据传输才能进行，数据传输也是网络运转的主要目的。所以保护网络，从某种意义上来讲，就是保护数据安全。任何的文件储存几乎都可以使用到：文件系统加密技术，但对于一些文件，不能使用透明数据加密。比如：大数据数据库系统、数据库系统，也能够使用文件加密技术。但是，文件加密技术没有针对性，无法为用户额外添加权限控制，对于一些必须严密加密的数据库不适用。如今，大部分数据加密使用者都更喜欢透明加密技术，对于一些简单的应用不需要升级等步骤，对于数据的保护也能起到保障，阻止黑客的攻击，绕开防护系统窃取数据，阻止使用者对数据的滥用，极大程度上阻碍了非法窃入，读取数据，保证在文件储存的过程中的安全性。信息技术很容易受到外界攻击，没有抵抗能力。其中信息系统主要分为：信息资源、硬件资源、通信资源、软件等等，其中有很多原因是可预料的，不可预料的都会造成数据被更改、破坏、功能失效、泄漏等，这时系统无法处于正常运转状态，还有系统崩盘、瘫痪的风险。数据加密可以中三个层面解说：网络与通信协议、软件组件、硬件组件。

二、计算机网络产生危害的因素

（一）计算机网络操作系统中的安全隐患

运转时的计算机，最重要的系统是操作系统，使用计算机时，通过操作系统来对计算机程序进行分工，计算机运转。一旦，使用者无法操作系统，计算机的工作将出现问题，当计算机无法正常运转时，不法分子就有了可趁之机，通过找出计算机的问题，入侵计算机，进而控制电脑，窃取使用者的信息。用户使用电脑时，利用操作系统进而改变电脑的硬件设备。一般情况下，系统都带有软件、应用程序，应用程序在运行时，一旦出现错误，系统就会出现漏洞。计算机系统发生错误，或者软件携带病毒无论是在计算机的系统出现问题，还是软件，硬件或者是协议问题，这些计算机的缺陷，不足一旦被查出，无论是否授权，外人就可以自如的破坏系统，从而危害计算机的系统。主要威胁：破坏计算机数据的完整性，泄漏数据，使数据不可用，拒绝服务，未授权访问[3]。信息泄漏表现在数据上，数据的泄漏、透露或者丢失，信息泄漏的主要过程为，在传输过程中，通过信息数据等分析，推导出数据。完整性破坏：通过某些技术手段，掌握数据的管理权，自身对数据进行修改、创建、重放、删除等，让信息的完整性消失。拒绝服务：让信息的价值降低，或者减少信息的实用性。使用的手段：攻击数据系统，使用非法手段、没有访问成功可能性的大量尝试，大量的信息涌入，造成系统无法负荷，从而降低服务能力，或者直接破坏服务能力。信息系统受到破坏，或者组件受到破坏，物理方面的、逻辑方面的都会中断服务。未授权访问：没有得到授权的用户通过一些非法手段，获取访问资源的权限，或者查看超出自己权限的信息。

（二）计算机网络中的不良因素

计算机网络具有开放性、公平性的特点，用户可以查看信息，也能随意传播信息，所以网络中的危害很多，用户在使用时，就有危险因素，黑客可以使用自己设计的程序，攻击计算机系统，主要是通过数据在传输线上传播。此外，计算机协议，也有一定的安全隐患，一旦，协议本身产生问题，或者协议被攻击，攻击者就可以查看数据信息。黑客掌握软件、硬件等知识，黑客可以独立的攻击电脑。黑客有很多攻击手段，非法获取口令，置入木马、病毒，攻击电脑系统，使用邮件，web欺骗技术，通过一个漏洞来攻击系统，寻找漏洞，然后信息监听，最终窃取特权。计算机数据的安全性，包括网络的安全、使用者的身份确认、访问或控制网络资源、数据传输过程中也有风险，保密性、完整性都有可能被破坏，如：路由系统是否安全，远程接入是否安全，域名是否安全，黑客入侵，

网络中的病毒等。应用层的安全：这个有关的安全问题分为数据安全性、应用软件等包括DNS、Web服务等。除此，数据信息还有被病毒植入的风险。冒充：没有得到授权伪装成其他的实体，以此得到进行访问，或者获得不属于自己的权力。攻击者会进行很多的假冒、伪装成管理者，查阅密件，发布命令，欺骗使用者，假冒成管理者获取权限，后者套取权限，密钥，口令等，使用管理者的权利使用数据资源，网络设备，通过用户来欺骗系统，占用数据资源。旁路控制：攻击者会在系统中，找到进入数据的其他路线，得到权限，攻击者还善于寻找计算机数据系统的不足，缺陷，加以利用，躲开系统检测，进入系统。破坏信息的完整性，攻击者可以从很多的方面来完成操作，一般分为3种：管理者违规操作、越权操作、不当操作，可能损坏计算机系统，造成安全事故[4]。

