# SSL MiM Angriff

## *Mittendrin statt nur dabei*

# Inhalt

- Kurzer historischer Abriss
- SSL/TLS Handshake und Key Derivation
- X.509 Zertifikate
- SSL/TLS API
- Dynamic Certificate Assembly
- Vorführung eines Angriffes

# Historie

- 1994 Netscape SSLv1, unreleased
- 1994 Netscape SSLv2
- 1995 Netscape SSLv3
- 1996 SSLv3.1 = TLSv1 IETF
- vornehmlich Einsatz für HTTPS, neuerdings VPNs

1. C > S: Liste unterstützter Chiffren, Zufallszahl
2. C < S: Gewählte Chiffre, Zufallszahl, X.509 Zertifikat(e)
3. C > S: verschlüsseltes pre_master_secret
4. beide Seiten leiten die Schlüssel her
5. C > S: MAC des Handshakes
6. C < S: MAC des Handshakes

# Key Derivation

```
MasterSecret := KDF(ClientRandom,
                    PreMasterSecret,
                    ServerRandom);

KeyBlock := KDF(MasterSecret,
                ClientRandom,
                ServerRandom);
```

# X.509 Certs I

```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=DE, ST=Brandenburg, L=Potsdam, O=Uni Potsdam, OU=AStA,
    CN=www.stud.uni-potsdam.de/Email=computer@asta.uni-potsdam.de
    Validity
        Not Before: May  1 12:08:44 2003 GMT
        Not After : Apr 30 12:08:44 2004 GMT
    Subject: C=DE, ST=Brandenburg, L=Potsdam, O=Uni Potsdam, OU=AStA,
    CN=www.stud.uni-potsdam.de/Email=computer@asta.uni-potsdam.de
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
```

# X.509 Certs II

```
RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:d5:47:e7:04:83:b2:e8:5c:e5:98:55:96:60:65:
      67:db:ff:44:1b:51:7f:f8:50:75:68:02:74:ba:39:
      e3:46:dd:0c:3e:14:fe:61:ba:05:5b:84:22:e2:a5:
      3e:16:0f:6c:bb:13:c1:ba:e3:6b:af:42:1b:7e:56:
      41:af:eb:cc:d9:a6:b2:71:fe:ea:f8:df:ab:72:a0:
      8e:ac:21:64:31:1a:a7:f5:c9:34:b3:87:ae:8a:af:
      5d:ec:24:3b:fe:d3:90:19:3f:c8:01:75:8c:83:1a:
      40:e1:9e:b0:43:a3:3d:f9:68:a0:77:ef:1b:61:ce:
      80:db:88:1a:9a:65:e0:df:65
    Exponent: 65537 (0x10001)
```

# X.509 Certs III

```
X509v3 extensions:
 X509v3 Subject Key Identifier:
   DB:3C:8B:AA:BB:AE:27:8E:95:07:F9:FD:DB:27:AB:14:E3:C6:63:43
 X509v3 Authority Key Identifier:
   keyid:DB:3C:8B:AA:BB:AE:27:8E:95:07:F9:FD:DB:27:AB:14:E3:C6:63:43
     DirName:/C=DE/ST=Brandenburg/L=Potsdam/O=Uni Potsdam/OU=AStA/
     CN=www.stud.uni-potsdam.de/Email=computer@asta.uni-potsdam.de
     serial:00

   X509v3 Basic Constraints:
     CA:TRUE
```

# X.509 Certs IV

```
Signature Algorithm: md5WithRSAEncryption
   8e:b2:e4:b3:d0:8e:24:ca:7d:44:99:65:1e:5e:d0:60:d1:c9:
   50:5d:19:4f:70:66:31:50:27:c6:b2:43:c2:37:a1:cc:96:ea:
   4f:34:88:45:36:a7:f2:f8:00:78:21:62:eb:9e:48:7f:c1:98:
   1f:bf:6a:5c:57:cb:6f:06:28:ee:72:cf:e1:cc:0e:af:26:2b:
   65:94:2c:27:e0:f4:41:ee:0f:b0:7f:aa:60:b4:ee:5b:2f:58:
   d1:66:f0:f2:24:73:c4:43:57:2a:f3:07:8f:27:96:b2:89:3e:
   df:3e:10:56:a9:ad:3d:66:48:01:aa:e2:12:73:f9:be:de:d8:
   13:25
```

# TLS API - Serverseitig

- Normalerweise vorher festgelegt durch SSLv23_server_method()
- Laden des private keys: SSL_CTX_use_certificate_file(), SSL_CTX_use_PrivateKey_file()
- Annehmen der Verbindung: SSL_accept()
- I/O durch SSL_read()/SSL_write()

# TLS API - Clientseitig

- Normalerweise vorher festgelegt durch SSLv23_client_method()
- Laden der Zertifikate: SSL_CTX_load_verify_locations()
- Setzen der verify routine: SSL_CTX_set_verify(), oft Ursache von Fehlern (prüfen des CN Feldes)
- Verbindung herstellen: SSL_connect()

# Einige HTTP(S) clients

- mozilla, Konquerer, opera, ...
- wget, w3m, lynx
- apt-get install, up2date

# Dynamic Certificate Assembly (DCA)

- entwickelt 2001 um statisches SSL MiM abzulösen (HAL2001 :-)
- aus zwei mach eins (mergen von zwei Zertifikaten)
- 4 merge-Methoden die sich bewährt haben
- mitterweile von HTTPS Content-Filtern benutzt

