Redirecting and modifying SMTP mail with TLS session renegotiation attacks

Wietse Venema
Postfix mail server project
www.postfix.org
November 8, 2009

Executive summary

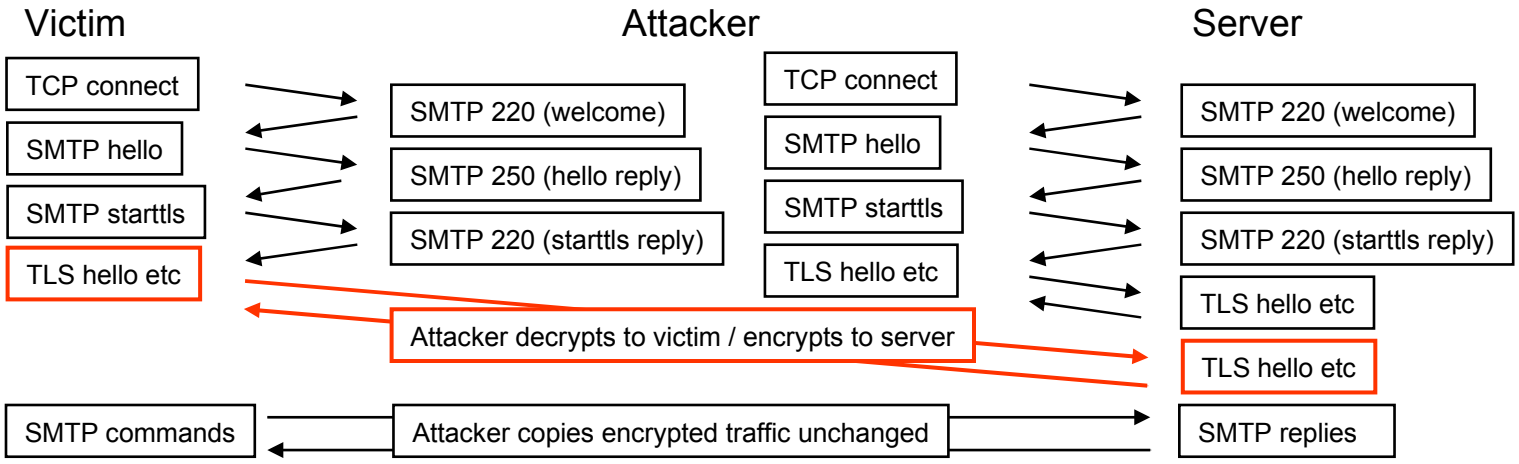
- **The setting: an attacker, a victim, and a server. The attacker sits on the network path between victim and server (ARP[1] spoofing, etc.).**
- **The TLS renegotiation attack allows the attacker to prepend data to a TLS session between the victim and server.**
  - The attack was originally discussed in the context of HTTP.
- **We present a specific attack that would allow an attacker to redirect and modify SMTP mail that is sent over a TLS session.**
- **For the server side, we show what SMTP-over-TLS implementations would be vulnerable to this attack, plus SMTP-level workarounds.**
  - We show why the Postfix SMTP server is not affected by this attack.
- **For the client side, we propose SMTP-level workarounds for several session renegotiation attacks.**

[1]Address Resolution Protocol. This translates IP addresses into e.g., ethernet hardware addresses.

Basic TLS session renegotiation for SMTP

See appendix for an example of a normal SMTP over TLS session

- **With SMTP, the attacker must initiate TLS session renegotiation.**
- **Simplest possible example: the attacker prepends no input to the victim-server session (prepending input comes next).**



