第 42 卷 第 6A 期
2015 年 6 月

计 算 机 科 学
Computer Science

Vol. 42 No. 6A
June 2015

一种增强型 WAI 证书鉴别过程

肖跃雷 朱志祥 张 勇

(西安邮电大学物联网与两化融合研究院 西安 710061) (陕西省信息化工程研究院 西安 710075)

摘 要 在现有 WAI 证书鉴别过程的基础上提出了一种增强型 WAI 证书鉴别过程,它除了实现现有 WAI 证书鉴别过程的功能外,还可以建立站(STA)与鉴别服务单元(ASU)之间的安全通道,以及接入点(AP)与 ASU 之间的安全通道,从而能很好地支撑可信连接架构(TCA)的平台认证。此外,利用串空间模型(SSM)证明了该增强型 WAI 证书鉴别过程是安全的,并指出了它与现有 WAI 证书鉴别过程是向后兼容的。

关键词 WAI,证书鉴别过程,串空间模型,向后兼容

中图法分类号 TP393.08 文献标识码 A

Enhanced WAI Certificate Authentication Process

XIAO Yue-lei ZHU Zhi-xiang ZHANG Yong

(Institute of IOT and IT-based Industrialization, Xi'an University of Posts & Telecommunications, Xi'an 710061, China)

(Shaanxi Provincial Information Engineering Research Institute, Xi'an 710075, China)

Abstract Based on the existing WAI certificate authentication process, an enhanced WAI certificate authentication process was proposed. Besides implementing the function of the existing WAI certificate authentication process, it can establish a secure channel between the Station(STA) and the authentication service unit(ASU), and a secure channel between the access point(AP) and the ASU, supporting the platform-authentication of the trusted connect architecture (TCA) well. Moreover, this enhanced WAI certificate authentication process was proved securely by using the strand space model(SSM) and we pointed out backward compatibility with the existing WAI certificate authentication process.

Keywords WAI, Certificate authentication process, Strand space model, Backward compatibility

1 引言

WAPI 是中国 WLAN 标准中的安全机制[1-3],它由 WAI 和 WPI 两部分构成。前者实现站(Station, STA)和接入点(Access Point, AP)之间,或者对等 STA 之间的鉴别及密钥协商,后者是在 WAI 的基础上为 STA 和 AP(或对等 STA)之间的数据通信提供安全保证。WAI 由证书鉴别过程、单播密钥协商过程和组播密钥协商过程组成,且已经被证明是安全的[4,5],其中 WAI 证书鉴别过程实现 STA 和 AP(或对等 STA)之间的鉴别并协商 STA 和 AP(或对等 STA)之间的基密钥,以及实现 STA 和 AP(或对等 STA)的证书验证。

近年来随着可信计算技术的产生和发展,使得可信计算技术不仅可以建立终端的可信计算环境,而且可以将终端的可信计算环境扩展至网络,使网络成为一个可信计算环境,从而从源头上遏制住恶意攻击,有效解决日渐突出和复杂的网络安全问题。可信网络连接的目标就是将终端的可信计算环境扩展至网络,它包括用户认证和平台认证,其中平台认证包括平台身份认证和平台完整性验证[6]。为了实现可信网络连接,文献[7]提出了一种基于虎符三元对等鉴别(Tri-element Peer Authentication, TePA)[8]的可信网络连接架构,简称为可信连接架构(Trusted Connect Architecture, TCA)。通过对 TCA 实现的分析可知,现有 WAI 证书鉴别过程不能很好地支撑 TCA 的平台认证。

为了解决这一问题,本文提出了一种增强型 WAI 证书鉴别过程。该增强型 WAI 证书鉴别过程除了实现现有 WAI 证书鉴别过程的功能外,还建立了 STA 与鉴别服务单元(Authentication Service Unit, ASU)之间的安全通道,以及 AP 与 ASU 之间的安全通道,从而能够很好地支撑 TCA 的平台认证。此外,本文证明了该增强型 WAI 证书鉴别过程在串空间模型[9,10]下是安全的,并指出了它与现有 WAI 证书鉴别过程是向后兼容的。

2 TCA 实现分析

TCA 是我国可信网络连接国家标准中定义的一种可信网络连接架构,如图 1 所示。

在图 1 中,需要执行基于虎符 TePA 的用户认证协议和平台认证协议来实现访问请求者和访问控制器之间的双向用户认证和平台认证,其中策略管理器集中实现用户身份证书验证、平台身份证书验证和平台完整性验证。也就是说,在 TCA 的双向平台认证过程中,访问请求者和访问控制器需要

本文受国家自然科学基金项目(61402367),陕西省信息化技术研究项目(2013-008),西安邮电大学青年教师科研基金项目(401-1201)资助。

肖跃雷(1979—),男,博士,讲师,主要研究方向为可信计算、安全协议分析与设计、无线网络安全,E-mail:xiao-yuelei@163.com;朱志祥(1959—),男,博士,教授,主要研究方向为计算机网络、多媒体通信、信息化应用和网络安全;张 勇(1974—),男,博士,高级工程师,主要研究方向为信息安全、云计算与存储技术。

