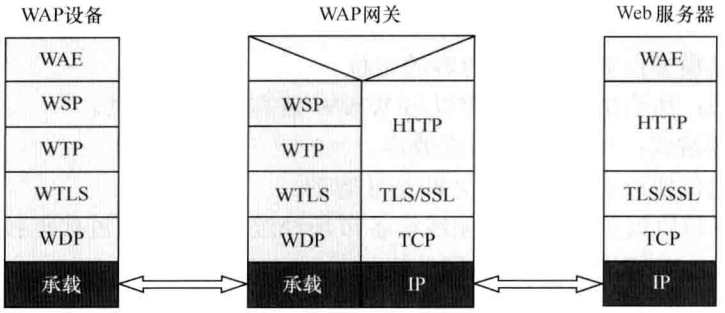

图 20-14　WAP v1.x 协议栈

WAP v2.0 的协议栈模型如图 20-15 所示。WAP v2.0 用 TLS 替换了 WTLS 协议，而且通过 TLS 协议实现了端到端的安全性。

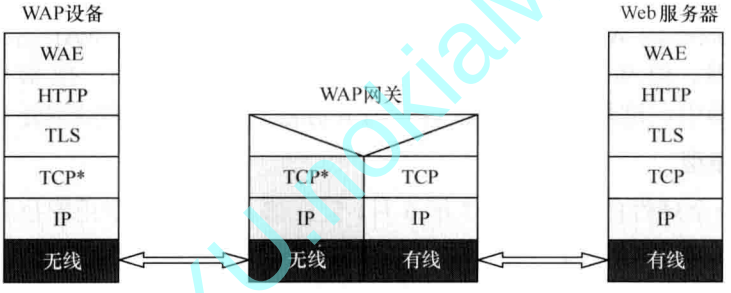

图 20-15　WAP v2.0 协议栈

20.8　S/MIME

1．简介

S/MIME 是 Secure/Multipurpose Internet Mail Extensions 的缩写，是一种 Internet 标准，在安全方面对 MIME 协议进行了扩展，它可以把 MIME 实体（如数字签名和加密信息等）封装成安全对象，为电子信息应用增添了消息真实性、完整性和保密性服务。S/MIME 不局限于电子邮件，也可以被其他支持 MIME 的传输机制使用，如 HTTP。在 S/MIME 之前，使用最广泛的电子邮件协议为简单邮件传输协议（SMTP，Simple Mail Transfer Protocol），该协议由于其内在的原因而缺乏安全性。

S/MIME v1 是由许多安全供应商于 1995 年开发出来的，只是实现邮件安全性的几个规范之一。例如，Pretty Good Privacy （PGP）是实现邮件安全性的另一个规范。在 S/MIME v1 推出时，安全邮件并没有公认的单一标准，但有几个相互竞争的标准。

1998 年，随着 S/MIME v2 的推出，情况开始发生变化。与版本 1 不同的是，出于希望成为 Internet 标准的考虑，S/MIME v2 被提交到 Internet 工程任务组（IETF）。通过这一步，S/MIME 从许多可能的标准中脱颖而出，从而成为邮件安全标准的领跑者。S/MIME 2 由两份 IETF 征求意见文档（RFC）组成：建立邮件标准的 RFC 2311 和建立证书处理标准的 RFC 2312。这两份 RFC 共同提供了第一个基于 Internet 标准的框架，供应商可以按照该框架来提出可互操作的邮件安全解决方案。有了 S/MIME 2，S/MIME 开始成为邮件安全的

标准。

1999 年，为增强 S/MIME 功能，IETF 提议使用 S/MIME 版本 3。RFC 2632 建立在 RFC 2311 基础上，指定为安全邮件的标准；RFC 2633 增强了证书处理的 RFC 2312 规范。RFC 2634 通过向 S/MIME 添加其他服务扩展了总体功能，如安全回执、三层包装和安全标签。目前，S/MIME v3 已被广泛接受为邮件安全标准，很多邮件软件产品均支持 S/MIME v3，如 Microsoft Outlook、Microsoft Exchange、Foxmail 等。

S/MIME 增加了新的 MIME 数据类型，用于提供数据保密、完整性保护、认证和鉴定服务等功能，这些数据类型包括：application/pkcs7-MIME、multipart/signed 和 application/pkcs7-signature 等。如果邮件包含了上述 MIME 复合数据，邮件中将带有有关的 MIME 附件。在邮件的客户端，接收者在阅读邮件之前，S/MIME 模块将处理这些附件。

