维普资讯 http://www.cqvip.com

WAPI 协议的可用性分析与改进*)

铁满霞[1,2]　李建东[1]　王育民[1]
(西安电子科技大学通信工程学院　西安 710071)[1]
(中国科学院研究生院信息安全国家重点实验室　北京 100039)[2]

摘　要　本文分析 WAPI 安全关联建立过程存在的脆弱性。由于 WAPI 协议没有强调可用性，因此攻击者可通过未受保护的管理帧引入 DoS 攻击，本文对其造成的危害进行详细讨论，并给出合理的防御措施。为提高协议的健壮性与可用性，本文还讨论了协议失败的恢复手段，提出了一种改进的 WAPI 协议实施方案，在尽可能不改变原有协议的框架和封装结构的前提下，最大程度降低或避免所讨论的 DoS 攻击。

关键词　无线局域网，WAPI，安全性，可用性

Availability Analysis and Improvements for WAPI

TIE Man-Xia[1,2]　LI Jian-Dong[1]　WANG Yu-Min[1]
(School of Telecommunication Engineering, Xidian University, Xi'an 710071)[1]
(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039)[2]

Abstract　This paper analyzes the security of the establishment procedure of WAPI security association. Since the WAPI design does not emphasize its availability, it is possible to introduce several DoS attacks. We detail the DoS attacks on unprotected management frames and propose some reasonable countermeasures. In order to enhance the robust and availability, some tradeoffs in failure-recovery strategies are discussed and an improved variant of WAPI is proposed to maintain its primary structure and encapsulation and address all the discussed vulnerabilities.

Keywords　WLAN(Wireless Local Area Network), WAPI(WLAN Authentication and Privacy), Security, Availability

1　引言

为了解决无线局域网 WLAN(Wireless Local Area Network)国际标准 ISO/IEC 8802-11 中定义的 WEP(Wired Equivalent Privacy)安全机制存在的安全漏洞，我国分别于 2003 年与 2006 年颁布了无线局域网国家标准及其第一号修改单[1,2]，其中采用的安全机制——无线局域网鉴别与保密基础结构 WAPI(WLAN Authentication and Privacy Infrastructure)很好地解决了无线局域网的安全问题。WAPI 是由我国宽带无线 IP 标准工作组提出的具有创新性的安全技术，主要包含两个部分：无线局域网鉴别基础结构 WAI(WLAN Authentication Infrastructure)和无线局域网保密基础结构 WPI(WLAN Privacy Infrastructure)，其中 WAI 提供安全策略协商、用户身份鉴别、密钥协商、接入控制的功能，而 WPI 则提供用户通信数据的保密性、完整性及数据源鉴别等。

WAPI 安全关联 WAPISA(WAPI Security Association)建立过程包括证书鉴别与密钥管理协议，涉及到的实体有鉴别请求者 ASUE(Authentication Supplicant Entity)、鉴别器 AE (Authentication Entity)及鉴别服务器 AS(Authentication Server)。通常，成功鉴别意味着 ASUE 与 AE 通过 AS 相互验证对方的身份，并为后续密钥管理协议提供共享的基密钥 BK(Base Key)。基于该共享 BK，密钥管理协议为数据通信会话协商并分发可用密钥。AS 可与 AE 驻留于同一设备，也可位于不同设备上。基于证书鉴别方式建立 WAPISA 的完整握手过程包括 6 个阶段：网络及安全能力发现、串路验证与关联、证书鉴别、单播密钥协商、组播密钥通告与安全的数据通信。对每个阶段这里不再赘述，详见文[2]。

在无线局域网中，常见的攻击方法有被动监听/业务分析(Passive Eavesdropping/Traffic Analysis)、消息注入/主动监听(Message Injection/Active Eavesdropping)、消息的删除与拦截(Message Injection/Active Eavesdropping)、伪装与恶意 AP(Masquerading and Malicious AP)、会话劫持(Session Hijacking)、中间人攻击 MitM(Man-in-the-Middle)、拒绝服务攻击 DoS(Denial-of-Service)等[3]。无线局域网的串路层存在 3 种类型的帧，即数据帧、管理帧及控制帧。任何操纵这些帧直接或间接破坏数据的机密性、完整性、双向鉴别及可用性均被视作攻击。

