DOI :10. 3969/J. ISSN. 1672-6693. 2010. 03. 016

云计算与无线局域网安全研究*

汪 建[1], 方洪鹰[2]
(1. 重庆邮电大学 计算机科学与技术学院, 重庆 400065 ;2. 重庆交通大学 理学院, 重庆 400075)

摘要 :无线局域网以无线信道作为传输媒介,其开放性特点使窃听、身份假冒和信息篡改等威胁无处不在。本文首先依据云计算模型,搭建每秒数亿次的超级计算平台 ;其次以破解 WLAN 中最常用的 WEP 加密协议为例,验证 IEEE802. 11 协议提出的身份认证和数据加密等一系列安全机制已经失效 ;然后用实验数据证明了以云计算作为支撑的破解平台严重威胁到无线局域网可靠性和安全性,它可以将破解时间缩短上万倍 ;最后提出行之有效的解决方案——采用 WAP/WAP2 和 TKIP 替代简单固定的 RC4 算法。

关键词 :云计算 ;无线局域网 ;WEP ;RC4 ;预测判断法
中图分类号 :TP311. 13 **文献标识码** :A **文章编号** :1672-6693(2010)03-0064-05

无线局域网(Wireless local area network, WLAN)作为有线联网方式的补充和延伸,逐渐成为计算机网络中一个至关重要的组成部分[1]。WLAN 使用无线电波作为数据传送的媒介,用户通过无线网卡方便地接入无线接取器(Wireless access point, WAP),有效距离可达数十米。较之有线局域网络,其具有联网方便、扩展性强、减少布线故障的优点。

无线媒介的开放性导致其在防范窃听、身份假冒和信息篡等安全威胁方面的弱势,因此它要求比有线网络更严格的安全措施来解决这些安全隐患。IEEE 802. 11 协议提出了一系列标准化规范和安全机制来实现身份验证和数据加密,使 WLAN 技术变得成熟与完善。但是随着云计算时代的来临,面对全球性的超级计算平台,目前 WLAN 中的加密协议显得相形见拙。本文以 WLAN 中最常用的 WEP(Wired equivalent privacy)加密协议为例,详细分析并实验证明无线局域网安全威胁的严重性。

1 云计算

云计算(Cloud computing)[2]是分布式计算技术的一种,其最基本的概念,是透过网络将庞大的计算处理程序自动分拆成无数个较小的子程序,再交由多部服务器所组成的庞大系统经搜寻、计算分析之后将处理结果回传给用户。透过这项技术,网络服务提供者可以在数秒之内,达成处理数以千万计甚至亿计的信息,达到和‘超级计算机’同样强大效能的网络服务——维基百科(Wikipedia)。

1. 1 云计算的原理

云计算是分布式处理(Distributed computing)、并行处理(Parallel computing)和网格计算(Grid computing)的发展。其原理是 :使计算分布在大量的分布式计算机上,而非本地计算机或远程服务器中,让企业能够将资源切换到需要的应用上,根据需求访问计算机和存储系统。云计算平台具有综合利用网络上的软件和数据的能力,把计算资源和存储资源联合起来,供每一个成员使用。

1. 2 云计算的特征

云计算是‘海量存储’和‘高性能计算服务’的高度融合。高性能计算服务(云计算)部署依赖于计算机集群,也吸收了自主计算和效用计算的特点 ;海量存储(Cloud storage,云存储)是一种将数据保存在虚拟存储池上的实现方式,数据独立存储,而非与计算部件共享服务器上。

从事云计算服务研究的结构众多,包括 Wikipedia, Google, Microsoft, Garmer 和 Forrester 等,它们依据各自的利益和不同的研究视角给出了云计算不同的定义和理解。但是无论广义的还是狭义的云计算,均具有如下特征 :快速部署资源或获得服务 ;按需扩展和使用 ;可以按使用量计费 ;通过网络提供服务。

1. 3 云计算的优点[3]

* 收稿日期 :2009-08-28
资助项目 :重庆市教育委员会科学技术研究项目(No. 050305)
作者简介 :汪建,男,讲师,硕士,研究方向为智能信息处理、数据挖掘。

