无线局域网 WEP 协议安全隐患分析

王 莉[1],刘志愚[2],刘一兰[3]
(1.中南民族大学 计算与实验中心,湖北 武汉 430074;
2.北京邮电大学,北京 100876; 3.深圳腾讯公司,广东 深圳 518052)

摘 要:近年来,无线局域网技术和市场都有了突飞猛进的发展。而随着 IEEE802.11 无线局域网的普及,网络的安全性问题也正在变得日益严峻。WEP 协议是 IEEE802.11 标准规定的数据加密机制。WEP 虽然提供了 64 位和 128 位长度的密钥机制,但是它仍然存在许多缺陷。文中详细分析了 WEP 加密和解密的原理,从 3 个方面说明了 WEP 存在的安全隐患,并依次讨论了各安全隐患所对应的解决方案。

关键词:无线局域网;有线等效加密;IV 碰撞;网络安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0055-02

Analysis on Secure Hidden Troubles of Wireless Local Area Network's WEP

WANG Li[1], LIU Zhi-yu[2], LIU Yi-lan[3]
(1. Center of Computing and Experimenting, South-Central University for Nationalities, Wuhan 430074, China;
2. Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Tencent Inc, Shenzhen 518052, China)

Abstract: Recently, the technology and market of wireless local area network have gained great development. With the popularization of IEEE802.11 wireless local area network, the network security has become more and more important. WEP algorithm is the data encryption technology prescribed by IEEE802.11. Although WEP provides 64bit and 128bit key mechanism, it still has many limitations. This paper analyzes the encryption principle, decryption principle of WEP, and narrates the secure hidden troubles of it from three aspects, then discusses the troubles' corresponding projects.

Key words: wireless local area network; wired equivalency privacy; IV collision; network security

0 引 言

随着无线技术和网络技术的不断成熟和普及,无线局域网在全球范围内的应用已经成为一种趋势。由于无线通信的本性使然,空中传播的数据本身就是不安全的,随着无线局域网的逐渐普及,无线数据流的安全问题就显得尤为突出。

无线局域网的 IEEE802.11 标准规定了两部分安全机制:一是访问认证机制;二是数据加密机制,也就是有线等效加密(Wired Equivalency Privacy,WEP)协议[1,2]。它们是现在常用的无线局域网系统中安全机制的主要形态和基础。在 802.11 安全机制的 IEEE 核准过程中,加密专家只对 WEP 算法进行了很少的组内评审工作,正是这一疏忽,造成 WEP 的多处漏洞,这为各种窜改数据的主动攻击和窃听数据的被动攻击提供了方便之门。

1 WEP 安全机制分析

WEP 为等效加密,即加密和解密的密钥相同。为了保护数据,WEP 使用 RC4 算法来加密从无线接入点或者无线网卡发送出去的数据包。RC4 是一个同步流式加密系统,这种加密机制将一个短密钥扩展成一个任意长度的伪随机密钥流,发送端再用这个生成的伪随机密钥流与报文进行异或运算,产生密文。接收端用相同的密钥产生同样的密钥流,并且用这个密钥流对密文进行异或运算得到原始报文。

从图 1 可以看到,发送端首先计算原始数据包中明文的 32 位 CRC 循环冗余校验码,也就是计算其完整性校验值(Integrity Check Value,ICV),然后将明文与校验码一起构成传输载荷。在发送端和无线接入点 AP 之间共享一个密钥,长度可选 40bit 或 104bit。发送端为每一个数据包选定一个长度为 24bit 的数作为初始向量(Initialized Vector,IV),然后将 IV 与密钥连接起来,构成 64bit 或

收稿日期:2005-11-11
基金项目:湖北省科技攻关重大项目(2004AA103A01)
作者简介:王 莉(1978-),女,湖北人,助教,硕士,研究方向为网络安全。

128bit 的种子密钥，再送入 RC4 的伪随机数生成器(Pseudo－Random Number Generator，PRNG)中，生成与传输载荷等长的随机数，该随机数就是加密密钥流。最后将加密密钥流与传输载荷按位进行异或操作，就得到了密文。

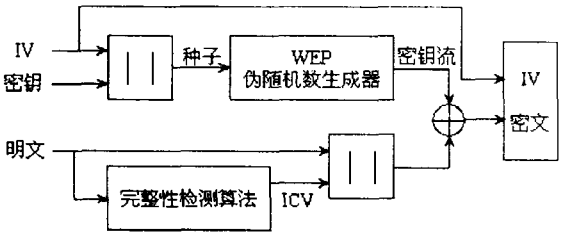

图 1 WEP 加密过程

接收端的解密过程如图 2 所示。由于发送端是将 IV 以明文形式和密文一起发送的，当密文传送到 AP 后，AP 从数据包中提取出 IV 和密文，并将 IV 和自己所持有的共享密钥一起送入伪随机数发生器，得到解密密钥流，该解密密钥流实际上和加密密钥流是相同的。然后接收端再将解密密钥流和密文进行异或运算，就得到了明文，将明文进行 CRC 计算后就可以得到校验码 ICV′。如果 ICV′和 ICV 是相等的，那么就得到了原始明文数据，否则解密就失败了[3,4]。