S/MIME 只保护邮件的邮件主体，对头部信息则不进行加密，以便让邮件成功地在发送者和接收者的网关之间传递。S/MIME 提供两种安全服务：数字签名和邮件加密。

2．数字签名

（1）基本原理

数字签名提供了下列安全功能：

① 身份验证。通过签名来验证身份。它能够将该实体与其他所有实体区分开来，并证明它的唯一性，从而确认“您是谁”这个问题的答案。由于 SMTP 电子邮件中不存在身份验证，因此无法知道实际上是谁发送了邮件。数字签名中的身份验证使收件人可以知道邮件是声称已发送该邮件的那个人或组织发送的，从而解决了这一问题。

② 认可。签名的唯一性可防止签名的所有者否认签名，此功能称为“认可”。因此，签名所提供的身份验证提供了一种强制认可的手段。人们最熟悉的是书面合同上下文中认可的概念：已签名的合同是具有法律约束力的文档，要否认已通过身份验证的签名是不可能的。数字签名提供相同的功能，并且，在某些领域中，逐渐被公认为与书面签名一样具有法律约束力。由于 SMTP 电子邮件不提供身份验证手段，因此无法提供认可功能。发件人很容易否认自己是某个 SMTP 电子邮件的所有者。

③ 数据完整性。数字签名提供的另一安全服务是数据完整性。数据完整性是使数字签名成为可能的特定操作的结果。有了数据完整性服务，当经过数字签名的电子邮件的收件人验证数字签名时，他们可以确信所收到的电子邮件确实是被签名并发送出来的那封邮件，并且在传送过程中未发生改变。如果邮件在签名后的传送过程中发生了任何改变，该签名都将无效。这样，数字签名便能够提供书面签名所无法提供的保证功能，因为书面文档在经过签名后可能被改变。

虽然数字签名提供数据完整性，但不提供保密性。与 SMTP 邮件类似，仅有数字签名的邮件将以明文形式发送，并且可能被其他人阅读。如果邮件是不透明签名的邮件，则会出现一定程度的混乱局面，这是因为虽然邮件是以 Base64 编码的，但它仍然是明文形式。若要保护电子邮件的内容，必须使用邮件加密。

身份验证、认可和数据完整性是数字签名的核心功能。在它们的共同作用下，可以使收件人确信邮件来自发件人，并且所收到的邮件是所发送的邮件。

简单来说，数字签名的工作形式是在邮件发送时对电子邮件的文本执行签名操作，而

在邮件被阅读时执行验证操作，如图 20-16 所示。

图 20-16　S/MIME 数字签名服务

（2）发送邮件

发送邮件时，执行签名操作所需要的信息只能由发件人提供。在签名操作中，通过捕获电子邮件并对邮件执行签名操作来使用此信息。此操作产生实际的数字签名。然后，此签名将附加到电子邮件中，并随同邮件一起发送。邮件签名过程的具体步骤如下：

① 捕获邮件。

② 检索用来唯一标识发件人的信息。

③ 使用发件人的唯一信息对邮件执行签名操作，以产生数字签名。

④ 将数字签名附加到邮件中。

⑤ 发送邮件。

图 20-17 显示了邮件签名过程。

图 20-17　S/MIME 邮件签名过程

由于此操作需要来自发件人的唯一信息，因此数字签名提供了身份验证和认可功能。此唯一信息可以证明邮件只能来自该发件人。

（3）接收邮件

当收件人打开经过数字签名的电子邮件时，系统会对数字签名执行验证过程，并会从邮件中检索邮件所包含的数字签名。此外还会检索原始邮件，然后执行签名操作，从而产生另一个数字签名。将邮件所包含的数字签名与收件人所产生的数字签名进行比较，如果签名匹配，则证明邮件确实来自所声称的那个发件人；如果签名不匹配，则将邮件标记为无效。邮件签名验证过程的具体步骤如下：

① 接收邮件。

② 从邮件中检索数字签名。

③ 检索邮件。

④ 检索用来标识发件人的信息。

⑤ 对邮件执行签名操作。

⑥ 将邮件所附带的数字签名与收到邮件后所产生的数字签名进行比较。

⑦ 如果数字签名匹配，则说明邮件有效。

图 20-18 显示了邮件签名验证过程。

图 20-18　S/MIME 邮件验签过程

验证签名时所使用的发件人信息与对邮件进行签名时发件人所提供的信息不是同一个信息。通过这样一种方式叙述收件人使用的信息：使收件人在验证发件人的唯一信息时不必实际知道该信息，从而保护发件人的信息。

