Secure Networks for IoT Devices

David Hausheer (OVGU Magdeburg), Adrian Perrig (ETH Zürich)
Internet of Things (IoT)

- Network of smart objects, to collect and analyze data

- Characteristics: Small-scale devices, sensors, low cost, low energy usage

- Bain predicts IoT market to grow to about $520B in 2021 ($235B in 2017)
Security of Internet of Things

- Security is the biggest concern in adopting IoT technology (especially IoT adoption in enterprises)

- Threats:
  - Potential failures and attacks hinder adoption in critical infrastructures with high availability requirements (e.g. transportation or Grid infrastructures)
  - IoT devices often use weak authentication which may facilitate unauthorized access (e.g. smart home, healthcare devices)
  - Use of unencrypted communication may leak privacy-sensitive data (e.g. healthcare)
SCION: Next–generation Internet Architecture

- Secure by design, most attacks are fundamentally impossible
- Path–aware networking: sender knows packet’s path
  - Enables geo–fencing
- Highly available communication
- Multi–path communication
  - Caution: use is highly addictive!
- BGP–free Internet communication
- Better scalability than current Internet
- Improved network operation
  - Higher network utilization
  - Advanced traffic engineering
## SCION Mechanisms to Satisfy IoT Requirements

<table>
<thead>
<tr>
<th>Key Management</th>
<th>Enable E2E encryption and authentication</th>
<th>DRKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled / restricted remote access</td>
<td>Prevent exploitation of device vulnerabilities</td>
<td>Hidden path (EPIC)</td>
</tr>
<tr>
<td>Guaranteed access for command-and-control</td>
<td>Packet delivery Traffic filtering at high data rates</td>
<td>Multipath in multi-homed environments EQ for guaranteed low-bw packet delivery Lightning Filter for high-speed filtering</td>
</tr>
<tr>
<td>Privacy</td>
<td>Complicate traffic analysis</td>
<td>Multipath communication can complicate traffic analysis</td>
</tr>
<tr>
<td>Compliance</td>
<td>Geofencing to avoid traffic leakage</td>
<td>Geofencing to avoid traffic leakage</td>
</tr>
</tbody>
</table>
Use Case: Secure Networks for IoT Devices

Deployment Scenario
- Site A is the monitoring site for IoT devices
- IoT Devices E, F, G are at ISP Z
  - Connected to SCION via CG-SIGs
  - Path Segments to the CG-SIGs are hidden and only given to site A

Benefits
- Secure network access
- Only site A can access E, F, G
- High availability for the IoT network by using CG-SIG

Use Hidden Paths
Default-off security model
Thank you for your attention!
Questions?
david.hausheer@gmail.com
Online Resources

- https://www.scion-architecture.net
  - Book, papers, videos, tutorials

- https://www.scionlab.org
  - SCIONLab testbed infrastructure

- https://github.com/scionproto/scion
  - Source code

- https://www.anapaya.net
  - SCION commercialization