文章编号：2095-2163(2019)04-0292-03 中图分类号：TP393.08 文献标志码：A

计算机网络信息安全中的数据加密技术

孔德武
(河南工业和信息化职业学院，河南 焦作 454000)

摘 要：网络信息安全直接影响着信息技术的应用与推广，也可能带来商业或经济方面的损失。基于此，本文以当前计算机网络信息安全面临的威胁作为切入点，予以简述，包括信道安全威胁、节点安全威胁、计算机安全威胁等。在此基础上重点分析可行的数据加密技术，针对实际问题给出通信过程加密、节点加密、综合加密防御机制等内容。最后依据仿真实验论证其可行性，实验以参数模拟法在计算机环境下开展，通过模拟不同的威胁形式为后续工作提供参考。

关键词：计算机；网络信息安全；数据加密技术；节点安全

Data encryption technology in computer network information security

KONG Dewu
(Henan College of Industry & Information Technology, Jiaozuo Henan 454000, China)

【Abstract】 Network information security affects the application and promotion of information technology, and may also cause commercial or economic losses. Based on this, this paper takes the threats of current computer network information security as an entry point, and make a systematic research on channel security threats, node security threats and computer security threats. After that, the paper analyzes the feasible data encryption technology, and gives the communication process encryption, node encryption, and comprehensive encryption defense mechanism for practical problems. Finally, the feasibility of the simulation experiment is demonstrated. The experiment is carried out in the computer environment by the parameter simulation method, which provides reference for the follow-up work by simulating different threat forms.

【Key words】 computer; network information security; data encryption technology; node security

0 引 言

数据加密技术是指将数字化信息经过加密钥匙及加密函数进行转换，变成无意义的密文，接收方将此密文经过解密函数、解密钥匙还原成初始信息。该过程中应用的加密钥匙/函数和解密钥匙/函数的匹配具有唯一性，可有效保证信息安全。现代社会计算机得到广泛应用，这也使得网络信息安全、数据加密技术得到了更多关注、重视，就其安全威胁和可行应对方式进行分析具有突出的现实意义。

1 网络信息安全面临的威胁

1.1 信道安全威胁

来自信道的安全威胁，主要是指网络信息传输过程中被破坏、截取，从而导致数据丢失的情况，包括点对点的信息传输(一般为有线式)、点对面的模拟传输(一般为无线式)2 大类。如在现代远距离光纤通信作业中，下载获取的信息呈现为乱码，不能转化和读取。该问题多与通信有关，通信过程中，信息有可能遭遇频率相近信道内其它信号的干扰或木马攻击。而且木马攻击带有一定的随机性，难以在通信行为发生前预知危险，导致信息安全相关问题难以避免。

1.2 节点安全威胁

计算机网络信息安全牵涉到 2 个关键主体，即通信节点、信息存储节点。如人员甲利用计算机获取与网络资源共享池的连接，此时该计算机既属于一个通信节点，也属于一个信息存储节点。如果计算机内存在潜伏的木马、恶意程序，可能通过网络连接侵入互联网，并向其它节点(计算机终端)蔓延，带来计算机网络信息安全问题；如果网络资源共享池(某一个或几个，要求计算机与此取得连接或进行通信)存在恶意程序、病毒，也可能侵入到人员甲的计算机中，使该节点的网络信息面临安全威胁。

1.3 计算机安全威胁

计算机本身不存在网络意义上的安全威胁，但计算机的作用一般需要在互联网的支持下得到发挥，这使其内部存储的网络信息、数据面临来自云端、虚拟程序等方面的困扰。如大部分计算机在未设置防火墙、启动拦截程序时，防御能力并不理想，

作者简介：孔德武(1981-)，男，硕士，讲师，主要研究方向：计算机应用技术、计算机网络。

收稿日期：2019-04-02

可能在短暂连接了某一个被感染的 U 盘、网站后，快速被恶意程序侵入。病毒进入计算机的时间往往不超过 1 s，一旦形成病毒潜伏，该计算机内的网络信息安全已经无法保证，其它与感染计算机存在有效连接的设备，网络信息安全也面临极大的威胁。