将自己的平台配置信息发送给策略管理器进行集中验证。由于平台配置信息涉及平台配置隐私，因此需要对访问请求者和访问控制器所发送的平台配置信息进行安全保护，否则攻击者获知这些平台配置信息后便可以分析平台漏洞，从而很容易地实现对平台的攻击。为了支撑 TCA 的平台认证，TCA 的用户认证协议要求如下：

(1)如果访问控制器还没有和策略管理器建立它们之间的安全通道，那么 TCA 的用户认证协议除了需要建立访问请求者和访问请求者之间的共享密钥(扩展后保护它们之间的通信数据)外，还需要建立访问请求者和策略管理器之间的安全通道(保护访问请求者的平台配置信息)，以及访问控制器和策略管理器之间的安全通道(保护访问控制器的平台配置信息)；

(2)如果访问控制器已经和策略管理器建立了它们之间的安全通道，那么 TCA 的用户认证协议除了需要建立访问请求者和访问请求者之间的共享密钥(扩展后保护它们之间的通信数据)外，仅需要建立访问请求者和策略管理器之间的安全通道。

对于(1)，需要执行 3 次 WAI 证书鉴别过程和 2 次单播密钥协商过程才能满足，对于(2)，需要执行 2 次 WAI 证书鉴别过程和 1 次单播密钥协商过程才能满足。因此，现有 WAI 证书鉴别过程不能很好地支撑 TCA 的平台认证。

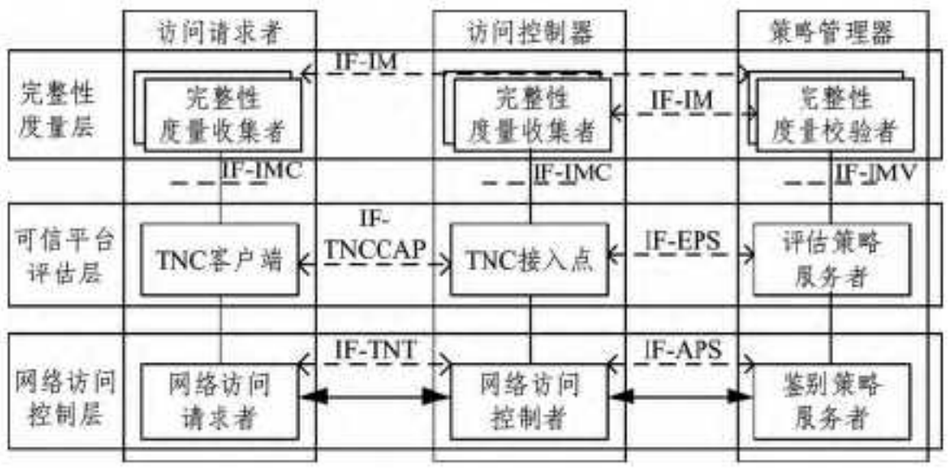

图 1 TCA

3 增强型 WAI 证书鉴别过程

在增强型 WAI 证书鉴别过程中，鉴别请求者实体(Authentication Service Unit Entity，ASUE)驻留在 STA 中，鉴别器实体(Authentication Entity，AE)驻留在 AP 或 STA 中，ASUE 和 AE 信任相同的 ASU。令 $flag_1$ 和 $flag_2$ 分别为两个 8 比特标识信息。对于 $flag_1$，若比特 0 的值为 1，则表示 ASUE 需要利用 ASU 验证对方的证书或 AE 需要利用 ASU 验证对方的证书，否则表示 ASUE 不需要利用 ASU 验证对方的证书且 AE 不需要利用 ASU 验证对方的证书；若比特 1 的值为 1，则表示 ASUE 需要建立与 ASU 之间的安全通道，否则表示不需要；若比特 2 的值为 1，则表示 AE 需要建立与 ASU 之间的安全通道，否则表示不需要。对于 $flag_2$，若比特 0 的值为 1，则表示是 BK 更新，否则表示不是 BK 更新；若比特 1 的值为 1，则表示是预鉴别，否则表示不是预鉴别；若比特 2 的值为 1，则表示 ASUE 需要利用 ASU 验证对方的证书，否则表示不需要；若比特 3 的值为 1，则表示存在可选字段，否则表示不存在；若比特 7 的值为 1，则表示 ASUE 需要建立与 ASU 之间的安全通道，否则表示不需要。值得注意的是：ASUE 和 AE 需要利用信标帧或探询响应帧，或在关联过程中协商 ASUE 是否需要建立与 ASU 之间的安全通道。增强型 WAI 证书鉴别过程的具体步骤如下：

(1)当 STA 关联或重新关联至 AP 或 STA，ASUE 和 AE 选择采用证书鉴别及密钥管理方法，或 AE 收到 ASUE 的预鉴别请求时，若 ASUE 需要建立与 ASU 之间的安全通道，或 AE 需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_1 = flag_1 \| ECDH_{params}$，其中 $ECDH_{params}$ 为 AE 选择的 ECDH 参数，否则 AE 向 ASUE 发送 $m_3 = flag_2 \| A_{id} \| ID_{asu} \| Cert_{ae} \| ECDH_{params}$，其中 A_{id} 为鉴别标识且为 AE 产生的一个随机数，ID_{asu} 标识 AE 信任的 ASU，$Cert_{ae}$ 为 AE 所驻留的 AP 或 STA 的证书。

