ON ROUTES EXCHANGE AT IXPs AND PRIVACY

- Internet eXchange Points (IXPs) are physical networks where members connect to exchange traffic.
- Routing information exchanged via BGP sessions among members.
- Route Servers (RSes) at IXPs ease BGP route-dispatch
- Members that use RSes must disclose their confidential route-export policies to the IXP.
  - Export-policy: what BGP routes a member is willing to announce to other members.
  - Privacy concerns deter some networks from subscribing to RS services.
- How can a member leverage the functionalities of a centralized RS without disclosing its export policies?

SIXPACK!

- A privacy-preserving route dispatching service.
- Based on provable security guarantees and recent developments in Secure Multi-Party Computation (SMPC).
- Two non-colluding entities perform SMPC computation in order to dispatch the BGP routes to participants.
- Two approaches:
  - ALL: dispatch all exportable BGP routes.
  - SINGLE: dispatch the “best” exportable BGP route according to the RS ranking.

EXAMPLE - “ALL” APPROACH

- Member A wants to announce a route \( R \) to member B.
- Route \( R \) is encrypted with key \( K \) and sent to each member.
- The export policy of A is secret-shared between RS1 and RS2 as an input to the SMPC.
- SMPC is responsible for dispatching \( K \) only to member B.
- Neither RS1 nor RS2 learns anything about the export policy of member A.

PRACTICALLY GOOD SMPC PERFORMANCE

- Emulate large IXP with 750 members.
- 1 Gbps link connection between the two parties.
- ABY framework based on the GMW protocol.
- The setup phase is independent of the actual inputs and can be precomputed.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Inputs</th>
<th>Setup [ms]</th>
<th>Online [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>2</td>
<td>1.7</td>
<td>0.6</td>
</tr>
<tr>
<td>SINGLE</td>
<td>2</td>
<td>41.7</td>
<td>1.6</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>42.2</td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>54.8</td>
<td>9.2</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>66.0</td>
<td>19.1</td>
</tr>
</tbody>
</table>

PROTOTYPE EVALUATION

- Based on a real-world trace of BGP updates from one of the largest IXPs worldwide.
- More than 600 members, 10.62 BGP route announcements/withdrawals per second.
- SIXPACK prototype in Python.
- Bandwidth requirement RS1 \( \leftrightarrow \) RS2 below 11Mbps.

FUTURE RESEARCH

- Enhancing RS ranking by incorporating members’ local-preference and IXP’s ranking.
- Extending our approach to Software-Defined-eXchanges.
- Optimizing the SIXPACK prototype.

PRESENTER CONTACT
Email: marco.chiesa@uclouvain.be