在 WAPI 协议中，只有对数据帧通过 WPI 进行了保护，而未对管理帧与控制帧采取安全措施。笔者基于完整的 WAPISA 建立过程，考虑每种可能的攻击，将主要从管理帧与失败恢复等方面分析 WAPI 协议面临的攻击及应采取的防御措施。为提高协议的可用性，在尽可能维持基本协议原定义的框架与封装结构的前提下，提出一种 WAPI 协议的改

*)国家自然科学基金和微软亚洲研究院联合资助项目(60372048)(大规模宽带无线自适应 Ab hoc 网络)；教育部科学技术研究重点项目(104171)(大规模宽带无线分布式网络关键技术)；中科院研究生院信息安全国家重点实验室开放课题(无线 Ad hoc 网的安全技术)。**铁满霞**　副教授，博士研究生，主要研究方向：宽带无线 IP 技术、移动通信、信息安全等；**李建华**　教授，博士生导师，博士，主要研究方向：宽带无线 IP 技术、移动通信、软件无线电、Ab hoc 自组织网络等；**王育民**　教授，博士生导师，研究方向：信息论、编码、密码等。

维普资讯 http://www.cqvip.com

进实施方案，以避免这些 DoS 攻击或使攻击造成的危害降低到最小程度。

2 证书鉴别协议的安全性分析

为方便讨论，首先简要分析阶段 3 证书鉴别过程的安全性。WAPI 证书鉴别协议实际是一种鉴别的 DH(Diffle-Hellman)密钥交换。对于鉴别密钥建立协议的分析，应确定攻击者的能力和协议的设计目标。

对不安全的信道作如下假设：

(1)攻击者具有足够的计算能力；

(2)攻击者不能从协议以外的范围获取安全信息；

(3)攻击者有能力获取、删除、加入、修改、重放网络上的报文。

鉴别密钥建立协议除完成显式密钥鉴别外，还应具有以下性质[4]：已知密钥安全 KKS(Known Key Security)、完善前向保密 PFS(Perfect Forward Secrecy)、非密钥泄漏伪装 Non-KCI(no Key Compromise Impersonation)、非未知密钥共享 Non-UKS(no Unknown Key Share)。

WAPI 证书鉴别协议完成了显式密钥鉴别。接入鉴别请求中的签名字段 Sig_{ASUE} 是由相应 ASUE 实体节点产生的，接入鉴别响应中的签名字段 Sig_{AE} 是由 AE 实体节点产生的，而根据 DH 难题，基密钥 BK 只能被 ASUE 和 AE 节点计算出来。所以包含在请求和响应 (12)中的双方一次性随机数 *Snonce*、*ANonce* 与双方临时公钥 $x.G$、$y.G$ 作为询问，双方通过验证对方的签名来鉴别对方的身份，并且保证了请求和响应签名字段的新鲜性。签名字段 Sig_{ASUE}、Sig_{AE} 包含 ASUE 节点和 AE 节点的身份以及包含 DH 交换的两个临时公钥 $x.G$、$y.G$，保证了会话密钥和身份的正确绑定，因此协议有效地防止了中间人攻击、重放攻击、伪装、会话劫持等攻击方式，完成了显式密钥鉴别。

WAPI 证书鉴别协议除完成显式密钥鉴别外，还具有 PFS、KKS、Non-KCI 和 Non-UKS 的性质。由于 ASUE 和 AE 利用临时公钥的 DH 交换生成基密钥 BK，且每次鉴别时 *Snonce*、*ANonce* 与 $x.G$、$y.G$ 均是随机的，因此有：

(1)会话是独立的。某些或某次会话密钥暴露，不会影响其他会话密钥的安全，所以协议具有 KKS 的性质；

(2)提供完善的前向保密性 PFS。即使 ASUE 和 AE 的长期私钥丢失，攻击者面临 DH 难题，仍不能计算出以前协商过的所有会话密钥，也不能根据某次会话密钥来恢复以前的会话密钥；