(2)ASU 收到 AE 发送的 m_1 后，向 AE 发送 $m_2 = flag_1 \| ECDH_{params} \| N_{asu} \| WIE_{asu}$，其中 N_{asu} 为 ASU 产生的一个随机数，WIE_{asu} 为 ASU 选择的 WAPI 信息元素(包含 ASU 所支持的密码套件列表)。

(3)AE 收到 ASU 发送的 m_2 后，若 ASUE 不需要建立与 ASU 之间的安全通道，则 AE 向 ASUE 发送 $m_3 = flag_2 \| A_{id} \| ID_{asu} \| Cert_{ae} \| ECDH_{params}$，否则向 ASUE 发送 $m_3 = flag_2 \| A_{id} \| ID_{asu} \| Cert_{ae} \| ECDH_{params} \| N_{asu} \| WIE_{asu}$。

(4)ASUE 收到 AE 发送的 m_3 后，若 ASUE 不需要建立与 ASU 之间的安全通道，则 ASUE 向 AE 发送 $m_4 = flag_2 \| A_{id} \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params} \| IDs_{asu} \| \sigma_{asue}$，其中 N_{asue} 为 ASUE 产生的一个随机数，$x \cdot P$ 为 ASUE 产生的用于 ECDH 交换的临时公钥，ID_{ae} 标识 AE 所驻留的 AP 或 STA，$Cert_{asue}$ 为 ASUE 所驻留的 STA 的证书，IDs_{asu} 标识 ASUE 信任的一个或多个 ASU 且 IDs_{asu} 仅包含 ID_{asu}，σ_{asue} 为 ASUE 利用 sk_{asue} 对 m_4 中除本字段之外所有字段的签名，sk_{asue} 为 ASUE 所驻留的 STA 的私钥；否则，ASUE 向 AE 发送 $m_4 = flag_2 \| A_{id} \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}$，其中 $WIE_{asue\text{-}asu}$ 为 ASUE 选择的 WAPI 信息元素(包含 ASUE 选择的用于 ASUE 和 ASU 之间的一种密码套件)，$\sigma_{asue,2}$ 为 ASUE 利用 sk_{asue} 对 $x \cdot P$ 的签名。

(5)AE 收到 ASUE 发送的 m_4 后，若 ASUE 需要利用 ASU 验证对方的证书或 AE 需要利用 ASU 验证对方的证书，则 AE 执行步骤(i)，否则执行步骤(ii)。

(i)若 ASUE 不需要建立与 ASU 之间的安全通道，且 AE 不需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu}$，其中 $ADDID$ 为 ASUE 所驻留的 STA 的 MAC 地址与 AE 所驻留的 STA 或 AP 的 MAC 地址的级联值，N_{ae} 为 AE 产生的一个随机数。若 ASUE 不需要建立与 ASU 之间的安全通道，且 AE 需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{ae\text{-}asu} \| y \cdot P \| \sigma_{ae}$，其中 $WIE_{ae\text{-}asu}$ 为 AE 选择的 WAPI 信息元素(包含 AE 选择的用于 AE 和 ASU 之间的一种密码套件)，$y \cdot P$ 为 AE 产生的用于 ECDH 交换的临时公钥，σ_{ae} 为 AE 利用 sk_{ae} 对 $y \cdot P$ 的签名，sk_{ae} 为 AE 所驻留的 STA 或 AP 的私钥。若 ASUE 需要建立与 ASU 之间的安全通道，且 AE 不需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2}$。若 ASUE 需要建立与 ASU 之间的安全通道，且 AE 需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2} \|$

$WIE_{ae\text{-}asu} \| y \cdot P \| \sigma_{ae}$。

(ii)若 ASUE 不需要建立与 ASU 之间的安全通道,且 AE 不需要建立与 ASU 之间的安全通道,则 AE 首先本地验证 $Cert_{asue}$,若 $Cert_{asue}$ 为有效,则设定接入结果 $access$ 为成功,并计算 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$ 和 $A_{id} = hash(A_{seed})$,否则设定 $access$ 为不成功,然向后 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| \sigma_{ae,2}$,其中 $\sigma_{ae,2}$ 为 AE 利用 sk_{ae} 对 m_7 中除本字段之外所有字段的签名。若 ASUE 不需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 AE 本地验证 $Cert_{asue}$,若 $Cert_{asue}$ 为有效,则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| Cert_{ae} \| WIE_{ae\text{-}asu} \| y \cdot P \| \sigma_{ae}$,否则首先设定 $access$ 为不成功,然向后 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| \sigma_{ae,2}$。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 不需要建立与 ASU 之间的安全通道,则 AE 本地验证 $Cert_{asue}$,若 $Cert_{asue}$ 为有效,则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2}$,否则首先设定 $access$ 为不成功,然向后 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 AE 本地验证 $Cert_{asue}$,若 $Cert_{asue}$ 为有效,则 AE 向 ASU 发送 $m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2} \| WIE_{ae\text{-}asu} \| y \cdot P \| \sigma_{ae}$,否则首先设定 $access$ 为不成功,然向后 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$。如果 m_7 中的 $access$ 为不成功,则 AE 设置 m_7 中的 N_{ae}、$y \cdot P$、$z \cdot P$、$\sigma_{asu,2}$ 和 $MAC_{asu\text{-}asue}$ 为任意值。