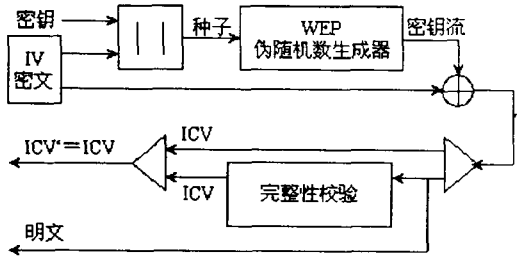

图 2 WEP 解密过程

2 WEP 安全隐患分析

由于 WEP 采用密钥长度可变的 RC4 流密码算法来保护数据传输，而在实际应用中，密钥经常基于用户所选择的密码，这就大大降低了密钥的安全有效长度。一些计算机专安全专家已经发现了危及 WLAN 安全的安全隐患。

2.1 RC4 算法自身的不足

在采用 IEEE802.11 协议的无线局域网产品中，主要有两种方法来给定 IV 的值：一种是当无线网卡在初始化时，IV 的值取为 0 或某一个随机数，然后随着数据包的个数逐次按模 2^{24} 递增，当增加到 2^{24} 时 IV 的值又回到 0；另一种方法是在 $[0,2^{24}-1]$ 上随机选取 IV 值。当采用第一种方法时，只要每隔几小时就会发生 IV 碰撞现象。当 IV 的值被随机选取时，在传输大约 4823 个数据包后，就会有 50% 的概率发生 IV 碰撞，12430 个数据包后将有 99% 的概率发生 IV 碰撞。

在 WEP 协议中，每一个封装的数据包中都包含一个初始向量 IV。IV 在数据帧中以明文形式传输，并和原始密钥一起作为种子密钥，用来生成加密有效载荷的密钥流。密钥流加密算法的一个缺陷就是，如果用相同的 IV 和密钥加密两个消息，将导致两条消息的同时泄漏。

这里，假设有两段明文 P1 和 P2，它们都采用相同的种子密钥{IV，Key}，对应的生成密文分别为 C1 和 C2，则：

$$C1 = P1 \oplus RC4\{IV, Key\}$$

$$C2 = P2 \oplus RC4\{IV, Key\}$$

$$C1 \oplus C2 = P1 \oplus P2$$

所以在 IV 和密钥相同的情况下，如果知道密文 C1，C2 和其中一段明文 P1，就可以得到另一段明文 P2。如果仅知道密文 C1 和 C2，那么就得到了两段明文 P1 和 P2 的异或值，使用字典攻击法，就可以对 P1 和 P2 的值进行猜测，并最终得到其中一条明文。随着已知密文数的增多，明文的内容会比较容易被猜测出来。而随着分析出明文数的增加，后面的解密过程就会变得越来越容易。

2.2 密钥管理带来的安全隐患

在 WEP 协议中，对密钥的生成和分布没有做任何规定，密钥的使用也没有具体规定，这些实际应用中重要的问题都被留给设备制造商自行解决，导致大批在密钥管理中存在安全隐患产品的出现。而这些产品中使用的 WEP 加密密钥通常在很长一段时间内都不会改变，导致攻击者在一个密钥生存周期内可以获得大量的无线传输数据包。从中选择出使用相同 IV 的数据包，只要知道一个明文和密文，就可以计算出这些数据包使用的密钥。如果攻击者将对应的 IV 和密钥组织成一个解密字典的形式，就可以对无线传输数据进行实时解密了。

此外，在具体应用中，大多数用户长时间共享同一密钥，并且使用 WEP 协议的设备都是将密钥保存在设备中，所以一旦设备丢失，所有使用这一共享密钥的计算机的安全都可能受到威胁[5]。

2.3 身份认证中的安全隐患

在 WEP 协议中，规定的身份认证是单向的，即 AP 对申请接入的客户端进行身份认证，而客户端并不对 AP 进行身份认证。这种单向的身份认证方式导致了假冒的 AP 的存在。

此外，在 WEP 协议身份认证过程中，AP 以明文的形式把 128 字节的随机序列流发送给客户端，如果能够监听一个成功的客户端与 AP 之间身份认证的过程，截获它们双方之间相互发送的数据包，通过把随机数与加密值相异或，就可以得到密钥流。而拥有了该密钥流，任何人都可以向 AP 提出访问请求。这样，WEP 协议所使用的身份认证方式，对于具有监听和截获数据能力的攻击者来说几乎形同虚设。

3 WEP 安全机制改进

WEP 加密采用的 CRC4 算法虽然简单高效，但并不

(下转第 59 页)