云计算为安全带来如下优点:1)数据集中存储[4]。数据的集中存储减少了数据泄露的可能性,可靠的安全监测提供实时安全保障,用户的存储成本也大大降低。2)事件快速反应。事件的快速反应是指云计算缩短了服务时间,降低了服务器出错概率,使服务更有针对性。3)密码可靠性测试。如果用户需要使用密码破解工具定期对密码强度进行测试,那么可以使用云计算减少密码破解时间,并更能保证密码强度的可靠性。4)无限期日志。在云存储模式下,如果磁盘空间不足,可以重新分配,并不会影响日志的存储使用,而且没有日期限制。完善日志索引机制提供实时索引功能。5)提升安全软件的性能。在云计算中,出现了越来越多的高性能安全软件,也可以在某种程度上说,云计算带来了安全产品的整体提升。6)可靠的构造。通过预控制机制减少漏洞,同时更容易检测到安全状况,有助于构造出更安全的工作环境。7)安全性测试。降低安全测试成本,节省昂贵的安全性测试费用。通过云计算还可以在潜在成本规模经济下开发产品。

2 云计算对无线网络安全的挑战

无线局域网是一种利用无线技术、实现局域网功能的技术。相对于有线通信技术而言,无线传输媒体的开放性导致监听变得无处不在。因此,IEEE 802.11-1999 标准中定义了有线网对等加密技术[5],希望从认证、加密和数据的完整性三方面为数据传输提供安全保障。

2.1 WEP 协议

WEP 安全技术源自于名为 RC4[6] 的 RSA 数据加密技术,以满足用户更高层次的网络安全需求。RC4 加密算法是 RSA Security 的 Ron Rivest 在 1987 年设计的密钥长度可变的流加密算法簇。该算法具有很高级别的非线性,其速度可以达到 DES 加密的 10 倍。RC4 将用户短密钥扩展成为指定长度 N 的伪随机比特流,信源使用这个伪随机比特流与 N 位明文数据做异或(XOR)运算来产生密文,信宿则使用相同的用户密钥值产生出相同的伪随机比特流,并与接收到的密文做异或操作之后得到原始明文。加密过程如图 1 所示。

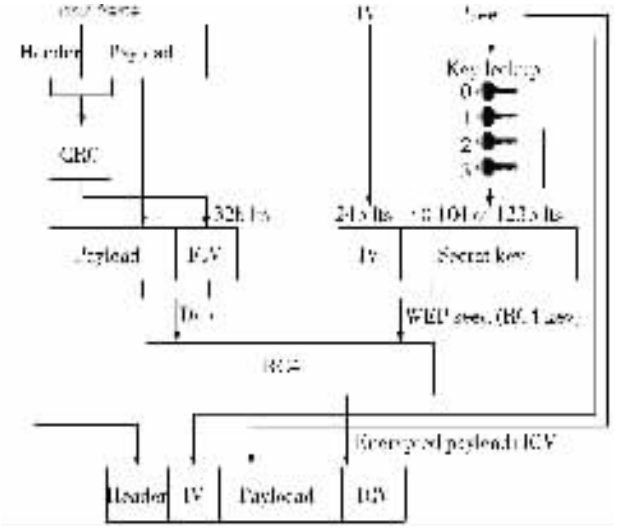

图 1　WEP 加密过程

RC4 包含密钥调度算法(Key scheduling algorithm,KSA)和伪随机序列发生算法(Pseudo-random generation algorithm,PRGA)两个算法,其伪代码描述如下。

1) KSA(key)算法

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap(&S[i],&S[j])
endfor
```

该算法的功能是构建一个 key 相关序列 S,作为产生流密钥的码盘使用。其中 S 序列长度可变,通常是 256,key 为密钥(初始向量 IV + 用户密钥 $pass$)。整个过程是先排定一个序列,然后再依据 key 的数值特征打散其顺序,确保 S 中的每一个元素都受到密钥 key 的影响,有足够的随机性,且 key 值不会出现在 S 中。

2) PRGA 算法

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(&S[i],&S[j])
    output S[(S[i] + S[j]) mod 256]
endwhile
```