(3)在协议中，通信双方用自己的私钥生成签名，所以协议具有 Non-KCI 的性质；

(4)在协议中，通信双方用自己的私钥所作的签名包含双方的身份，所以协议具有 Non-UKS 的性质。

3 管理帧面临的攻击及防御措施

证书鉴别协议虽然具有强壮的安全性，但由于 WAPI 协议没有对管理帧进行保护，因此攻击者很容易利用或伪造这些管理帧，干扰 WAPISA 的建立。

3.1 WAPI IE 字段的伪造与篡改

WAPISA 的阶段 1 和阶段 2 通过管理帧完成，因此极易遭受到被动监听、消息注入、消息的删除与拦截、伪装与恶意 AP 等 4 种攻击。攻击者可伪装成 AE 通过 Beacon 和 Probe Response 向 ASUE 发送虚假的安全能力与网络信息，一旦攻击成功，ASUE 将被强迫采用不合适的安全参数与合法的 AE 通信或关联至恶意的 AE。攻击者还能向具有较弱安全能力的 AE 伪造(Re)Association，如果没有采取进一步的保护措施，则将会带来问题[5]。

(1)降低安全等级

无线局域网 IEEE 802.11i[6] 提供与 WEP 的后向兼容，因此存在安全等级降低攻击(Rollback Attack)[3]。但在 WAPI 中，同一网络也可同时启用多种不同的鉴别机制，如基于证书的鉴别、基于预共享密钥的鉴别等，一般来说，基于证书的鉴别方式相比基于预共享密钥的鉴别方式安全性要高；为了满足不同用户对安全等级的不同需求，WAPI 还可以支持多种等级不尽一致的数据通信所用的密码算法。WAPI 并没有限定某一 AE 必须只能采用一种鉴别方式或者只能支持一种密码套件，为了确保 ASUE 漫游情况下的网络正常访问，因此有可能要求 AE 同时支持证书鉴别和预共享密钥鉴别及其他多种等级不同的密码算法，以便为各种 ASUE 提供服务。但这种混合配置不同于 IEEE 802.11i，它不会为系统带来安全等级降低的风险。因为 WAPI 不提供与 Pre-RSNA 技术的后向兼容性，攻击者虽然可以通过避免证书鉴别，有意采用较低等级的密码套件等试图降低安全等级，前期可以建立关联，但在后续的单播密钥协商过程中将不能通过验证，因此不会引入安全等级降低攻击，只是浪费了阶段 1 到阶段 3 的一些资源。需指出的是，引起资源的浪费在某种意义上讲也属于一种 DoS 攻击。

(2)污染 WAPI IE 字段

对 WAPI 进行的另一种类型的 DoS 攻击涉及到 WAPI IE 验证机制。WAPI IE 包含鉴别方法列表、单播密码套件列表、组播密码套件、能力字段、BKID 列表。AE 将所支持的 WAPI IE 添加在 Beacon 和 Probe Response 帧中，ASUE 将所选择的 WAPI IE 添加在(Re) Association 帧中。AE 和 ASUE 采用协商的安全套件执行鉴别和密钥管理协议，采用协商的密码套件保护数据通信。为了证实 WAPI IE，要求 ASUE 在单播密钥协商响应中包含与中相同的 WAPI IE，要求 AE 在单播密钥协商确认中包含与 Beacon 和 Probe Response 中相同的 WAPI IE。收到单播密钥协商响应后，AE 将其中的 WAPI IE 逐比特与收到的(Re)Association 中的对应字段比较，验证它们是否相同；收到单播密钥协商确认后，ASUE 将其中的 WAPI IE 逐比特与收到的 Beacon 和 Probe Response 中的对应字段比较，验证它们是否相同。若不同则 AE 和 ASUE 将相互解除串路验证，并记录下此次安全错误。