(6)ASU 收到 AE 发送的 m_5 后,若 ASUE 需要利用 ASU 验证对方的证书或 AE 需要利用 ASU 验证对方的证书,则执行步骤(i),否则执行步骤(ii)。

(i)若 ASUE 不需要建立与 ASU 之间的安全通道,且 AE 不需要建立与 ASU 之间的安全通道,则 ASU 向 AE 发送 $m_6 = flag_1 \| ADDID \| Res_{cert} \| \sigma_{asu}$,其中 Res_{cert} 为证书的验证结果,σ_{asu} 为 ASU 利用 sk_{asu} 对 Res_{cert} 的签名,sk_{asu} 为 ASU 的私钥。若 ASUE 不需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 ASU 向 AE 发送 $m_6 = flag_1 \| ADDID \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}ae}$,其中 $z \cdot P$ 为 ASU 产生的用于 ECDH 交换的临时公钥,$\sigma_{asu,2}$ 为 ASU 利用 sk_{asu} 对 $z \cdot P$ 的签名,$MAC_{asu\text{-}ae}$ 为 ASU 产生的一个消息鉴别码且 $MAC_{asu\text{-}ae} = hash(K_2, m_1 \| m_2 \| m_5 \| m_6')$,$K_2 = hash(y \cdot z \cdot P, N_{ae} \| N_{asu} \| str)$,$m_6'$ 为 m_6 中除 $MAC_{asu\text{-}ae}$ 之外的所有字段。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 不需要建立与 ASU 之间的安全通道,则 ASU 向 AE 发送 $m_6 = flag_1 \| ADDID \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue}$,$MAC_{asu\text{-}asue}$ 为 ASU 产生的一个消息鉴别码且 $MAC_{asu\text{-}asue} = hash(K_1, WIE_{asu} \| N_{asu} \| WIE_{asue\text{-}asu} \| N_{asue} \| Cert_{asue} \| x \cdot P \| \sigma_{asue,2} \| z \cdot P \| \sigma_{asu,2})$,$K_1 = hash(x \cdot z \cdot P, N_{asue} \| N_{asu} \| str)$。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 AE 向 ASU 发送 $m_6 = flag_1 \| ADDID \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| MAC_{asu\text{-}ae}$。

(ii)若 ASUE 不需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 ASU 向 AE 发送 $m_6 = flag_1 \| ADDID \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}ae}$。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 不需要建立与 ASU 之间的安全通道,则 ASU 向 AE 发送 $m_6 = flag_1 \| ADDID \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue}$。若 ASUE 需要建立与 ASU 之间的安全通道,且 AE 需要建立与 ASU 之间的安全通道,则 AE 向 ASU 发送 $m_6 = flag_1 \| ADDID \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| MAC_{asu\text{-}ae}$。

(7)AE 收到 ASU 发送的 m_6 后,若 ASUE 需要利用 ASU 验证对方的证书或 AE 需要利用 ASU 验证对方的证书,则 AE 执行步骤(i),否则执行步骤(ii)。

(i)AE 首先利用 Res_{cert} 验证 $Cert_{asue}$,若 $Cert_{asue}$ 为有效,则设定 $access$ 为成功,并计算 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$ 和 $A_{id} = hash(A_{seed})$,否则设定 $access$ 为不成功,然后,若 ASUE 不需要建立与 ASU 之间的安全通道,则 AE 向 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| \sigma_{ae,2}$ 或 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| CRes_{cert} \| \sigma_{ae,2}$,其中 m_7 中的 $CRes_{cert}$ 仅当 ASUE 需要利用 ASU 验证对方的证书时存在,$CRes_{cert}$ 为复合的证书验证结果且 $CRes_{cert} = Res_{cert} \| \sigma_{asu}$,否则 AE 向 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$ 或 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| idea \| ID_{asue} \| CRes_{cert} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$,其中 m_7 中 $CRes_{cert}$ 仅当 ASUE 需要利用 ASU 验证对方的证书时存在。如果 m_7 中的 $access$ 为不成功且 AE 不需要建立与 ASU 之间的安全通道,则 AE 设置 m_7 中的 $y \cdot P$ 为任意值。

(ii)AE 首先设定 $access$ 为成功,然后计算 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$ 和 $A_{id} = hash(A_{seed})$,最后,若 ASUE 不需要建立与 ASU 之间的安全通道,则向 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{asue} \| ID_{asue} \| \sigma_{ae,2}$,否则向 ASUE 发送 $m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$。

(8)ASUE 收到 AE 发送的 m_7 后,若 $access$ 为不成功,则 ASUE 解除与 AE 所驻留的 STA 或 AP 的链路验证,否则:若 ASUE 需要利用 ASU 验证对方的证书,则执行步骤(i),否则执行步骤(ii)。