该算法生成的任意位(Bit)伪随机数序列,最终用于同用户明文进行异或运算加密数据。伪随机数序列的长度等于"明文长度 + CRC 校验码"长度。

2.2 RC4 破解方法

针对WEP协议的破解主要有:①直接法[7],不试图破译加密密钥而直接解密密文;②间接法,截取密文并破译出加密密钥,再通过该密钥还原解密密文。

2.2.1 直接法　直接法解密数据主要是针对RC4算法中异或运算简单性开展工作。PRGA算法产生的伪随机密钥状态空间固然复杂,但密钥与明文的接触却过于脆弱。假设有两个明文:P_1 和 P_2,以同一个伪随机密钥 $prgakey$ 加密,则分别产生的明文是

$$C_1 = P_1 \oplus prgakey \tag{1}$$

$$C_2 = P_2 \oplus prgakey \tag{2}$$

破解者可以轻易地窃取它们,依据异或运算满足交换律和结合律的特点得知

$$C_1 \oplus C_1 = (P_1 \oplus prgakey) \oplus (P_2 \oplus prgakey) = (P_1 \oplus P_2) \oplus (prgakey \oplus prgakey) = (P_1 \oplus P_2) \oplus 0 = P_1 \oplus P_2 \tag{3}$$

只要知道"明文/密文数据对(C_1/P_1)",破解者即可解开同一伪随机密钥 $prgakey$ 加密过的等长的密文信息。即使攻击者不知道任何明文信息,对未进行分块处理的数据流加密算法RC4,也可以根据特定语言的字符频度特征猜解出明文的内容。

2.2.2 间接法　间接法可以获取用户密钥 $pass$ 为破解者带来更多的收获。破解的前提是对WEP数据帧有全面认识,WEP数据帧的基础是IEEE 802.11数据帧,其结构如图2所示。

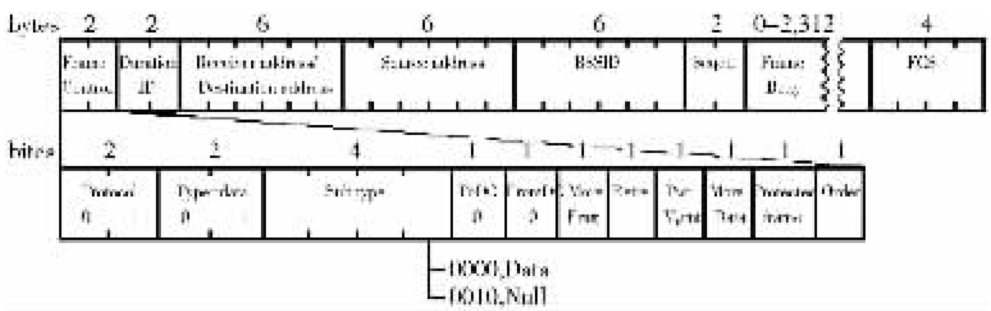

图2　IEEE 802.11 帧结构

对标准的IEEE 802.11数据帧中的"Frame Body"段和FCS段进行RC4加密并重新封装,便形成如图3所示的WEP数据帧结构。

传统的解密方法[8]是首先截获WEP数据帧,然后按如下步骤解密。

Step 1　假设密钥——穷举 N 位密钥字符串 $pass$。

Step 2　求伪随机数序列——使用RC4(IV, $pass$)算法,计算出与图4中数据负载部分($Payload + ICV$)等长的伪随机数序列 $prgakey$。

Step 3　尝试解密——求取($Payload' + ICV'$)得到。

Step 4　验证结果——因为ICV部分采用的算法是CRC32,在此,数据完整性验证变成破解者验证破解结果的标准。计算出CRC32($Payload'$),如果CRC32($Payload$) $= ICV'$,则证明当前 $pass$ 是正确的用户密钥;否则转Step 1尝试下一个密钥。

上述解密方法的弊端在于:每次尝试都包含KSA、PRGA和CRC32三个算法的完整计算过程,假设平均猜解次数 $n = 2^{keylength}/2 = 2^{keylength-1}$,通常用户密钥长度是40 Bit,即 $n = 2^{39} = 1/27$,数量级如此高的计算在有限的时间(保证用户存在且密钥不被修改)内是不可能完成的。

2.3 改进的RC4破解方法

时效性是衡量密钥破解算法优良与否的最高标准,针对破解算法时效性强的特点,现对传统的解密方式做两点修改:采用云计算,分布式完成猜解过程;修改猜解算法提高破解效率。

2.3.1 云计算　将传统的算法改变为符合云计算必须规范统一的数据规范和接口标准。以用户密钥长度是40Bit为例,密钥尝试序列如图3所示。

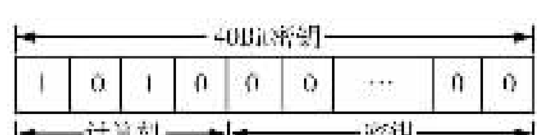

图3　密钥序列分段图

综合考虑主机和网络负载均衡的因素,云计算系统(简称云系统)中控制结点通过将用户密钥尝试序列进行分段,合理地将计算任务分配给云系统中每一台性能各异的计算机。假设云系统中有7台主机,其中"计算性能:数量(台)"配比为:1:3(台);0.25:4(台)。则密钥尝试序列按照4:36分段,任务分配如表1所示。