攻击者监听合法 AE 的 Beacon，篡改该帧中某些非关键比特。所谓非关键比特，指的是这些比特的篡改不会影响到帧的有效性与鉴别及密码套件的选择。例如，WAPI 能力字段中的保留比特就是非关键比特。攻击者广播这种伪造的 Beacon 来造成 ASUE 对 WAPI IE 的错误了解。由于这种伪造的 Beacon 只修改“非关键”比特，AE 和 ASUE 依然能采用有效的安全套件继续鉴别和密钥管理协议，但单播密钥协商却不可能成功，因为 WAPI IE 的验证会失败。当 ASUE 采用主动扫描而非被动方式，攻击者可以通过篡改 WAPI IE 伪造 Probe Response，这需要攻击者以更及时的方法干扰握手过程。攻击者还能篡改(Re)Association 的 WAPI IE 造成 AE 对 ASUE 的错误了解，同样也能阻塞协议。污染 WAPI IE 字段形成的攻击如图 1 和图 2 所示。

维普资讯 http://www.cqvip.com

阶段 1：*[Message 1: AE->ASUE] Beacon + AE RSNA IE*

[Message 1′: Attacker->ASUE] Beacon + AE RSNA IE′

[Message 2: ASUE->AE] Probe Request

[Message 3: AE->ASUE] Probe Response + AE RSNA IE

[Message 3′: Attacker->ASUE] Probe Response + AE RSNA IE′

阶段 2、阶段 3：……

阶段 4：*[Message 15: AE->ASUE] Unicast Negotiation Response + AE WAPI IE*

{ASUE 将收到 Message 15 中的 WAPI IE 与阶段 1 中的对营字段比较，发现不匹配，则协议失败，发送 Deauthentication 解除与 AE 的关联。}

图 1 污染阶段 1 的 IE 字段实施攻击

阶段 1：……

阶段 2：*[Message 4: ASUE->AE] Open System Authentication Request*

[Message 5: AE->ASUE] Open System Authentication Response

[Message 6: ASUE->AE] Association Request + ASUE RSNA IE

[Message 6′: Attacker->AE] Association Request + ASUE RSNA IE′

[Message 7: AE->ASUE] Association Response

阶段 3：……

阶段 4：*[Message 14: ASUE->AE] Unicast Negotiation Acknowledge + ASUE WAPI IE*

{AE 将收到 Message 14 中的 WAPI IE 与阶段 2 中的对营字段比较，发现不匹配，则协议失败，发送 Deauthentication 解除与 ASUE 的关联。}

图 2 污染阶段 2 的 IE 字段实施攻击

(3)防御措施

基于上述分析，攻击者污染或篡改 WAPI IE 虽然不会降低安全等级，却引入了 DoS 攻击，因为攻击者针对的不是建立连接成功，而只是简单地阻塞协议的执行。由于这种攻击非常易于实现，且伪造 Beacon 将会影响到所有的 ASUE，因此认为这种攻击具有较大的危害性。再者，AE 和 ASUE 在阶段 1 和阶段 2 不可能意识到 WAPI IE 的污染或篡改，有可能继续交互相当数量的消息，直到单播密钥协商过程失败。换言之，合法实体做相当多的工作，而攻击者只需用很小的手段就可干扰成功。这不仅浪费了 AE 和 ASUE 的资源，而且使得攻击者也将具有更多的时间周期性重复这种攻击。

这种薄弱性的存在主要有 3 方面原因：①Beacon、Probe Response 及(Re)Association 等未保护；②在 WAPI IE 协商与证实之间存在许多消息交互，这将耗去很多资源并为攻击者留下足够的时间；③阶段 4 的逐比特比较来验证 WAPI IE 过于严格。当然这种脆弱性采用管理帧的鉴别就可以被解决，并不失为一种好方法，但在某些情况下，譬如在开始阶段 AE 和 ASUE 尚未有共享密钥，使得鉴别 Beacon、Probe Response 及(Re)Association 变的不可行。因此，比较实用的一种方法就是在执行 WAPI IE 验证时尽可能地避免浪费消息交互，使攻击不至于带来太大的破坏性，譬如可在阶段 3 中提前验证 WAPI IE。

