A Multicast-Avoiding Privacy Extension for the Avahi Zeroconf Daemon
Daniel Kaiser, Andreas Rain, Marcel Waldvogel, Holger Strittmatter

Standard mDNS-SD

Private Data can be seen by anyone!
Hello everybody!
My name is Alice Wonder.
I use (Chat) I am currently gaming!
I share the folders: Masterthesis, Fuerteventura2015, MyMusic.
I want to synchronize with Alice’s and Bob’s smartphone.

Private information accessible by everybody
Zeroconf service discovery is very convenient as it allows users to share services in the local network with zero configuration overhead.
But there is a serious privacy problem: even in untrusted networks, a lot of private information is indiscriminately shared with everyone.

Our Goals

<table>
<thead>
<tr>
<th>Client Type</th>
<th>Public</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard mDNS-SD</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>untrusted</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>trusted</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Client access to service info

Transparent, tuneable and backwards compatible privacy
Publish private information only to select friends:
Using the Enhanced Service Browser the user is able to tune privacy settings while sensible defaults allow to get almost Zero-Configuration Privacy.
Our Privacy Extension is fully backwards compatible.

Our Privacy Extension

Pairing: Once per pair of users
To be able to privately offer and request services, users have to exchange pairing data only once. Pairing data can be synchronized among devices belonging to the same user.

Privacy socket distribution: When entering a network
When entering a new network, a user privately announces a private socket to her friends, on which she answers encrypted service requests. This socket can be distributed using either
1) encrypted multicast or
2) our Stateless DNS technique avoiding multicast altogether.
Stateless DNS uses the local organization’s unmodified caching name server to allow hosts to store key-value pairs, without having to register.

Privacy preserving service discovery
Now it is possible to offer and request services directly by sending the corresponding queries and answers via encrypted unicast to the privacy sockets of friends.
This also saves orders of magnitude in bandwidth on wireless networks.