三、在计算机网络信息安全数据加密技术的使用措施

数据加密有很多方式：专用加密，链路加密，节点加密。安全管理分为：设备管理、安全技术、安全制度等，管理制度的完善与否和网络的安全性有很大的关系，建立完善的制度，进行合理的职责划分，合理分配角色。密钥安全保密技术，主要的方式，管理工作中，基本使用数学、物理方式，对信息的储存、处理、信息传输等进行加密，尽量的让信息减少泄漏，较小被截获的可能。密钥引起了各界的高度关注，储存密钥有很多的方式，体现在很多方面。所以，要充分的重视密钥的储存、保管、更新。使用者根据自身需要储存密钥，具体的模式：就是两者有相同的密钥，进行加密或者解密，网络数据中密钥具有一致性，保证网络的安全，在一定程度上是加大了密钥的安全性。非对称密钥则可推出，数据密钥不尽相同，存在差异，使用的密钥具有唯一性，分为：公钥、私钥，解密不能推出密钥，非对称密钥的特点就是：具有稳定性、安全性。最近一段时间，很多计算机使用者会收到假冒数据，会有网络使用者被攻击电脑系统的人冒充，接收文件，或者发出文件，并修改信息。这对网络安全性造成了威胁，会导致网络的规则破坏，签名技术的运用，就可以解决这种问题，做好保密工作，提高安全性。从技术方面讲，主要就是标记数据源头，在处理工作，或者传递数据时，进行标记。

（一）在电子商务方面的运用

计算机的高速发展，通信技术也更加的成熟，在电商平台发挥了很大的作用，借助网络平台，电商有了更大的平台，更大的发展机会，也增加了很多的收益。电商在网络平台投入了很多的资金。因此，数据对于电商来讲尤为重要，计算机网络信息安全数据加密技术保护数据，比如：在某个平台购买东西，需要输入密码，来进行交易，很多的软件也需要验证登陆，就是为了用户的数据安全，建立安全制度，保护数据，强化安全，以此来避免麻烦。

（二）在计算机软件方面的运用

计算机的发展过程中，病毒、黑客也在不断的升级，计算机系统较为脆弱，容易受到伤害，必须不断的升级计算机的系统，并且，用户在使用计算机时也需要加密，保证数据的安全性，没有正确的密码，软件不会继续运行，保证使用者的安全。病毒一般很难查杀，很多防御软件可以有效的查到病毒的位置，即使查杀，防止计算机损坏。用户在使用软件时，如果检测到病毒，要及时的处理，或者交到专业人士手中，进行查杀修复，病毒在电脑中长期潜伏，会损坏电脑数据。

（三）在局域网方面的运用

如今，社会进入了计算机时代，局域网被很多的企业、公司组建，用来储存信息，不断的强化数据安全。在数据传输时，运用数据加密技术，在传输过程中，打包数据，储存在路由器中，路由器自身具有加密能力，把数据放在加密路由器中传播，在传输中自动解密，保证错误不会发生，直到数据被接收。对于多区域的网络，要需要加强安全性，就目前的技术来分析，加强不同局域网安全性，主要使用：在线加密技术，由于信息传递的途径、传输的范围不尽相同，所以密钥也会有比较达到差异，这就增加了非法用户破解的难度，给计算机数据带来了更多的安全。软件开发者会开发不同的软件，各种软件对于病毒的敏感度不同，数据容易受到攻击，管理者要及时的改进密钥，尽最大可能的防止病毒的入侵。

四、结束语

时代的快速发展离不开计算机技术的支撑，计算机行业成为新世纪人类工作中必不可少的工具。在使用计算机时，人们一定会格外的关注网络安全，网络安全具有通信面广、时效性强、通信方便、通信面广等特点，帮助人们提高工作效率。但是使用计算机也有风险，其中有黑客、病毒与漏洞的存在，这直接威胁到网络安全，所以要尽快的升级数据加密系统。

参考文献

[1]朱凯.计算机网络安全中数据加密技术的应用对策[].网络安全技术与应用，2019（12）：36.

[2]林金娜.数据加密技术在计算机网络安全中的应用探析].网络安全技术与应用，2019（12）：38—40.

[3]韦焯思.数据加密技术在计算机网络安全中的应用价值研究[J].计算机产品与流通，2019（11）：31，98.

[4]侯彦军.浅析数据加密技术在计算机网络信息安全中的应用[J]中国新通信，2019，21（21）：134.

作者简介:

李剑，1979年，性别，女，民族，汉，籍贯，陕西西安，职务，职称，计算机讲师，学位/学历，工学硕士，研究方向，计算机网络。