(i)ASUE 利用 $CRes_{cert}$ 验证 $Cert_{ae}$,若 $Cert_{ae}$ 为有效,则首先计算 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$ 和 $A_{id} = hash(A_{seed})$,然后,若 ASUE 不需要建立与 ASU 之间的安全通道,则向 AE 发送 $m_8 = flag_2 \| MAC_{asue\text{-}ae}$,否则向 AE 发送 $m_8 = flag_2 \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}$,其中 $MAC_{asue\text{-}asu}$ 为 ASUE 产生的一个消息鉴别码且 $MAC_{asue\text{-}asu} = hash(K_1, WIE_{asu} \| N_{asu} \| WIE_{asue\text{-}asu} \| N_{asue} \| Cert_{asue} \| x \cdot P \| \sigma_{asue,2} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue})$,$MAC_{asue\text{-}ae}$ 为 ASUE 产生的一个消息鉴别码且 $MAC_{asue\text{-}ae} = hash(BK, m_3 \| m_4 \| m_7 \| m_8')$,$m_8'$ 为 m_8 中除 $MAC_{asue\text{-}ae}$ 之外的所有字段。否则,ASUE 解除与 AE 所驻留的 STA 或 AP 的链路验证。

(ii)ASUE 本地验证 $Cert_{ae}$,若 $Cert_{ae}$ 为有效,则首先计算 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$ 和 $A_{id} = hash(A_{seed})$,然后,若 ASUE 不需要建立与 ASU 之间的安全通道,

则向 AE 发送 $m_8 = flag_2 \| MAC_{asue\text{-}ae}$，否则向 AE 发送 $m_8 = flag_2 \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}$。否则，ASUE 解除与 AE 所驻留的 STA 或 AP 的链路验证。

(9) AE 收到 ASUE 发送的 m_8 后，若 ASUE 不需要建立与 ASU 之间的安全通道，且 AE 需要建立与 ASU 之间的安全通道，AE 向 ASU 发送 $m_9 = flag_1 \| MAC_{ae\text{-}asu}$，其中 $MAC_{ae\text{-}asu}$ 为 AE 产生的一个消息鉴别码且 $MAC_{ae\text{-}asu} = hash(K_2, m_1 \| m_2 \| m_5 \| m_6 \| m_9')$，$m_9'$ 为 m_9 中除 $MAC_{ae\text{-}asu}$ 之外的所有字段。若 ASUE 需要建立与 ASU 之间的安全通道，且 AE 不需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_9 = flag_1 \| MAC_{asue\text{-}asu}$。若 ASUE 需要建立与 ASU 之间的安全通道，且 AE 需要建立与 ASU 之间的安全通道，则 AE 向 ASU 发送 $m_9 = flag_1 \| MAC_{asue\text{-}asu} \| MAC_{ae\text{-}asu}$。

在上述增强型 WAI 证书鉴别过程中，ASUE 和 AE 都可以发起基密钥 BK 更新，这时 A_{id} 为上一次增强型 WAI 证书鉴别过程所协商的鉴别标识，ASUE 不需要建立与 ASU 之间的安全通道，AE 不需要建立与 ASU 之间的安全通道。

当 STA 运行现有 WAI 证书鉴别过程，而 AP 运行增强型 WAI 证书鉴别过程时，AP 可以通过设置 $flag_1$ 中比特 1 和 2 的值为 0、$flag_2$ 中比特 7 的值为 0 和不接收 m_8 来实现向后兼容，这时 ASU 必须运行增强型 WAI 证书鉴别过程。当 STA 运行增强型 WAI 证书鉴别过程，而 AP 运行现有 WAI 证书鉴别过程时，STA 可以通过设置 $flag_2$ 中比特 7 的值为 0 和不发送 m_8 来实现向后兼容，这时 ASU 必须运行现有 WAI 证书鉴别过程。因此，增强型 WAI 证书鉴别过程与现有 WAI 证书鉴别过程是向后兼容的。

4 安全性分析

为了简化安全性分析，本文以一个完整的增强型 WAI 证书鉴别过程为对象进行串空间模型[9,10]分析，它涵盖了增强型 WAI 证书鉴别过程的所有情形，从而完整地实现了对增强型 WAI 证书鉴别过程的安全性分析。

