TLS Renegotiation Vulnerability

IETF-76
Joe Salowey
(jsalowey@cisco.com)
Eric Rescorla
(ekr@rtfm.org)
TLS Renegotiation Vulnerability

• Discovered by Marsh Ray and Steve Dispensa of PhoneFactor - 08/2009
• Re-Discovered by Martin Rex during Channel Binding Discussions on the TLS list – 11/2009
TLS Renegotiation

- Initial Handshake Establishes a protected channel
- Re-negotiation is a new handshake run under the protection of the existing channel
- Upon completion the new channel replaces the old channel
Renegotiation Attack

Client          Attacker          Server

←------ Handshake------→
←====== Initial Traffic =====→
←------------------------Handshake------------------------→
←================ Client Traffic================→

• Initial traffic and client traffic are treated as originating under the same context
• Attacker injected traffic may be processed under clients context
• Attacker injected traffic may set up context under which client’s traffic is processed
• Client handshake may use client certificates
Vulnerability

• Attacker injects data that is processed under client’s context
  – Process unauthenticated request under authenticated context
  – Attacker can inject data processed under client’s authorization based on client certificate
• Attacker sets up context that discloses information in client’s request
  – Client cert authentication not necessary for attack
• Complications
  – Renegotiation is often transparent to application
  – Client is not aware this is a renegotiation
  – Some HTTP servers support renegotiation to request client certs for a protected resource
• Other protocols may be vulnerable as well
  – IMAP, LDAP, XMPP, SIP, SMTP, …
Mitigation

• Disable renegotiation
  – May Be required by application
  – Some libraries do not have interface for this

• Proposed Extension
  – Fix TLS renegotiation

• Application Mitigation
  – Application dependent
Renegotiation Indication Extension

- draft-rescorla-tls-renegotiation-00
- Hello extension containing the contents of the finished messages from the previous handshake

```c
struct {
    opaque renegotiated_connection<0..255>;
} Renegotiation_Info;
```
Proposed Timeline for Renegotiation Extension Document

11/15 Adopt as Working Group Item
11/16 – 11/30 Working Group Last Call
12/01 – 12/04 Resolve Comments
12/04 – 12/07 Send to IESG – AD Review
12/08 – 12/22 IETF Last Call and External Review
12/22 – 01/07 Resolve Comments
01/07 – 01/14 IESG Review
01/14 – 02/14 RFC Editor and IANA Review
02/14 RFC publication
Current Open Issues

- Extension Number
- Requirements Language
  - particularly for client
- Interaction with session resumption
- Behavior on subsequent renegotiations
- Applicability of TLS extensions
- Dealing with broken extension support
- SSLv3?
- Needs Review
Follow-on Work

• Application interaction with re-negotiation
  – Identity comparison
  – API recommendations
Some References

- http://extendedsubset.com/Renegotiating_TLS.pdf