Am Schloßpark 18
D-82131 Gauting

info@atmes.de

www.atmes.de

AP-Note

IPsec für SOME/IP Simulation

Einführung

SOME/IP ist eine Kommunikationsmiddleware im Automobilbereich, welche unter anderem in AUTOSAR verwendet wird. SOME/IP ist die einzige Lösung, welche seit Anfang der Adaptive Plattform beide AUTOSAR Plattformen unterstützte. Hierdurch ist SOME/IP als Middleware für Ethernet-Kommunikation im Fahrzeug sehr weit verbreitet.

Internet Protocol Security (IPsec) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. IPsec arbeitet direkt auf der Vermittlungsschicht ("Internet Layer", entspricht OSI Layer 3) des DoD Models und ist eine Weiterentwicklung der IP-Protokolle. Das Ziel ist es, eine verschlüsselungsbasierte Sicherheit auf Netzwerkebene bereitzustellen. IPsec bietet durch die verbindungslose Integrität sowie die Zugangskontrolle und Authentifikation der Daten diese Möglichkeit an. Zudem wird durch IPsec die Vertraulichkeit sowie Authentizität der Paketreihenfolge durch Verschlüsselung gewährleistet.

Im Folgenden wird beschrieben, wie eine SOME/IP Kommunikation zwischen zwei Windows Rechnern mit Hilfe von IPsec abgesichert werden kann.

Voraussetzungen

Für die Verwendung von IPsec für eine SOME/IP Simulation sind folgende Komponenten nötig:

1. strongSwan (www.strongswan.org)
2. someIpSim (www.atmes.de)

Konfiguration

Für die IPsec Konfiguration wird auf einem Rechner ein strongSwan Server benötigt. Die Konfiguration des Servers im Verzeichnis /swanctl/swanctl.conf wird in Abbildung 1: strongSwan Server Konfiguration dargestellt.

```
connections {

   host-host {
      local_addrs  = 192.168.179.21
      remote_addrs = 192.168.179.59

      local {
         auth = pubkey
         certs = ip_21.pem
         id = 192.168.179.21
      }
      remote {
         auth = pubkey
         id = CN=192.168.179.59
      }
      children {
         host-host {
            rekey_time = 5400
            rekey_bytes = 500000000
            rekey_packets = 1000000
            ah_proposals = sha1
            mode = transport

         }
      }
      version = 2
      mobike = no
      reauth_time = 10800
      proposals = aes128-sha1-modp1024
   }
}
```

Abbildung 1: strongSwan Server Konfiguration

Auf diesem Server muss auch noch das Stammzertifikat hinterlegt werden. Dies geschieht über die „Microsoft Management Console“ mit dem Aufruf „mmc“. Darin über Datei->Snap-Ins hinzufügen von „Zertifikate“ und „Computerkonto“. In dieser Ansicht wird dann unter „Vertrauenswürdige Stammzertifikate“ das Stammzertifikat für die Verbindung importiert.

Der Client Rechner muss wie folgt konfiguriert werden. Über die „Microsoft Management Console“ werden das Stammzertifikat und das eigene Zertifikat importiert. Aufruf „mmc“ siehe oben. Zusätzlich muss noch eine Firewall Verbindungssicherheitsregel über die Powershell eingetragen werden. Siehe dazu Abbildung 2.

```
#Set up the certificate
$certprop = New-NetIPsecAuthProposal -machine -cert -Authority "CN=VPN root CA 1024"
$myauth = New-NetIPsecPhase1AuthSet -DisplayName "VPN root CA 1024" -proposal $certprop

#Create the IKEv2 Connection Security rule
New-NetIPsecRule  -DisplayName "My IKEv2 Rule" -LocalAddress  "192.168.179.21" -Phase1AuthSet
$myauth.InstanceID -InboundSecurity Require -OutboundSecurity Require -KeyModule IKEv2
```

Abbildung 2: IKEv2 Verbindungssicherheitsregel

Auf manchen Windows Rechnern ist ein IPsec Dienst aktiviert. Dies kann man über „netstat -banvo“ prüfen. Wenn auf Port 500 ein Eintrag ist, ist dieser Dienst aktiviert. Dann muss für eine IPsec Verbindung über die obige Konfiguration der Dienst „IKE- und AuthIp IPsec“ deaktiviert werden.

Je nach Verschlüsselungsverfahren muss noch ein Dword „1“ in der Registry unter „HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters\NegotiateDH2048_AES256“ eingetragen werden.

Nach erfolgreicher Konfiguration alle Komponenten kann man die Kommunikation mit Hilfe von Wireshark beobachten:

```
> Ethernet II, Src: Apple_a6:41:3a (64:76:ba:a6:41:3a), Dst: IntelCor_dc:da:7a (38:de:ad:dc:da:7a)
> Internet Protocol Version 4, Src: 192.168.179.21, Dst: 192.168.179.59
v Authentication Header
    Next header: UDP (17)
    Length: 4 (24 bytes)
    Reserved: 0000
    AH SPI: 0x6a13a0ec
    AH Sequence: 62
    AH ICV: 36cab7b8124b7cfef1e2488f
> User Datagram Protocol, Src Port: 30494, Dst Port: 30492
v SOME/IP
    Service ID: 0x000a
    Method ID: 0x0015
    Length: 0x00000009 (9 bytes)
    Client ID: 0x0000
    Session ID: 0x0040
    Protocol Version: 0x01
    Interface Version: 0x01
    Message Type: 0x00 (REQUEST)
    Return Code: 0x00 (OK)
```

Abbildung 3: Authentication Header für SOME/IP Nachricht

Zusammenfassung

Mit Hilfe von strongSwan und der ATMES someIpSim kann eine SOME/IP Kommunikation über IPsec realisiert werden.