另一种方法，可通过放宽证实条件避免这种对 WAPI IE 的污染攻击，换言之，AE 和 ASUE 在保证协商安全时可忽略某些 WAPI IE 中非关键比特的差别。实际上，在 WAPI IE 中，对后续阶段而言，只有鉴别和密钥管理套件选择为关键项，这是因为 AE 和 ASUE 在完成鉴别和共享了某些密钥后，总能安全地协商加密密码套件。如果攻击者不改变鉴别和密钥管理套件选择，由于已经正确执行了鉴别过程，WAPI IE 可以被接受。之后为了后续数据加密，AE 和 ASUE 可在单播密钥协商中采用鉴别的 WAPI IE。相反，若攻击者篡改了鉴别和密钥管理套件选择，在阶段 3 开始时甚至在阶段 2 的关联过程就能被检测出来，关联失败，ASUE 不会继续消息交互，而是快速重试。最坏情况，这种篡改在单播密钥协商中就被防止。

3.2 伪造 Deauthentication 或 Disassociation

如前所述，WAPISA 的阶段 1 和阶段 2 极易遭受到被动监听、消息注入、消息的删除与拦截、伪装与恶意 AP 等前 4 种攻击，但阶段 3 采用了强壮的双向鉴别协议，使这些攻击将不可能存在。由于证书鉴别协议能防止攻击者伪造、篡改、重放鉴别分组，从而避免了前 3 种攻击；又由于必须采用身份而非 MAC 地址完成成功的双向鉴别，使得伪装与恶意 AP 攻击不可能存在。即使阶段 3 省略，即采用 PSK 或缓存的 BK，对端仍能通过阶段 4 验证是否拥有共享密钥而实现相互鉴别，同样能抵御前 4 种攻击。

遗憾的是，即使采用了强壮的双向鉴别机制，第 5 种攻击会话劫持仍有可能存在。当合法站点成功完成证书鉴别后，攻击者伪造 Deauthentication 或 Disassociation 断开站点连接，并伪装成合法 ASUE 继续与合法 AE 会话。这里有两种可能性需要考虑：(1)如果会话只允许攻击者接收分组，这似乎成了监听攻击，此种情况可利用数据加密机制来防止；(2)如果会话需要攻击者拦截，则攻击者必须得到鉴别信息，譬如 USK 和 MSK，才能接收业务。尽管如此，会话劫持比监听和 DoS 攻击更具危害性。

维普资讯 http://www.cqvip.com

若没有采用证书鉴别机制，在无线局域网中可能存在第6种攻击，攻击者与ASUE和AE分别建立两个独立的连接实施MitM攻击。首先，攻击者伪造Deauthentication，断开合法ASUE与合法AE之间的连接，接着合法ASUE会进行数次重试，之后扫描到一个新AE，并最终与该恶意AE关联，合法AE和恶意AE有可能工作于不同信道，最后，攻击者伪装成合法ASUE关联到合法AE。然而当WAPI采用强壮的双向鉴别机制，由于攻击者没有合法身份，不能与ASUE或AE完成鉴别。当然攻击者可在AE和ASUE之间转发身份，但由于鉴别分组不能篡改或重放，攻击者只能扮演中继角色，其所造成的危害与监听攻击相当。但若没有采用双向鉴别机制，譬如单向鉴别，则攻击者可以通过扮演中继角色引入MitM并获得BK，就像IEEE 802.11i那样，当IEEE 802.1x鉴别为单向时，将引入MitM攻击。

最严重的危害就是在WAPISA建立的任何阶段，甚至在阶段6中，攻击者均可随时通过伪造Deauthentication或Disassociation断开站点连接，中止WAPISA，引起第7种攻击，DoS攻击。因此最好的防御措施就是在这两种帧中携带鉴别消息，只有鉴别消息验证通过，收方才作出响应，解除连接，否则认为是一种攻击，丢弃该管理帧，不予任何响应。

4 失败恢复方案

WAPI与诸多协议相似，在协议设计时更多强调的是安全性，而没有充分考虑方案的可用性，一旦与安全有关的事件或消息超时发生时，就可能建议解除串路验证或解除关联，使WAPISA恢复到阶段1之前的状态。这种措施虽然减少了信息泄漏，防止了进一步的恶意攻击，但却增加了潜在的DoS攻击。因此当认为DoS攻击为一严重问题时，就应重新考虑失败恢复方案的设计，而不应一律从头重新开始。