2　数据加密技术分析

2.1　通信过程加密

通信过程加密主要应对信道安全问题，强调保存通信行为发生前后的网络信息安全。在现有的 4G（包括此前的 3G 技术）技术、有线通信技术条件下，数据的重组、发送工作是在虚拟环境下进行的，存在下载需求的用户实际上无法控制这一过程。因此，通信加密更多重视上传加密。如某用户尝试借助计算机，将网络信息上传到云端，获取对应权限后，信息能够以明文形式呈现。云端管理方则生成对应的安全参数发送给用户：

$$[S,d,p,g,SK_0,t_1].$$

其中：SK_0 为随机参数，用户端根据参数集生成可匹配的一个公开密钥：

$$PK = SK_0^{2T} mod\ P.$$

公开密钥适用于对应的工作信道，所有在该信道内进行的通信活动，均可应用该密钥进行解密、信息共享（如常见的各类云盘）。为进一步提升网络信息安全性，可根据安全参数设置唯一密钥，默认 $i = T + 1$，可知 SK_i 为空串，可进一步获知，$1 < i < T$，获取唯一密钥计算式：

$$SK_i = SK_{i-1}^{\ 2} \bmod (P-1) = SK_0^{2Y} \bmod (P-1),$$

代入安全参数 k、μ 获知：

$$R = g^k \bmod P;$$

$$w = SK_i g^{\mu} \bmod P;$$

$$S = [H(m) + 2^{T-i}\mu r]k^{-1} \bmod (P-1).$$

S 即用户需求的唯一密钥。

2.2　节点加密

在非通信但存在网络连接的情况下，可以对计算机进行节点加密，且不必考虑与信道的关联（信道加密和节点加密是各自独立的加密技术，且不冲突）。假设用户 A 登录到计算机中，并与虚拟云实现连接，将网络信息存储至该服务器中。虚拟云管理方进行用户身份辨识，将身份标识 A_sN 作为用户身份的匹配信息。加密时，将用户 A_sN 尝试进行处理的信息分为若干小模块，各个模块的大小是相等的，均为 $P - 1(P > 2^{512})$，所有小模块和大模块均带有用户 A_sN 身份标识，云端进行加密时，计算方法包括：

$$C_0 = e[B,g^t] \cdot m; C_1 = g^t; C_2 = (g_1,g_2)^T \cdots\cdots$$

其中：m 即小模块的编号，从 1 到 n 不等。对应的密文根据加密算法的层次获取，如果仅使用了一重算法，密文 X 即 C_0、C_1 或 C_2，如果使用了多重算法，密文则带有层次化特点，可根据选取的算法情况获取。

2.3　综合加密防御机制

为保证计算机网络信息安全水平，在信道加密和节点加密的基础上，提出一种综合防御机制，以信道加密和节点加密为依托，额外加强了密文的可变性和灵活性。采取周期更新计划，每次更新后，增加一重动态变化。如节点加密方面，假设用户甲选取了一重算法进行加密，其对应的密文 X 为 C_0，一周后，对该节点进行二次加密，在 C_0 的基础上，随机选取一个固定参数，比如更新的日期为某月 27 日，将该数字代入到密文中，与所有参数进行叠加，获取新的密文。即便原有密文泄露，黑客/木马也需要进行几乎无限次的迭代计算，才能逼近、了解新密文的内容，从而加强计算机网络信息的安全性。通信信道加密同样采用类似的思路，每一次完成更新都添加一个随机固定参数，获取新的密文。

3　仿真实验

3.1　模拟对象和方案

选取某大型公共计算机为对象，该计算机常年处于网络连接状态，频繁进行数据的上传、下载，且拥有大量磁盘空间进行信息存储。2017 年 10 月、2018 年 4 月、2018 年 9 月，计算机先后 3 次出现数据丢失、下载不完整等问题，经分析分别为病毒攻击、信号干扰以及通信压力过大、下载不完整所致。收集该计算机的工作参数等信息建立虚拟仿真实验。观察计算机对病毒的抵抗能力，以参数调整法模拟病毒的攻击方式和强度，另以参数模拟法设定综合加密防御机制，同步应用通信过程加密、节点加密方式提升信息安全防御能力。

3.2　模拟过程和结果

实验共分为：病毒攻击、通信干扰、通信压力 3 组。

病毒攻击组共进行 150 次模拟实验，分别为节点攻击 50 次（强攻击 25 次、普通攻击 25 次）、随机攻击 50 次（强攻击 25 次、普通攻击 25 次）、信道攻击 50 次（强攻击 25 次、普通攻击 25 次）。记录攻击发生时，密钥保护下的信息是否丢失、应用密文是否能够常规读取信息内容。

通信干扰组共进行 150 次模拟实验,分别为无干扰 50 次、中等干扰 50 次、强干扰 50 次。记录不同等级干扰时,密钥保护下的信息是否丢失、应用密文是否能够常规读取信息内容。