- **Note: The attacker never knows the victim-server TLS session key.**

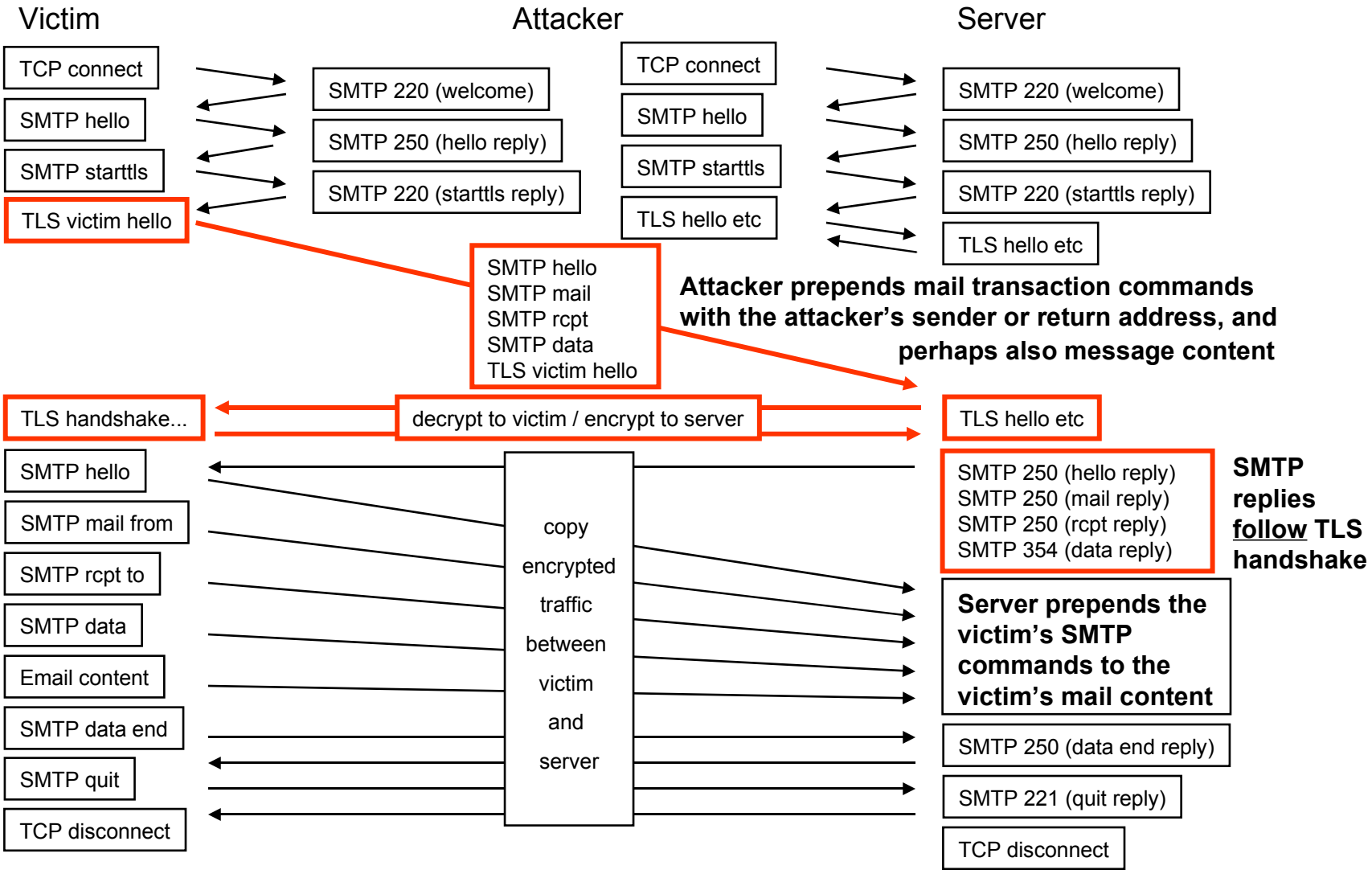
Prepending input to the victim-server session

- **Challenge: prepend input to the SMTP stream, then re-synchronize the victim and the server, so that the SMTP session does not break (or at least, does not break too early).**
  - SMTP has two command states (MAIL, other), and one major non-command state (DATA[1,2]) that recognizes no SMTP commands.
    - Many SMTP commands are valid only in specific protocol states (exceptions: NOOP, HELO, RSET, QUIT).
  - Most non-error replies are 2xx numerical codes. Most clients accept these in all but one command state (i.e. any xx will do).
    - The most common exception is the DATA command. This uses a 3xx non-error reply code.
      - 3xx Numerical replies are also used with e.g. SASL login commands.

[1]Few sites implement the BDAT command. To exploit this, the attacker needs to know precise details about the plaintext length or content of victim SMTP commands and email messages.

[2]Other non-command modes are used with e.g. SASL logins.