定义 1　完整的增强型 WAI 证书鉴别过程的串空间 $\sum$ 为以下 4 类串的并集：(1) 发起者串 $s \in \mathrm{Init}[STA, AP, ASU, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9]$，迹为：$\langle +m_1, -m_2, +m_3, -m_4, +m_5, -m_6, +m_7, -m_8, +m_9 \rangle$，$m_1 = flag_1 \| ECDH_{params}$，$m_2 = flag_1 \| ECDH_{params} \| N_{asu} \| WIE_{asu}$，$m_3 = flag_2 \| A_{id} \| ID_{asu} \| Cert_{ae} \| ECDH_{params} \| N_{asu} \| WIE_{asu}$，$m_4 = flag_2 \| A_{id} \| N_{asue} \| x \cdot P \| idea \| Cert_{asue} \| ECDH_{params} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}$，$m_5 = flag_1 \| ADDID \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{asue-asu} \| x \cdot P \| \sigma_{asue,2} \| WIE_{ae-asu} \| y \cdot P \| \sigma_{ae}$，$m_6 = flag_1 \| ADDID \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| MAC_{asu\text{-}ae}$，$m_7 = flag_2 \| N_{asue} \| N_{ae} \| access \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| CRes_{cert} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}$，$m_8 = flag_2 \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}$，$m_9 = flag_1 \| MAC_{asue\text{-}asu} \| MAC_{ae\text{-}asu}$，与这类串相关联的主体为 AP；(2) 响应者串 $s \in Resp[STA, AP, ASU, m_3, m_4, m_7, m_8]$，迹为：$\langle -m_3, +m_4, -m_7, +m_8 \rangle$。与这类串相关联的主体为 STA；(3) 服务者串 $s \in Serv[STA, AP, ASU, m_1, m_2, m_5, m_6, m_9]$，迹为：$\langle -m_1, +m_2, -m_5, +m_6, -m_9 \rangle$。与这类串相关联的主体为 ASU；(4) 入侵者串 $s \in P$。

命题 1　假设：① $\sum$ 为完整的增强型 WAI 证书鉴别过程的串空间，C 为 $\sum$ 中含有一个发起者串 s 的丛，发起者串 s 的迹为 $Init[STA, AP, ASU, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9]$；② $sk_{asue}, sk_{asu} \notin K_P$；③ $x \cdot P, y \cdot P$ 和 $z \cdot P$ 在 $\sum$ 中是唯一产生(arise)的，且 $x \cdot P \neq y \cdot P \neq z \cdot P$。那么 C 中存在一个响应者串 $t \in Resp[STA, AP, ASU, m_3, m_4, m_7, m_8]$ 和一个服务者串 $r \in Serv[STA, AP, ASU, m_1, m_2, m_5, m_6, m_9]$。

证明：由假设①和②可知，$\sigma_{asue} \subset m_4$ 源发(originate)于一个响应者串。根据假设③和定义 1，$x \cdot P \subset \sigma_{asue}$ 唯一产生于这个响应者串。由假设①、②、③和定义 1 可知，$z \cdot P \subset \sigma_{asu,2} \subset m_6$ 唯一产生于一个服务者串。根据假设①和③，$y \cdot P$ 惟一产生于 s。因为定义 1 所指的协议满足沉默性(silent)和保守性(conservative)，因此 $x \cdot y \cdot P$ 和 $y \cdot z \cdot P$ 不源发于 C 中。由于 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$，从而 $BK \notin K_P$，因此 $MAC_{asue\text{-}ae} \subset m_8$ 源发于一个响应者串 $t \in Resp[STA, AP, ASU, m_3, m_4, m_7, m_8]$。由于 $K_2 = hash(y \cdot z \cdot P, N_{ae} \| N_{asu} \| str) \notin K_P$，因此 $MAC_{asu\text{-}ae} \subset m_6$ 源发于一个服务者串 $r \in Serv[STA, AP, ASU, m_1, m_2, m_5, m_6, m_9]$。

由命题 1 可知：AP 鉴别了 STA 和 ASU，利用 ASU 验证了 STA 的证书，建立了与 STA 之间的基密钥 BK 以及与 ASU 之间的安全通道(K_2 和 $WIE_{ae\text{-}asu}$)。

命题 2　假设：① $\sum$ 为完整的增强型 WAI 证书鉴别过程的串空间，C 为 $\sum$ 中含有一个响应者串 s 的丛，响应者串 s 的迹为 $Resp[STA, AP, ASU, m_3, m_4, m_7, m_8]$；② $sk_{ae}, sk_{asu} \notin K_P$；③ $y \cdot P$ 和 $z \cdot P$ 在 $\sum$ 中是唯一产生的，且 $y \cdot P \neq z \cdot P$。那么 C 中存在一个发起者串 $t \in Init[STA, AP, ASU, m_1', m_2', m_3', m_4', m_5', m_6', m_7, m_8', m_9']$ 和一个服务者串 $r \in Serv[STA, AP, ASU, m_1', m_2', m_5', m_6', m_9']$，其中 $m_1' = flag_1' \| ECDH_{params}'$，$m_2' = flag_1' \| ECDH_{params}' \| N_{asu} \| WIE_{asu}$，$m_3' = flag_2 \| A_{id}' \| ID_{asu} \| Cert_{ae} \| ECDH_{params}' \| N_{asu} \| WIE_{asu}$，$m_4' = flag_2 \| A_{id}' \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params}' \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}'$，$m_5' = flag_1' \| ADDID' \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2} \| WIE_{ae\text{-}asu}' \| y \cdot P \| \sigma_{ae}$，$m_6' = flag_1' \| ADDID' \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| MAC_{asu\text{-}ae}'$，$m_8' = flag_2 \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}'$，$m_9' = flag_1' \| MAC_{asue\text{-}asu} \| MAC_{ae\text{-}asu}'$。

