Multipath TCP improvements

Q. De Coninck, M. Jadin, O. Bonaventure
UCLouvain
Agenda

• Improving Multipath TCP on smartphones

• Multipath TCP Secure
Multipath TCP on smartphones

• What are the benefits of using Multipath TCP on smartphones?
  – Higher bandwidth by bonding WiFi and LTE
    • Very few applications require this feature


  – Faster handovers between WiFi and LTE
    • This is the main reason why Siri uses Multipath TCP
Multipath TCP on smartphones

- Both LTE and WiFi active

![Diagram showing the process of multipath TCP with handshake and data transmission between a smartphone and a server.]
Multipath TCP on smartphones

- To minimise energy consumption, WiFi only

Enable LTE

SYN+MP_CAPABLE

SYN+ACK+MP_CAPABLE

Data

SYN+MP_JOIN

SYN+ACK+MP_JOIN

MP_JOIN ACK

ACK

Data (reinjection)
Improving handovers on smartphones

• Ideally, smartphones would like to do

Enable LTE

- SYN+MP_CAPABLE
- SYN+ACK+MP_CAPABLE
- Data
- SYN+MP_JOIN(backup)+Data (reinjection)
- SYN+ACK+MP_JOIN
- MP_JOIN ACK
- ACK
Faster handovers

- In RFC6824, we opted for a four-way handshake to establish the additional subflow
  - This is fine for bandwidth aggregation, but far too long for fast handovers on smartphones

- RFC6824bis should revisit this assumption by
  - Analysing the security threats caused by the transmission of data inside SYN+MP_JOIN
  - Devise a solution that allows to transmit/reinject data inside SYN+MP_JOIN
Agenda

• Improving Multipath TCP on smartphones

• Multipath TCP Secure
Multipath TCP Secure

• TLS over Multipath TCP
  – Works out of the box, but attackers could cause denial of service by
    • Changing TCP headers or MPTCP options
    • Injecting/modifying data

• Multipath TCP Secure's design objective
  – Preserve connectivity when attacker is not active on all paths
Attack scenario
TLS over Multipath TCP

- Attacker on one path, e.g. WiFi

  - Change payload
  - Invalid TLS record
    - Terminate entire TLS session
Attack scenario
Multipath TCP Secure

• Attacker on one path, e.g. WiFi

Change payload
Invalid AEAD
Terminate subflow, Connection continues

Reinjected Data
Building blocks

• A secure handshake allows to negotiate keys
  – TLS 1.3 for example

• AEAD : Authenticated Encryption with Additional Data
  – Used to securely encrypt and authenticate both data and key Multipath TCP options
Authentication information

• Where should we place the authentication information?
  - As an extension of Multipath TCP options
    • Not enough space inside TCP extended header
  - Inside the payload
    • Authentication information is added at the end of each mapped data
Authenticating data and options

TCP Segment
In clear

TCP Segment
Encrypted

TCP header

TCP options

MPTCP options

Application Data

Associated Data

Associated Data

Plaintext

AEAD

AEAD

Ciphertext Data

Authentication tag of the options

(key based on Data Sequence Number)
Implementation status

• Linux Kernel v.4.1, inside the MPTCP code
• Use of the Linux/GNU CryptoAPI
• Regular MPTCP still negotiable
• ~5000 lines of diff
• https://bitbucket.org/mptcpsecteam/mptcpsec
**Benchmarks**

<table>
<thead>
<tr>
<th></th>
<th>Client</th>
<th>Server</th>
<th>Server [eth1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>4 GB</td>
<td>2 GB</td>
<td>100</td>
</tr>
<tr>
<td>CPUs</td>
<td>Intel i5</td>
<td>Intel Core 2</td>
<td>100</td>
</tr>
<tr>
<td>Speed (Mb/s)</td>
<td>1500</td>
<td>1500</td>
<td>1500</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>Offloading</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>
Benchmarks: goodput

Throughput from server perspective

- TLS
- MPTCPsec
- MPTCP
Benchmarks: request/response

Echo and reply of different sizes

- TLS
- MPTCPsec
- MPTCP

Time elapsed (ms)

Message data size (bytes)
Conclusion

• Multipath TCP on smartphones
  – RFC6824bis should include solutions to reduce handover times

• Multipath TCP secure
  – First step towards a version of Multipath TCP that can cope with on-path attackers
  – More details in
    https://inl.info.ucl.ac.be/publications/secure-multipath-tcp-design-implemementation