Redirecting or modifying SMTP mail with TLS session renegotiation



Implications of this attack

- **SMTP mail can be redirected and modified even though the server's TLS certificate provides strong assurance that the client-server channel is secure.**
  - To modify email, prepend an Internet-style email header followed by a MIME segment that hides the victim's real email message.
  - Most SMTP clients don't verify server TLS certificates. These clients are already vulnerable to ordinary man-in-the-middle attacks. Here, TLS session renegotiation introduces no new threat.
- **Renegotiation attacks affect only configurations that rely on TLS server certificate verification to secure their SMTP mail traffic.**
  - For example, email between business partners.
- **After a discussion of the attack's feasibility we discuss a number of possible workarounds.**

Servers: what makes implementations vulnerable to the SMTP mail redirection/modification attack

- **The attack requires that:**
  - The server processes the entire attacker's TCP packet with:
    - The attacker's SMTP (hello, mail, rcpt, data) commands[1].
    - The victim's TLS hello request.
  - The server negotiates a new TLS session with the victim before responding to the SMTP (hello, mail, rcpt, data) commands[2].
    - The server encrypts the SMTP (hello, mail, rcpt, data) replies under the new TLS session key, which is known only to server and victim.
- **Implementations may be vulnerable when the TLS engine processes network input before the SMTP engine requests network input.**
  - Postfix-OpenSSL does not work this way, and it is therefore not vulnerable to this attack

[1]To work around the attack, the SMTP engine could abort when the SMTP mail command arrives before the SMTP hello reply is sent, in clear violation of the SMTP protocol.

[2]To work around the attack, the SMTP engine could abort when a TLS session is renegotiated.

Servers: why the SMTP mail redirection/ modification attack fails with Postfix-OpenSSL

- **Assumption: the attacker sends one TCP packet with SMTP (hello, mail, rcpt, data) commands plus the victim's TLS hello request.**
- **The Postfix SMTP layer asks the OpenSSL layer for the next input.**
  - The OpenSSL layer has no direct access to the network socket.
  - The OpenSSL layer asks the Postfix socket layer for the next TLS record header with data byte count, and then asks for that data.
    - This TLS record contains only the attacker's SMTP commands.
    - The OpenSSL layer does not ask for more input (victim TLS hello).
- **The Postfix SMTP layer gives the SMTP (hello, mail, rcpt, data) replies to the OpenSSL layer.**
  - The attack fails because the server sends the SMTP replies before the SSL layer handles the (still unread) victim's TLS hello request.
    - The replies are not encrypted in the victim-server TLS session key.

Clients: working around the SMTP mail redirection/ modification attack

- **The attack signature:**
  - The server sends SMTP (hello, mail, rcpt, data) replies in the victim-server TLS session, before the victim has sent its own SMTP (hello, mail, rcpt, data) commands.
- **To work around the attack in the SMTP client:**
  - Send the SMTP hello command and receive the hello reply.
  - If the network input queue is non-empty, set a flag.
  - Send the SMTP mail command and receive the mail reply.
  - If there is no error, but the flag was set, then assume that the mail reply was received before the mail command was sent.

Clients: working around “partial command” attacks

- **The attacker may prepend an incomplete SMTP command that does not end in <CR><LF>, so that the victim’s first command in the TLS session is replaced with the attacker’s command. For example:**

  Attacker sends: NOOP<SPACE>

  Victim sends: EHLO client.example<CR><LF>

  Server reads: NOOP blah blah<CR><LF> (this is valid SMTP)

  Server replies: 250 2.0.0 Ok<CR><LF>

  – Unlike the NOOP reply, the real EHLO reply would have no enhanced status code (the 2.0.0 in the example). Instead, the EHLO reply would show the server’s name, and would list the server’s protocol features.

- **The SMTP client can work around this attack by sending its own NOOP command at the beginning of the TLS session, or by rejecting EHLO replies with an unexpected syntax.**

Credits

- **Wietse Venema proposed the attack to redirect or modify TLS-encrypted SMTP mail.**
- **Victor Duchovni proposed the “COMMAND<SPACE>” partial command prepend attack.**
- **Victor found that Wietse’s attack cannot work with Postfix SMTP servers that are built op top of OpenSSL, because such systems don’t use server-side read-ahead.**
- **Wietse and Victor concocted detection mechanisms and workarounds. Some may even end up in Postfix.**

Appendix: normal SMTP over TLS session

For simplicity, without ESMTP command pipelining