证明：由假设①、②和定义 1 可知，$\sigma_{ae,2} \subset m_7$ 源发于一个发起者串 $t \in \mathrm{Init}[STA, AP, ASU, m_1', m_2', m_3', m_4', m_5', m_6', m_7, m_8', m_9']$。根据假设③和定义 1，$y \cdot P \subset \sigma_{ae,2}$ 唯一产生于 t。由假设①、②、③和定义 1 可知，$z \cdot P \subset \sigma_{asu,2} \subset m_7$ 唯一产生于一个服务者串。因为定义 1 所指的协议满足沉默性和保守性，因此 $y \cdot z \cdot P$ 不源发于 C 中。由于 $K_2 = hash(y \cdot z \cdot P, N_{ae} \| N_{asu} \| str) \notin K_P$，因此 $MAC_{asu\text{-}ae}' \subset m_6'$ 源发于 C 中的一个服务者串 $r \in Serv[STA, AP, ASU, m_1', m_2', m_5', m_6', m_9']$。由定义 1 可知：$m_1' = flag_1' \| ECDH_{params}'$，$m_2' = flag_1' \| ECDH_{params}' \| N_{asu} \| WIE_{asu}$，$m_3' = flag_2 \| A_{id}' \| ID_{asu} \| Cert_{ae} \| ECDH_{params}' \| N_{asu} \| WIE_{asu}$，$m_4' = flag_2 \| A_{id}' \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params}' \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}'$，$m_5' = flag_1' \| ADDID' \| N_{ae} \| N_{asue} \| Cert_{asue} \| Cert_{ae} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| x \cdot P \| \sigma_{asue,2} \| WIE_{ae\text{-}asu}' \| y \cdot P \| \sigma_{ae}$，$m_6' = flag_1' \| ADDID' \| Res_{cert} \| \sigma_{asu} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| MAC_{asu\text{-}ae}'$，$m_8' = flag_2 \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}'$，$m_9' = flag_1' \| MAC_{asue\text{-}asu} \| MAC_{ae\text{-}asu}'$。

由命题 2 可知：STA 鉴别了 AP 和 ASU，利用 ASU 验证

了 AP 的证书，建立了与 AP 之间的基密钥 BK 以及与 ASU 之间的安全通道（K_1 和 $WIE_{asue\text{-}asu}$）。在首次增强型 WAI 证书鉴别过程中，虽然攻击者可以替换 AP 发送给 STA 的 A_{id}，但是并不能形成有效攻击。因为 STA 所接收的 $ECDH_{params}$ 为可识别参数且被用于生成 STA 和 AP 之间的 BK，因此它不可能被替换。此外，虽然 AP 和 ASU 之间的某些参数不为 STA 所知，但是由于 AP 和 ASU 之间的消息不可能被替换，因此这些参数也不可能被替换。

命题 3　假设：①$\sum$为完整的增强型 WAI 证书鉴别过程的串空间，C 为$\sum$中含有一个服务者串 s 的丛，服务者串 s 的迹为 $\mathrm{Serv}[STA, AP, ASU, m_1, m_2, m_5, m_6, m_9]$；② $sk_{asue}, sk_{ae} \notin K_P$；③$x \cdot P, y \cdot P$ 和 $z \cdot P$ 在$\sum$中是唯一产生的。那么 C 中存在一个发起者串 $t \in Init[STA, AP, ASU, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9]$和一个响应者串 $r \in Resp[STA, AP, ASU, m_3, m_4, m_7, m_8]$，其中 $m_8' = flag_2' \| A_{id}' \| ID_{asu} \| Cert_{ae} \| ECDH_{params} \| N_{asu} \| WIE_{asu}$，$m_4' = flag_2' \| A_{id}' \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}'$，$m_7' = flag_2' \| N_{asue} \| N_{ae} \| access' \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| CRes_{cert} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}'$，$m_8' = flag_2' \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}'$。

证明：由假设①和②可知，$\sigma_{ae} \subset m_5$ 源发于一个发起者串。根据假设③和定义 1，$y \cdot P \subset \sigma_{ae}$ 唯一产生于这个发起者串。由假设①、②、③和定义 1 可知，$x \cdot P \subset \sigma_{asue,2} \subset m_5$ 唯一产生于一个响应者串。根据假设①和③，$z \cdot P$ 唯一产生于 s。因为定义 1 所指的协议满足沉默性和保守性，因此 $x \cdot y \cdot P$ 和 $y \cdot z \cdot P$ 不源发于 C 中。由于 $K_2 = hash(y \cdot z \cdot P, N_{ae} \| N_{asu} \| str) \notin K_P$，因此 $MAC_{ae\text{-}asu} \subset m_9$ 源发于一个发起者串 $r \in Init[STA, AP, ASU, m_1, m_2, m_3', m_4', m_5, m_6, m_7', m_8', m_9]$。由于 $BK \| A_{seed} = hash(x \cdot y \cdot P, N_{ae} \| N_{asue} \| str)$，从而 $BK \notin K_P$，因此 $MAC_{asue\text{-}ae}' \subset m_8'$ 源发于一个响应者串 $t \in Resp[STA, AP, ASU, m_3', m_4', m_7', m_8']$。由定义 1 可知：$m_3' = flag_2' \| A_{id}' \| ID_{asu} \| Cert_{ae} \| ECDH_{params} \| N_{asu} \| WIE_{asu}$，$m_4' = flag_2' \| A_{id}' \| N_{asue} \| x \cdot P \| ID_{ae} \| Cert_{asue} \| ECDH_{params} \| IDs_{asu} \| WIE_{asue\text{-}asu} \| \sigma_{asue,2} \| \sigma_{asue}'$，$m_7' = flag_2' \| N_{asue} \| N_{ae} \| access' \| x \cdot P \| y \cdot P \| ID_{ae} \| ID_{asue} \| CRes_{cert} \| z \cdot P \| \sigma_{asu,2} \| MAC_{asu\text{-}asue} \| \sigma_{ae,2}'$，$m_8' = flag_2' \| MAC_{asue\text{-}asu} \| MAC_{asue\text{-}ae}'$。