配表见表 1(以 S_1 与 S_1' 之间的匹配表为例)。

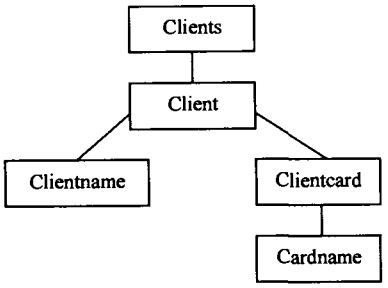

图 2　XML 的数据模式

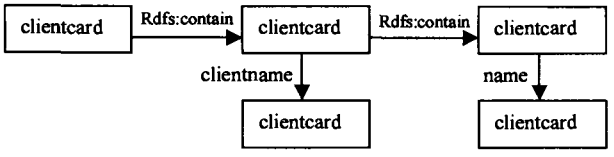

图 3　基于 RDF 的局部本体

表 1　XML 与 RDF 之间的匹配表

S_1 中的 Xpath 表示	S_1'中的 RDF 表示
/clients	clients
/clients/client	client
/clients/client/clientname	client. clientname
/clients/client/clientcard	clientcard
/clients/client/clientcard/cardname	clientcard. cardname

(3)Protege－2000 是一种半自动化的本体集成工具,在用户指定参与集成的本体后,系统会自动找出本体间的冲突,并提供可供选择的解决方案。在用户选择相应方案后,系统会继续寻找本体间的其余冲突,反复循环,直至集成过程的结束。利用此工具把图 3 中的两个局部本体集成为全局本体。

(4)用户根据界面提示输入"查询所有客户所持卡的卡号"的请求,根据上文中的查询转换算法对用户的查询请求进行重写,并向数据库提交查询请求。实验结果表明,可从数据库中检索出 28 条相应数据。虽然集成效率仍有待提高,但也说明此方案是可行的。

3　结束语

文中针对具有相同语义的 XML 数据经常具有不同表达形式的问题,通过在语义集成中融入本体的思想,构建了基于本体的语义集成方案,使用户不需了解 XML 数据的结构和模式,就可以实现查询。方案着重对局部本体、全局本体、匹配表、查询转换等几部分进行了设计和探索,并通过一个实验证明此方法是可行性的。方案采用 RDF 作为本体描述语言,然而 RDF 的表达能力毕竟有限,在 OWL 趋于成熟时应过渡到 OWL。

参考文献:

[1] HP Labs. RDQL－RDF Query Language[J]. The art of Semantic Web,2001(5):64－69.

[2] Schneider P. The Yin/Yang Web:XML Syntax and RDF Semantics[A]. AAAI/IAAI－2000[C]. 北京:清华大学出版社,2000. 146－153.

[3] 李丽萍,马文阁,梁　勇. XML 深入剖析[J]. 辽宁工程技术大学学报,2002(4):41－45.

[4] Brickley D. RDF Schema Specification[EB/OL]. http://www.w3.org/TR/PR2rdf2schema, 2004.

[5] Stumme G. Ontology Merging for Federated Ontologies on the Semantic Web[A]. FMII－2001[C]. 北京:机械工业出版社,2001. 413－418.

(上接第 56 页)

适合需要高度保密的无线局域网应用环境,可以采用基于 OCB(Offset CodeBook,分支编码本)模式的 AES(Advanced Encryption Standard,高级加密标准)的保密机制。AES 加密算法是美国的标准加密算法,其抗攻击型已经得到验证和检验。

一个加密系统的核心是密钥管理,而 WEP 协议的一个主要问题就是不存在密钥管理机制,使得系统的安全性得不到保证。所以,采用高效、合理的密钥管理机制,是解决问题的根本方法。

传统 WEP 协议规定的是单向的身份认证,其身份认证机制存在种种问题,解决问题的关键是完善认证机制,建立双向的、性能良好的身份认证机制。

4　结束语

无线局域网不需要有线连接就能收、发数据,人们能够自由地把计算机设备放置在最合适的地方。并且无线局域网很大程度上的灵活性,使人们能够及时对有变动的要求做出应对。虽然无线局域网拥有诸多优势,但同样面临着一些阻碍其发展的问题,而安全性就是最主要的问题之一。作为一个不断改善和升级的过程,只有采取一套严密的安全方案以确保无线局域网的安全,才能让无线局域网得到更大范围的发展。

参考文献:

[1] 钱　进. 无线局域网技术与应用[M]. 北京:电子工业出版社,2004.

[2] Haslestad T, Telenor R D. Wireless Local Area Network IEEE 802.11[EB/OL]. http://www.tele.ntnu.no,2004.

[3] Jani K. Wireless Local Area Network Security－Obscurity Trough Security[EB/OL]. http://www.ee.oulu.fi,2004.

[4] Madge Limited. Wireless LAN Security White Paper[EB/OL]. http://www.madge.com,2003.

[5] 钟晓珊,刘　旭. 无线局域网接入的安全性问题[J]. 信息技术,2004,12(28):10－13.