当然，较好的失败恢复方案也不可能从根本上避免DoS攻击，但却能使协议变得更为有效，并使得攻击者引入DoS攻击变得更加困难。例如，对于组播密钥通告过程，超时将使AE解除与ASUE的关联或串路验证，ASUE与同一AE重新关联或扫描其他AE，这将花费较长的时间；而且只有当对所有的ASUE均完成组播密钥通告过程后，AE才安装MSK，因此某一ASUE的重新关联势必将影响到其他所有的ASUE。可见，协议失败时简单地采用解除串路验证或解除关联的处理方法并非最佳，可考虑采用其他办法，如从最近点恢复，即此时AE和ASUE仅仅重试组播密钥通告过程或单播密钥协商过程，则它们很有可能很快继续连接。但是任何措施并非都是绝对的，若组播密钥通告超时恰恰就是由于ASUE不可用，譬如已经移出AE的覆盖范围，重试组播密钥通告过程或单播密钥协商过程将比直接解除与当前AE的关联并重新关联到别的AE花费更多的时间。

协议失败恢复方案可认为是在一种恶意环境下对信任关系的恢复过程。若协议从头重新开始，则将易遭受所谓的“防御性DoS攻击(defensive DoS attack)”；相反，若协议从最近处恢复，攻击者将没有足够的时间构造“防御性DoS攻击”，然而协议却易遭受到另一种类型的DoS攻击，称为“俘获的DoS攻击(captured DoS attack)”。因此协议恢复点的选择依赖于网络现象的假定与攻击者的能力。

在WAPISA建立过程中，由于阶段3证书鉴别过程难以伪造，AE和ASUE之间的握手协议位于证书鉴别之后，若密钥管理协议失败，则为了提高协议的效率，恢复点应选在最近处，因为阶段3已经保证了参与通信的两个实体是合法的。反之，若AE和ASUE尚未完成证书鉴别，则协议失败最好从头重新开始恢复。当然，在高速移动的环境下，由于实体不可用，失败会更频繁地发生，因此从最近处恢复将浪费更多的时间，但是，在阶段3不存在的前提下，信道扫描远比协议执行时间更长，从最近处恢复相比从头恢复不会带来太多的延时。因此，实现者必须根据网络的当时状况进行权衡，采取比较合理的措施。

5 WAPI可用性实施方案

基于上述分析，针对可用性，笔者提出了改进WAPI协议的实施方案。图3原始未考虑可用性的WAPI方案，图4示为改进的WAPI协议的可用性实施方案。

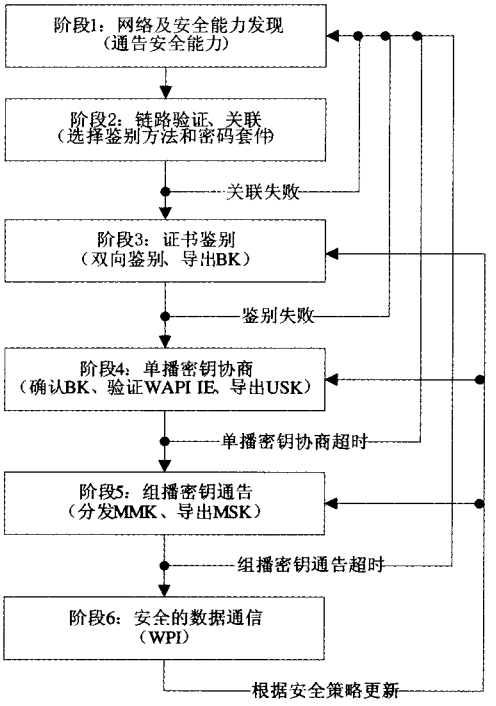

图3 未考虑可用性的WAPI实施方案

相比原方案，对WAPI协议基于可用性考虑的实施方案描述如下：

(1)在阶段2中删除串路验证过程，只保留关联过程，使协议更为简洁。这是因为目前的串路验证仅为开放系统串路验证，不提供任何安全性，仅为了后向兼容。

(2)在证书鉴别过程中增加对WAPI IE的验证功能，使攻击造成的危害降低到最低程度。基本的WAPI协议是在阶段4进行WAPI IE的验证，若攻击者伪造或篡改阶段1或2的WAPI IE，验证不通过将引起前4个阶段协议失败，因此在阶段3的接入鉴别请求和接入鉴别响应中增加该字段的验证过程，将使资源的浪费降低到最小。文[3]针对IEEE 802.11i，提出可利用IEEE 802.1x鉴别完全取代ISO/IEC 8802-11实体的串路验证，即交换阶段2和阶段3，关联在鉴别之后执行。但该方法在此处并不适用，若证书鉴别直接取代串路验证，将无法完成鉴别方法和密码套件的自动协商。