由命题 3 可知：ASU 鉴别了 STA 和 AP，验证了 STA 和 AP 的证书，建立了与 STA 之间的安全通道（K_1 和 $WIE_{asue\text{-}asu}$）以及与 AP 之间的安全通道（K_2 和 $WIE_{ae\text{-}asu}$）。虽然 STA 和 AP 之间的某些参数不为 ASU 所知，但是由于 STA 和 AP 之间的消息不可能被替换，因此这些参数也不可能被替换。

结束语　基于对 TCA 实现的分析，本文指出了现有 WAI 证书鉴别过程不能够很好地支撑 TCA 的平台认证。为了解决这一问题，本文在现有 WAI 证书鉴别过程的基础上提出了一种增强型 WAI 证书鉴别过程，它除实现 WAI 证书鉴别过程的功能外，还可以建立 STA 与 ASU 之间的安全通道，以及 AP 与 ASU 之间的安全通道，而且与现有 WAI 证书鉴别过程是向后兼容的。最后，本文通过串空间模型分析证明了该增强型 WAI 证书鉴别过程是安全的。

参 考 文 献

[1] 黄振海，郭宏，王育民，等. GB15629.11-2003 信息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[S]. 北京：中国标准出版社，2003

[2] 宽带无线 IP 工作组. GB15629.11-2003 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和 GB15629.1102-2003 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：2.4GHz 频段较高速物理层扩展规范实施指南[EB/OL]. [2006-01-10]. http://www.chinabwips.org/

[3] 赖晓龙，曹军，铁满霞，等. GB 15629.11-2003/XG1-2006 信息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[S]. 北京：中国标准出版社，2006

[4] Tang Qiang. On the security of three versions of the WAI protocol in Chinese WLAN implementation plan[C]// Proc of the second International Conference on Communications and Networking in China. Shanghai: ePrint, 2007: 333-339

[5] 铁满霞，李建东，王育民. WAPI 密钥管理协议的 PCL 证明[J]. 电子与信息学报，2009，31(2)：444-447

[6] Trusted Computing Group. TCG trusted network connect architecture for interoperability specification version 1.4[EB/OL]. [2009-05-18]. http://www.trustedcomputinggroup.org/

[7] 沈昌祥，肖跃雷，曹军，等. GB/T 29828-2013 信息安全技术 可信计算规范 可信连接架构[S]. 北京：中国标准出版社，2006

[8] ISO/IEC. ISO/IEC 9798-3:1998/Amd.1:2010 Information technology-Security techniques-Entity authentication-Part 3: Mechanisms using digital signature techniques AMENDMENT 1[S]. ISO/IEC, 2010

[9] Fabrega F J T, Herzog J C, Guttman J D. Strand space: proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2/3): 191-230

[10] Herzog J C. The Diffie-Hellman key-agreement scheme in the strand-space model[C]// Proc of the 16th IEEE Computer Security Foundations Workshop. Pacific Grove: IEEE, 2003: 234-247

(上接第 387 页)

[15] Newsome E J, Karp B, Song D. Polygraph: Automatically generating signatures for polymorphic worms[C]// Proceedings of the IEEE Symposium on Security and Privacy. May 2005: 1-6

[16] Lu S, Li Z, Qin F, et al. Bugbench: Benchmarks for evaluating bug detection tools[C]// Workshop on the Evaluation of Software Defect Detection Tools. 2005: 1-5

[17] Dixit K M. The SPEC benchmarks [J]. Parallel computing, 1991, 17(10): 1195-1209

[18] Avijit K, Gupta P. TIED, LibsafePlus: Tools for Runtime Buffer Overflow Protection[C]// Proc of 13th USENIX Security Symposium (Security'04). USENIX Association, 2004: 45-56

[19] Denning P J. The working set model for program behavior[J]. Communications of the ACM, 1968, 11(5): 323-333

[20] Han W, Ren M, Tian S, et al. Static Analysis of Format String Vulnerabilities[C]// 2011 First ACIS International Symposium on Software and Network Engineering (SSNE). IEEE, 2011: 122-127

[21] 严芬，袁赋超，等. 防御缓冲区溢出攻击的数据随机化方法[J]. 计算机科学，2011，38(1)：1-5