# one2oneSpace

```
[ Subject B ]  [ Subject E ]
[ Issuer  B ]  [ Issuer  E ]
[ Key     B ]  [ Key     E ]
[ Sign    B ]  [ Sign    E ]
```

```
[ Subject B          ]
[ Issuer  B + " " ]
[ Key  E             ]
[ Sign E             ]
```

# subject4issuer

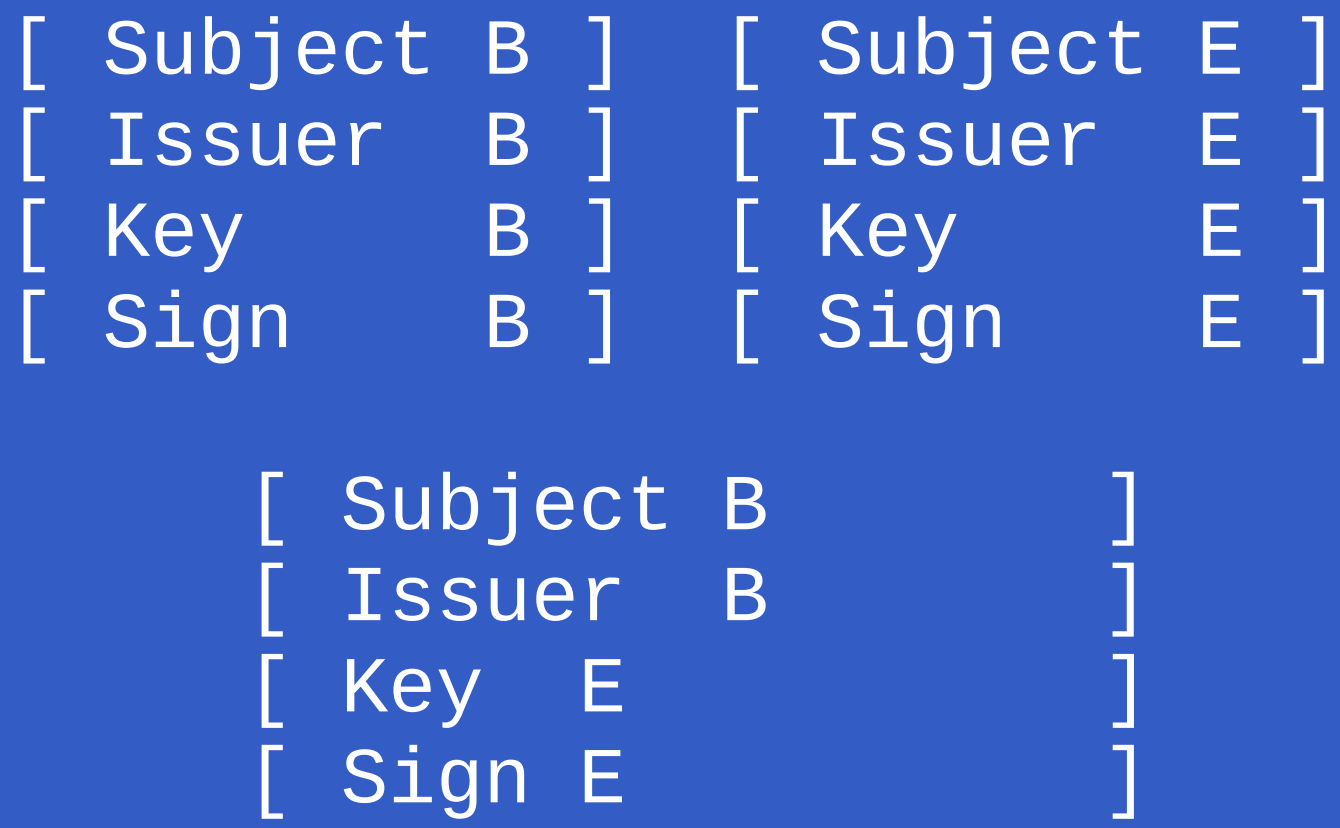
```
[ Subject B ]  [ Subject E ]
[ Issuer  B ]  [ Issuer  E ]
[ Key     B ]  [ Key     E ]
[ Sign    B ]  [ Sign    E ]

      [ Subject B        ]
      [ Subject B        ]
      [ Key  E           ]
      [ Sign E           ]
```

# subject4issuerSpace

```
[ Subject B ]  [ Subject E ]
[ Issuer  B ]  [ Issuer  E ]
[ Key     B ]  [ Key     E ]
[ Sign    B ]  [ Sign    E ]
```

```
[ Subject B          ]
[ Subject B + " " ]
[ Key  E             ]
[ Sign E             ]
```

# one2one


[ Subject B ]
[ Issuer B ]
[ Key B ]
[ Sign B ]
[ Subject E ]
[ Issuer E ]
[ Key E ]
[ Sign E ]
[ Subject B ]
[ Issuer B ]
[ Key E ]
[ Sign E ]

# Referenzen

- OpenSSL
  *http://www.openssl.org*
- OpenVPN
  *http://openvpn.sf.net*
- DCA
  *http://www.phrack.org/show.php?p=57&a=13*