(3)WAPI IE验证条件放宽。不论在证书鉴别过程还是在单播密钥协商过程进行WAPI IE字段的验证，应放宽验证的条件，即仅验证其中的关键字段，非关键字段不予识别，以

(下转第102页)

维普资讯 http://www.cqvip.com

4.3 结果分析

由矩阵 M_{AB} 可以看出，Otway-Rees 协议中主体 A 和 B 并没有对 S 分配的会话密钥 K 达成一致，从而导致了协议的失败。为什么会出现这样的结果呢？通过参数一致性矩阵 M_{AB} 的生成过程可以得到说明，由 M_{AS} 可知主体 A 和 S 在密钥 K 上达成一致，也就是说 A 能够确认 K 是 S 为 A 和 B 分配的会话密钥；而由 M_{SB} 可知主体 S 和 B 并没有在密钥 K 上取得一致，也就是说 S 不能确认 B 是否收到了会话密钥 K，正因如此，才使得主体 A 和 B 对 K 不能达成一致造成协议失败。

通过对协议失败原因的分析，为我们提供了两种改进协议的思路：(1)使主体 B 和 S 在参数 K 上也能够达成一致；(2)在 A 和 B 之间提供直接的认证测试组件，使主体 A 和 B 在密钥 K 和其他关键参数上直接达成一致。

总结 认证测试技术的出现，使安全协议的分析过程变得更为简捷与直观。本文使用认证测试技术结合参数一致性矩阵，对安全协议的一致性进行了更为深入的分析，从而揭示了协议失败的原因，并针对这些原因给出相应改进的思路。对那些在协议中没有直接提供认证测试的主体来说，通过矩阵运算的方法实现间接认证，由于过程更为形式化使得对协议的分析更容易实现自动化。

参 考 文 献

1 Guttman JD, Fàbrega FJT. Authentication tests and the structure of bundles. Theoretical Computer Science, 2002, 283(2): 333～380

2 Guttman JD. Security protocol design via authentication tests. In: Proc. of the 2002 IEEE Computer Society Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2002. 92～103

3 Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct[A]? In: Proceedings of the 1998 IEEE Symposium on Security and Privacy[C]. Los Alamitos: IEEE Computer Society Press, 1998. 160～171

4 Thayer FJ, Herzog JC, Guttman JD. Honest ideals on strand spaces[A]. In: Proceedings of the 1998 IEEE Computer Security Foundations Workshop[C]. Los Alamitos: IEEE Computer Society Press, 1998. 66～77

5 Burrows M, Abadi M, Needham R. A logic of Authentication[J]. ACM Transactions on Computer systems, 1990(8): 18～36

6 YANG Ming, LUO Jun-Zhou. Analusis of Security rotocols Based on Authentication Test. Journal of Software, 2006, 17(1): 148～156

(上接第 87 页)