通信压力组进行 150 次模拟实验,分别为低压力 50 次、中等压力 50 次、高压力 50 次。记录不同通信压力时,密钥保护下的信息是否丢失、应用密文是否能够常规读取信息内容。另以当前计算机的工作参数为基准,设立对照组,进行对照组实验,包括病毒攻击、通信干扰、通信压力实验各 50 次,设定不同攻击强度、干扰等级和通信压力进行观察,其参数变化与其它实验相同。结果见表 1。

表 1 实验结果

Tab. 1 Experimental results

组别	信息丢失(n/%)	信息可读性(%)	试验次数
病毒攻击组	2/1.33	98.3	150
通信干扰组	2/1.33	91.6	150
通信压力组	0/0.00	99.4	150
对照组	19/12.67	77.2	150

由实验结果可见,对照组共出现信息丢失 19 次,占比 12.67%。在面临强病毒攻击、强干扰和较大通信压力时,信息可读性出现明显下降,综合为 77.2%。应用综合加密防御机制、通信过程加密、节点加密 3 项措施,计算机网络信息的安全性较为理想。面对强病毒攻击,出现信息丢失 2 次,占比 1.33%,信息可读性为 98.3%,面对强通信干扰,出现信息丢失 2 次,占比 1.33%,信息可读性为 91.6%,通信压力的变化没有导致信息丢失,信息可读性为 99.4%。进一步分析发现,因病毒带有多变性,现有防御机制无法实现所有刻意程序的完全识别,因此参数模拟上存在不足,导致了信息丢失问题。通信干扰会直接破坏信号强度,导致其传输过程中出现衰减、甚至丢失,也降低了其可读性。

以实验结果为基础,建议在后续工作中应用综合加密防御机制、通信过程加密、节点加密措施提升计算机网络信息安全等级,同时进一步对系统进行优化,包括建立规范化、大范围立体防御机制,提升干扰应对能力 2 个方面。防御机制要求涵盖防火墙和扫描软件,以防火墙实现可疑程序的直接隔离,以扫描软件做进一步分析,并清除计算机、数据包中的潜伏病毒。抗干扰能力的提升,可借助信道建设等方式实现,同时使计算机、通信系统远离各类干扰源,提升网络信息的安全水平。

4 结束语

综上,计算机网络信息的安全在现代社会得到广泛关注,也客观催生了各类加密技术。总体来看,来自通信信道、节点以及计算机本身的威胁均可能导致数据丢失、可行的加密技术则包括通信过程加密、节点加密以及综合加密防御机制。模拟实验中,来自各个反向的木马威胁均得到应对,可作为后续工作的参考。

参考文献

[1] 王岩. 数据加密技术在计算机网络安全中的应用价值[J]. 数字技术与应用, 2017(12):198-199.
[2] 隋天威. 计算机网络安全中的数据加密技术[J]. 电子技术与软件工程, 2016(18):226.
[3] 许子桓. 计算机安全中数据加密技术的应用分析[J]. 科技经济导刊, 2018,26(28):36.
[4] 刘博. 数据加密技术在计算机安全中的应用[J]. 电子技术与软件工程, 2017(14):207-208.
[5] 许飞丽. 数据加密技术在计算机网络安全中的应用价值研究[J]. 电脑迷, 2017(9):31.

(上接第 291 页)

3 结束语

Weka 是一个开源的数据挖掘软件,使用户能够很容易地将其应用于所要挖掘的数据集,挖掘出知识点。本文借助著名的开源数据挖掘软件 Weka3.6.2 版本,对 KDDCUP99 数据集的“KDDCUP.data_10_percent”子集中 R2L 攻击类型进行了关联分析,实现了 Weka 在网络入侵检测数据集中的应用。对数据格式的转换、数据类型的转换有了完整的认识,挖掘出特征属性及行为之间的关联关系,提高了检测的效率和准确率。

参考文献

[1] HAN Jiawei, KAMBER M. 数据挖掘概念与技术[M]. 2 版. 范明, 孟小峰,译. 北京:机械工业出版社,2007.
[2] 全亮亮. 基于数据挖掘算法的入侵检测研究[D]. 武汉: 武汉科技大学,2013.
[3] WITTEN I H, FRANK E. 数据挖掘实用机器学习技术[M]. 董琳,译. 北京:机械工业出版社,2006.
[4] NEWMAN D. Welcome to the UCI knowledge discovery in databases archive[EB/OL]. [2005-09-09].
[5] 孙元军,郑新奇,常伟倩. 基于 Weka 的城市建设用地结构特征挖掘研究[J]. 计算机工程与应用,2008,44(27):231-235.