Yodel: Strong Metadata Security for Real-Time Voice Calls

David Lazar, Yossi Gilad, Nickolai Zeldovich

MIT CSAIL
Metadata is data that can’t be encrypted.
What can you learn from metadata?

Dan

Huawei Executive

Saudi Dissident

Erin

Fred

Bob

Alice

Guardian

NYT

Passive Network Adversary
Security goal: hide who is talking to whom
Performance goal: sub-second latency

< 1s × millions

< 1s
Prior work doesn’t meet goals

<table>
<thead>
<tr>
<th></th>
<th>Passive attacks</th>
<th>Active attacks</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tor</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Pung [OSDI 2016]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Karaoke [OSDI 2018]</td>
<td>✓</td>
<td>△</td>
<td>△</td>
</tr>
<tr>
<td>Herd [SIGCOMM 2015]</td>
<td>△</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

Differential privacy

7s

Trusted server
Contributions

**Yodel**: the first system for real-time voice calls with

- Strong protection against passive & active attacks
- Distributed trust (any-trust or fractional trust)
- Sub-second latency for 5M users with 100 servers

**Two key insights**

- **Self-healing circuits** & **Guarded circuit exchange**
Mixnets hide who sent which message

Onion-encrypted Message

Server 1

Server 2

Server 3
Mixing is expensive: public key operation for each message at every hop
Yodel’s mixnet: send public key onions to setup symmetric key circuits

Circuit setup onion
Circuit messaging

Server 1

Server 2

Server 3

= circuit (symmetric key) onion
Challenge: attacker has many chances to learn shuffle of honest server!
Yodel’s key insight: self-healing circuits
Yodel round steps

1. Users establish circuits

2. Users exchange circuits

3. Users connect to circuits

4. Users send voice packets

= random string
Evaluation

Does Yodel achieve low latency for large numbers of users?

Does Yodel offer acceptable voice quality?
Yodel achieves sub-second latency for 5M users

![Graph showing voice packet latency versus number of users for 100 servers in US & EU]
Yodel achieves acceptable voice quality

• Joanna and I had a short conversation over Yodel, with 5M other “users” actively using the system

• She ran Yodel over her laptop speakers and recorded the convo with her phone

  • (phone records her voice directly)

• Some latency (~1s) is due to us waiting to not talk over each other
Pre-recorded demo
Conclusion

**Yodel:** the first system for real-time voice calls with

- Strong metadata privacy (against passive & active attacks)
- Distributed trust (any-trust or fractional trust)
- Sub-second latency for 5M users with 100 servers

Full paper and code coming soon:

- [vuvuzela.io](https://vuvuzela.io)
- [davidlazar.org](https://davidlazar.org)