表 1　主机破解任务分配表

主机号	性能	计算任务
1	1	0x0 ~ 0x3FFFFFFFF
2	1	0x4000000000 ~ 0x7FFFFFFFF
3	1	0x800000000 ~ 0xBFFFFFFFF
4	0.5	0xC000000000 ~ 0xCFFFFFFFF
5	0.5	0xD000000000 ~ 0xDFFFFFFFF
6	0.5	0xE000000000 ~ 0xEFFFFFFFF
7	0.5	0xF000000000 ~ 0xFFFFFFFFF

不难看出,当前云系统的整个运算时间减少为单机系统的 1/4。并且随着云系统中主机增多,系统的时间复杂度呈线性递减。

2.3.2 预测判断算法　提高传统破解算法的效率的突破口在于减少 KSA、PRGA 和 CRC32 子算法的计算量。KSA 算法用于构建码盘,无优化的可能,忽略之。PRGA 用于生成与明码等长的伪随机密钥。IEEE 802.11 规范了标准 WEP 帧结构和 MIC 增强 WEP 帧结构,如图 4 所示。

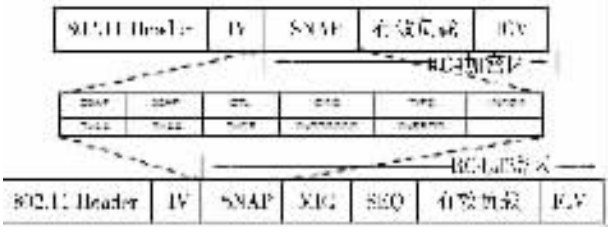

图 4　IEEE 802.11 WEP 帧结构

其中 SNAP 结构是 LLC 协议的一部分, DSAP 和 SSAP 两个属性的值固定为“ 0xAA ”。根据这一特点,提出改进的解密算法——预测判断算法。步骤如下:

Step 1　假设密钥——穷举 N 位密钥字符串 *pass*。

Step 2　生成码盘——使用 KSA(*key*)算法构建一个 *key* 相关序列 S 做码盘,其中 $key = IV + pass$。

Step 3　求短伪随机数序列——使用 PRGA 算法,计算出长度为 2B 的伪随机数序列 *prgakey'*。

Step 4　预验结果——取出 WEP 帧中 *Payload* 的前两个字节,它们应该是 *DSAP* 和 *SSAP* 加密之后的密文 *DSAP'* 和 *SSAP'* ;然后求取(*DASP'* + *SSAP'*) ⊕*prgakey'* 得到(*DSAP''* + *SSAP''*) ;如果,(*DSAP''* + *SSAP''*) = 0xAAAA 证明当前猜解的密钥不正确,转 Step 1 尝试下一个密钥。

Step 5　二次解密——求取(*Payload* + *ICV*) ⊕ *prgakey* 得到(*Paylaoad'* + *ICV'*)。

Step 6　终验结果——因为 *ICV* 部分采用的算法是 CRC32,在此数据完整性验证变成破解者验证破解结果的标准。计算出 CRC32(*Payload'*),如果 CRC32(*Payload'*) = *ICV'*,则证明当前 pass 是正确的用户密钥 否则转 Step 1 尝试下一个密钥。

预测判断算法是将传统算法的 Step 2 分解为 3 个步骤来预验证假设密钥的正确性。假设 *payload* 的长度为 2312 B,预测判断 PRGA 算法的 2B/3 312B ≈ 0.000 865,计算量是传统 PRGA 算法的,运算 CRC32 算法的次数减少为传统算法的 2^{-35}。