进一步降低污染 WAPI IE 造成的危害。

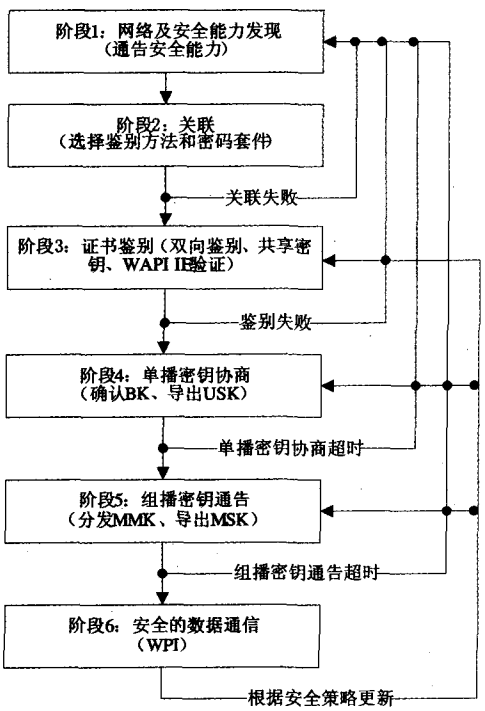

图 4 WAPI 的可用性实施方案

(4)采用合适的失败恢复方案提高整个协议的效率。在低速移动的无线网络中，若证书鉴别已成功完成，则协议失败应从最近处恢复；反之，将从头开始恢复。在高速移动的无线网络中，则协议失败从头恢复较好。因此，改进后的协议失败恢复点要比原始方案多出一些。

(5)为了提高安全性，尽可能对管理帧进行鉴别。一旦成功完成了鉴别过程，导出的共享基密钥可用于鉴别后续的管理帧，特别是 Deauthentication 和 Disassociation。这种方法可避免对多数管理帧的攻击，除 WAPISA 建立之前的管理帧由于共享密钥尚未得到而未被鉴别外。

(6)AE 和 ASUE 端口打开后，WAPI 协议数据以明文方式传输。在 IEEE 802.11i 中，4 步握手完成后，IEEE 802.1x 鉴别与密钥管理协议数据以密文形式传输，即受 WEP、TKIP 或者 CCMP 的保护。当 ASUE 收到消息 3 发出消息 4 后，将受控端口打开(Unblocked)，而 AE 由于无线丢包的原因未收到消息 4，则 AE 端的受控端口的状态仍为关闭(Blocked)。此时 AE 超时重传明文的消息 3 时，ASUE 端因只能接受加密的协议数据而收不到消息 3，从而造成此次 4 步握手协议失败。众所周知，无线的丢包率较高，那么 4 步握手协议的失败率也就不言而喻，这是 IEEE 802.11i 中 4 步握手协议存在的一大瑕疵。为了避免这种现象，在 WAPISA 中，AE 和 ASUE 的端口不论是否打开，WAPI 协议数据均以明文传输。

通过上述措施，WAPI 改进方案可避免有可能遭受的脆弱性，使得协议更加实用，提高执行效率。

结束语 WAPI 是为了解决无线局域网国际标准中的安全漏洞而设计的安全增强协议，主要保护无线网络中数据传输的机密性、完整性、鉴别性，同时对请求接入网络的用户进行身份鉴别和访问控制，保障合法的用户安全接入并安全访问合法的网络。笔者从协议的可用性角度分析了管理帧面临的各种攻击，并定义了一些防范措施，为 WAPI 协议的更好实施提供建议。但由于无线串路的脆弱性，DoS 攻击总能通过频率阻塞、网络阻塞及其他手段存在，因此这里给出的 WAPI 可用方案能有效地防御串路层的 DoS 攻击，并不能避免所有脆弱性。

参 考 文 献

1 黄振海，郭宏，王育民，等. GB15629.11-2003/XG1-2006《信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分：无线局域网媒体访问控制和物理层规范》. 中国标准出版社，2003

2 赖晓龙，曹军，铁满霞，等. GB15629.11-2003/XG1-2006《信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分：无线局域网媒体访问控制和物理层规范第 1 号修改单》. 中国标准出版社，2006

3 He Changhua, Mitchell J C. Security Analysis and Improvements for IEEE 802.11i. In: Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS05), 2005

4 Canetti R, Krawczyk H. Analysis of Key exchange Protocol and Their Use for Building Secure Channels[A]. In: Proceeding of Eurocrypt 2001: LNCS 2 045[C]. Berlin: Springer 2 Verlag, 2001. 453～474

5 AusCERT AA-2004.02. Denial of Service vulnerability in IEEE 802.11 wireless devices. May 13, 2004. http://www.auscert.org.au/render.html?it=4091

6 IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements. ANSI/IEEE Std 802.11i, 2004-6-24

7 IEEE Computer Society LAN MAN Standards Committee. Port-based Network Access Control. ANSI/IEEE Std 802.1x, 2004-11-15