同时采用数字签名过程和数字签名验证过程可验证电子邮件发件人的身份，并确定已签名的邮件中数据的完整性。验证发件人身份会提供其他认可功能，即防止已通过身份验证的发件人声称他们未发送过该邮件。数字签名是防止假冒身份和篡改数据的解决方案，而假冒和篡改这两种情况在基于标准 SMTP 的 Internet 电子邮件中均有可能出现。

3．邮件加密

（1）基本原理

邮件加密提供了针对信息泄露的解决方案。基于 SMTP 的 Internet 电子邮件并不确保邮件的安全性。SMTP Internet 电子邮件可能被在发送过程中看到它或在所存储的位置查看它的任何人阅读，S/MIME 已通过采用加密措施解决了这些问题。

加密是一种更改信息的方式，它使信息在重新变为可读或可理解的形式之前无法阅读或理解。虽然邮件加密不像数字签名那样普遍使用，但是它确实解决了被许多人认为是 Internet 电子邮件的最重大缺陷的问题。

邮件加密提供两种特定的安全服务：

① 保密性。邮件加密用来保护电子邮件的内容。只有预期的收件人能够查看该内容，因而该内容是保密的，不会被可能收到或查看到该邮件的其他任何人知道。加密在邮件传送和存储过程中均提供保密性。

② 数据完整性。使用数字签名时，由于采用了使加密成为可能的特定操作，因此邮件加密提供了数据完整性服务。

虽然邮件加密提供保密性，但它不会以任何方式验证邮件发件人的身份。已加密但未签名的邮件与未加密的邮件一样，很容易被他人假冒为发件人。由于认可是身份验证的直接结果，因此邮件加密也不提供认可。虽然加密提供了数据完整性，但是加密的邮件可能仅显示邮件自发送以来未发生过改变，而不提供有关邮件发件人的信息。要证明发件人的身份，邮件必须使用数字签名。

保密性和数据完整性提供了邮件加密的核心功能。它们确保了只有预期的收件人才能查看邮件，并且所收到的邮件就是所发送的邮件。

邮件加密通过在发送邮件时对邮件执行加密操作来使邮件的文本不可读。收到邮件时，通过在阅读邮件时执行解密操作来使文本再次成为可读文本，如图 20-19 所示。

图 20-19　S/MIME 邮件加密服务

（2）发送邮件

加密操作在发送邮件时执行，它捕获电子邮件，并使用预期收件人所特有的信息来对邮件进行加密。加密的邮件替换了原始邮件，然后将邮件发送至收件人。邮件加密过程的具体步骤如下：

① 捕获邮件。

② 检索用来唯一标识收件人的信息。

③ 使用收件人的信息对邮件执行加密操作，以产生加密的邮件。

④ 加密的邮件替换邮件中的文本。

⑤ 发送邮件。

图 20-20 显示了电子邮件加密过程。

图 20-20　S/MIME 邮件加密过程

由于此操作需要有关收件人的唯一信息，因此邮件加密提供了保密性。只有预期的收件人具有执行解密操作所需的信息，从而确保了只有预期的收件人能够查看邮件，因为必须首先提供收件人的唯一信息，然后才能查看未加密的邮件。

加密邮件时所使用的收件人信息与解密邮件时收件人所提供的信息不是同一个信息。通过这样一种方式叙述发件人使用的信息：使发件人在使用收件人的唯一信息时不会实际知道该信息，从而保护了收件人的信息。

（3）接收邮件

当收件人打开加密邮件时，会对加密邮件执行解密操作。此时，将同时检索加密的邮件和收件人的唯一信息。然后，使用收件人的唯一信息对加密邮件执行解密操作。此操作返回未加密的邮件，然后该邮件将显示给收件人。如果邮件在传送过程中发生过改变，解密操作将失败。邮件解密过程的具体步骤如下：

① 接收邮件。

② 检索加密邮件。

③ 检索用来唯一标识收件人的信息。

④ 使用收件人的唯一信息对加密邮件执行解密操作，以产生未加密的邮件。

⑤ 将未加密的邮件返回给收件人。