Abstract

Extensible Authentication Protocol is a generic framework supporting multiple types of authentication methods. In systems where EAP is used for authentication, it is desirable to not repeat the entire EAP exchange with another authenticator. Microsoft has developed EAP TLS which is an authentication protocol based on TLS (Transport Layer Security). Authentication server and client use TLS protocol to negotiate session key. The EAP re-authentication Protocol provides a consistent, method-independent and low-latency re-authentication. It is extension to current EAP mechanism to support intra-domain handoff authentication. This paper analyzed the security cost of EAP TLS & ERP with increased processor speed.
Analyzing EAP TLS & ERP Protocol with varying processor speed

- H. Orman, Purple Streak Dev., RFC 3766 Determining Strengths For Public Keys Used For Exchanging Symmetric Keys, April 2004
- B. Aboba, L. Blunk, J. Vollbrecht, Extensible Authentication Protocol (EAP), IETF RFC 3748 June 2004
- P. Calhoun, J. Loughney, E. Guttmann, Diameter Base Protocol, IETF RFC 3588, September 2004
- P. Eronen, Diameter Extensible Authentication Protocol Application, IETF RFC 4072, August 2005
- B. Aboba, M. Beadles, Network Access Identifier (NAI), IETF RFC4282, December 2005
- C. Kaufman, Internet Key Exchange (IKEv2) Protocol, RFC 4306, December 2005
- Kaouthar Sethom, “Requirements and Adaptation Solutions for Transparent Handover between Wifi and Bluetooth”, Mobile Computing and Communications Review, Volume 8, Number 1, pp. 61-83, San Jose State University, San Jose, CA, USA.
- M. Nakhjiri, Y. Ohba, "Derivation, delivery and management of EAP based keys for handover and re-authentication ", IETF draft
- Carolin Latze, Ulrich Ultes-Nitsche, Strong Mutual Authentication in a User-Friendly Way in EAP-TLS.
- R Housely, B. Aboba, Guidance for AAA key management, RFC 4296, July 2008

Index Terms

Computer Science

Security
Analyzing EAP TLS & ERP Protocol with varying processor speed

**Key words**

<table>
<thead>
<tr>
<th>Key word</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP</td>
<td></td>
</tr>
<tr>
<td>EAP-TLS</td>
<td></td>
</tr>
<tr>
<td>EMSK</td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td></td>
</tr>
</tbody>
</table>