电子邮件安全

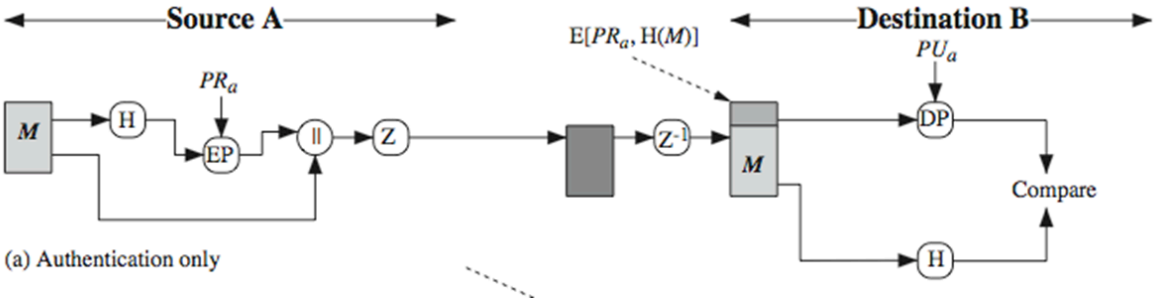
- 电子邮件的消息内容的安全隐患：
  - 在传输过程中可能被查看
  - 在邮件服务器中被特权管理员查看
- 电子邮件安全涉及多个方面
  - **保密性**：防止邮件泄露
  - **认证性**：发送方身份认证
  - **邮件完整性**：防止邮件被修改
  - **不可否认性**：防止发送方否认曾发送过邮件

PGP协议

功能

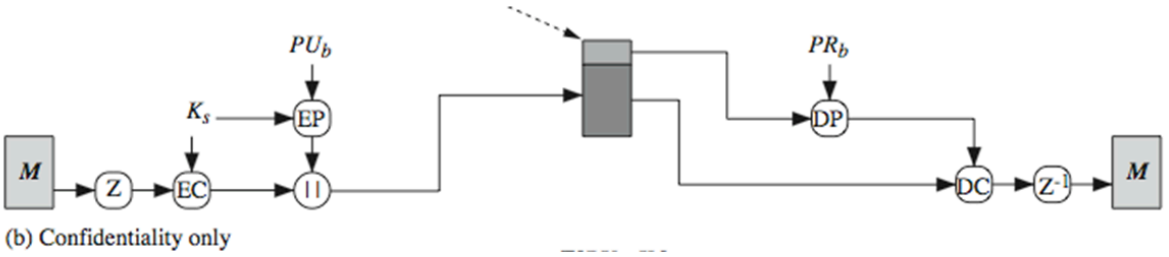
消息认证

1. 发送方准备待发送消息
2. 计算消息摘要（SHA-1160-bit）
3. 使用RSA签名消息摘要
4. 接收方使用签名算法验证消息摘要正确性
5. 接收方使用加密算法及摘要，验证消息正确性



消息保密

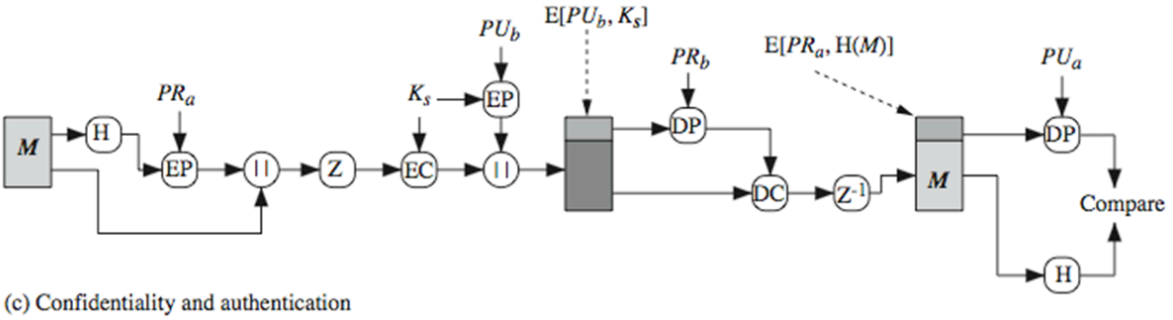
1. 发送方生成128bit随机会话密钥
2. 使用会话密钥加密消息
3. 使用RSA加密会话密钥，并附加于消息
4. 接收方先解密会话密钥
5. 接收方进而解密消息