2.4 实验结论

通过在局域网中搭建云计算系统,对 40Bit 的用户密钥进行解密,实验结果如图 5 所示。

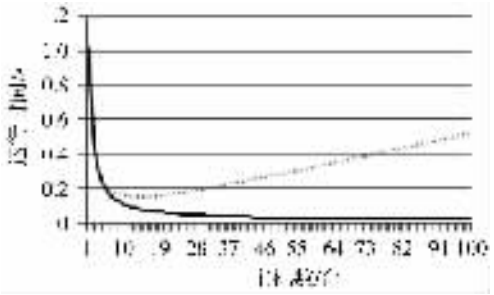

图 5　云计算性能状态图

实验数据表明,如果开启系统“ 负载动态均衡 ”功能,随着主机数的增加,网络负载对系统的影响越来越显著,当主机数目达到 14 台时,系统性能达到峰值 0.151 429,即云计算系统解密速度是单机系统解密速度的 1/0.151 429 ≈ 6.6 倍。如果采用“ 静态分配任务 ”方式,网络开销可以忽略,主机数与系统运行时间成反比。

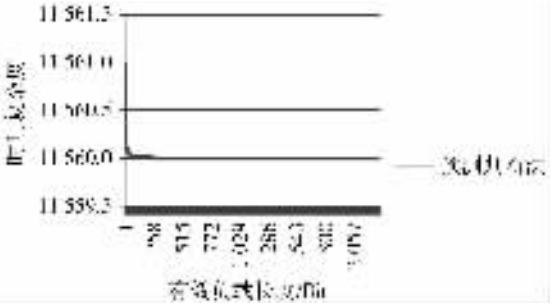

图 6　PRGA 算法性能状态图

预测判断算法的优越性体现在 Payload 较长的情况,如图 6 所示。假设负载长度为 2 312 B,实验表明预测判断算法中 PRGA 的性能是传统解密算法性能的 16 184/4 624 ≈ 3.5 倍。

3 结束语

本文研讨了云计算对无线网络安全带来的挑战,充分展现了云计算的高效性。实验证明,“ 云计算 + 预测判断算法 ”的运算性能提高为传统破解方法的百万倍,使原本需要花费上百年的破解过程,在

10 min 内得以完成。国际上流行无线网络安全工具 BT4 也是采用了类似的方法对 WEP 进行解密,64Bit 密钥的破解也就是数分钟的工作。

目前针对无线网络安全的保护技术除了 WEP 外还有更安全的 WAP/WAP2 和 TKIP。安全研究是把双刃剑,既可能对系统造成破坏,使用得当也可以预测和避免网络威胁。

参考文献:

[1] 张丰翼,刘晓寒,马文平,等. 无线局域网安全的关键问题[J]. 信息安全与通信保密,2004(5):34-37.
[2] 顾理琴. 浅谈云计算(Cloud computing)——未来网络趋势技术[J]. 电脑知识与技术,2008(S2):11-12.
[3] 编者. 云计算为安全带来的七大利好[J]. 计算机与网络,2008(17):37-38.
[4] 姚渝春. 网络存储与 UAMS 模式研究[J]. 重庆师范大学学报(自然科学版),2008(3):42-45.
[5] 谢四江,冯雁. 浅析云计算与信息安全[J]. 北京电子科技学院学报,2008(4):1-3.
[6] Matthew Gast. 802.11® Wireless Networks the definitive Guide [M]. 2nd ed. Sebastopol,CA:O'Reilly Media, Inc,2005.
[7] 孙宏,杨义先. 无线局域网协议 802.11 安全性分析[J]. 电子学报,2003(7):1098-1100.
[8] 张丽丽,张玉清. 基于分布式计算的 RC4 加密算法的暴力破解[J]. 计算机工程与科学,2008(7):15-17,20.

Cloud Computing and Research into WLAN Security

WANG Jian[1], *FANG Hong-ying*[2]

(1. College of Computer Science and Technology, Chongqing University of Posts and Telecoms, Chongqing 400065;
2. College of Science, Chongqing Jiaotong University, Chongqing 400074, China)

Abstract: The WLAN treats wireless channel as transmission medium, but its open characteristics cause wiretapping, identity threats, counterfeiting and tampering of information are actually ubiquitous. In this paper, based on cloud computing model, we set up hundreds of millions of times per second, super-computing platform; Secondly, we crack WEP the most common WLAN encryption protocol to verify a series of safety mechanism proposed by IEEE 802.11 to be ineffective, such as identification authentication and the data encryption and so on. Then we use the experimental data to prove the system supported by cloud computing threat WLAN's reliability and security seriously, to shorten the time to crack thousands of times; inally, we recommend WAP/WAP2 and TKIP to replace simple fixed RC4 as solution.

Key words: cloud computing; WLAN; WEP; RC4; predictive judgment

(责任编辑 游中胜)