消息认证及保密

即同时使用认证及保密功能

- 生成签名，附加于消息
- 同时加密消息、签名
- 附加会话密钥



(c) Confidentiality and authentication

压缩

- 默认情况下，PGP签名后、加密前压缩待加密消息
  - 因而，可以先存储消息，验证可以延后
  - 压缩是非确定性的
- 使用ZIP压缩算法

邮件兼容性

- 邮件发送协议仅支持文本，如何处理任意二进制数据?
- 需要转化为ASCII字符
- 使用radix-64编码算法：将3字节，映射为4个可打印的ASCII字符
- 如果消息过大，PGP也会分割消息

S/MINE协议

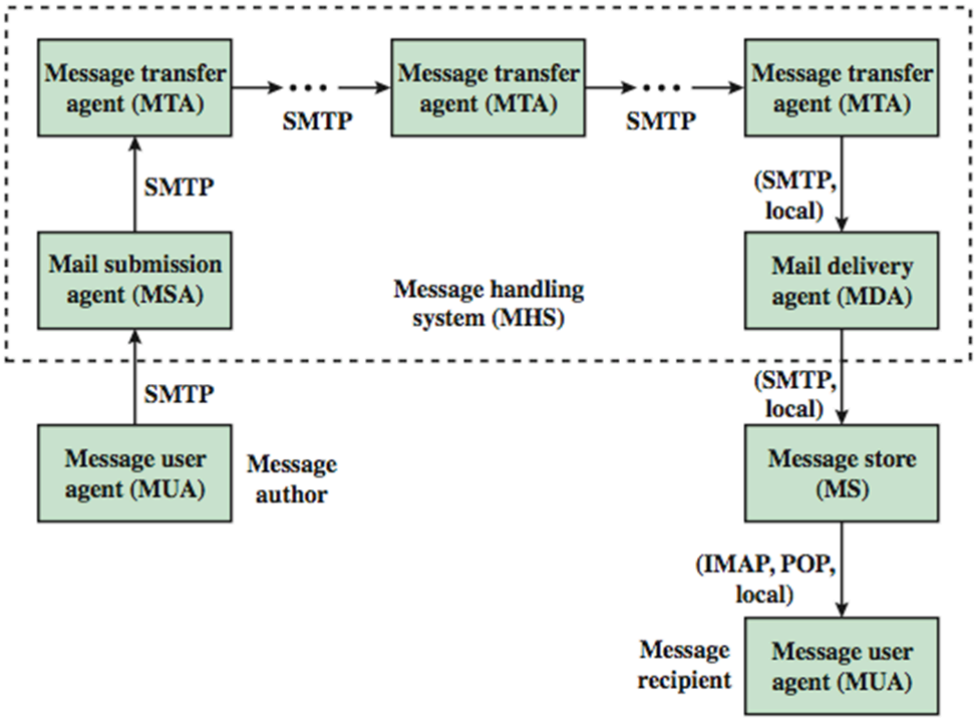
- 对MINE协议做了安全性增强：签名的接收方、安全标签和安全邮件列表
- 使用X.509v3证书

功能

- 数据保密（enveloped data）：加密内容及密钥
- 数据签名（signed data）：消息编码 + 摘要签名
- 仅签名消息（clear-signed data）：未编码消息 + 编码后摘要签名
- 数据保密及签名（signed & enveloped data）：保密及签名功能套嵌

DKIM协议

- 域名密钥识别邮件：协议描述了如何由邮件服务提供商使用密码学工具对消息进行安全保护，消息接收方对消息进行验证
- 架构


Message transfer agent (MTA)
SMTP
Message transfer agent (MTA)
SMTP
Message transfer agent (MTA)
SMTP
(SMTP, local)
Mail submission agent (MSA)
Message handling system (MHS)
Mail delivery agent (MDA)
SMTP
(SMTP, local)
Message user agent (MUA)
Message author
Message store (MS)
(IMAP, POP, local)
Message recipient
Message user agent (MUA)