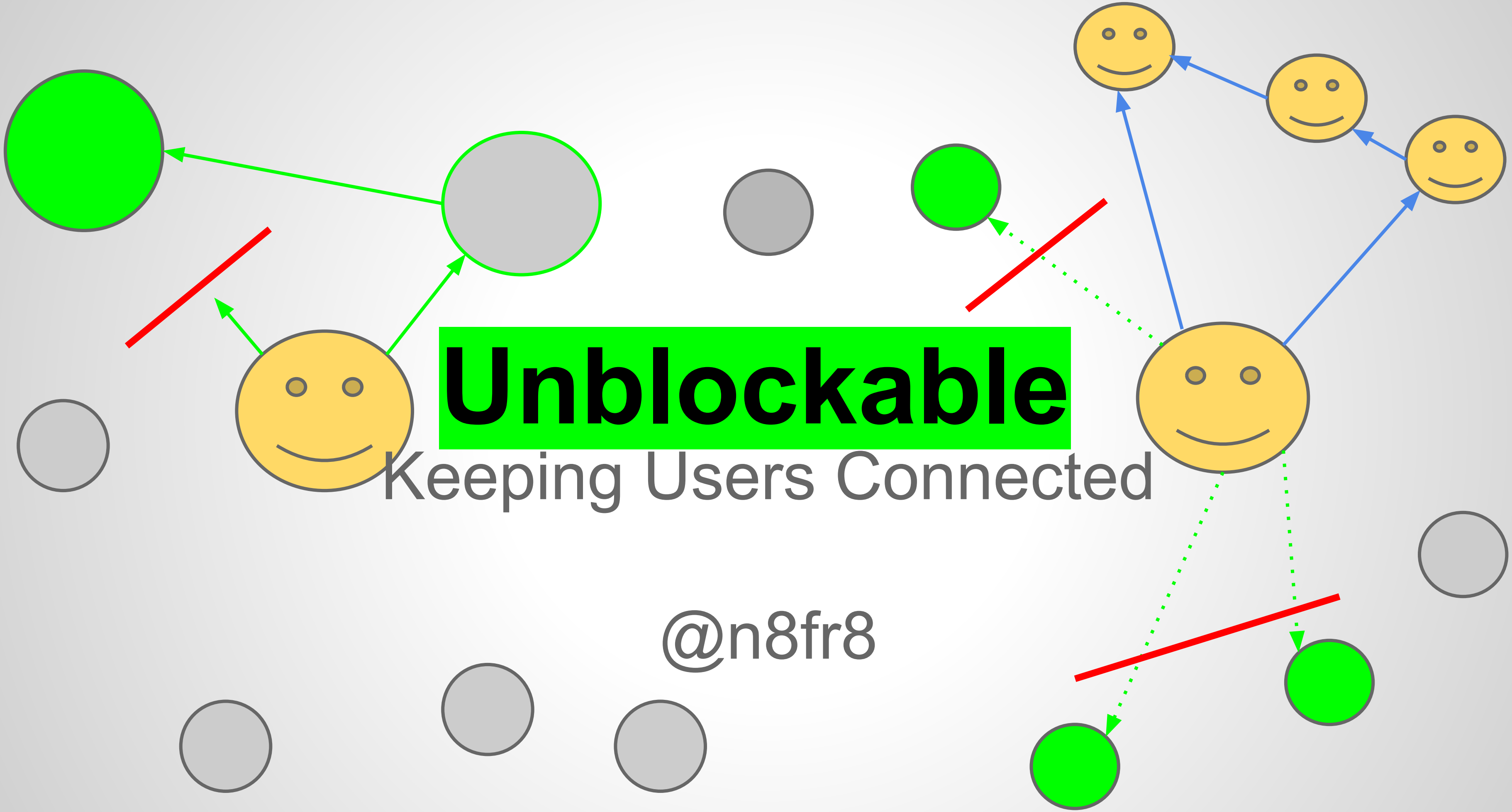


Unblockable

Keeping Users Connected

@n8fr8

Most Apps...

- Have fixed, centralized infrastructure
- Expect DNS to tell the truth
- Do not know how to use proxy servers
- Require the Internet to work

In other words, only work in ideal conditions...

Adversaries can...

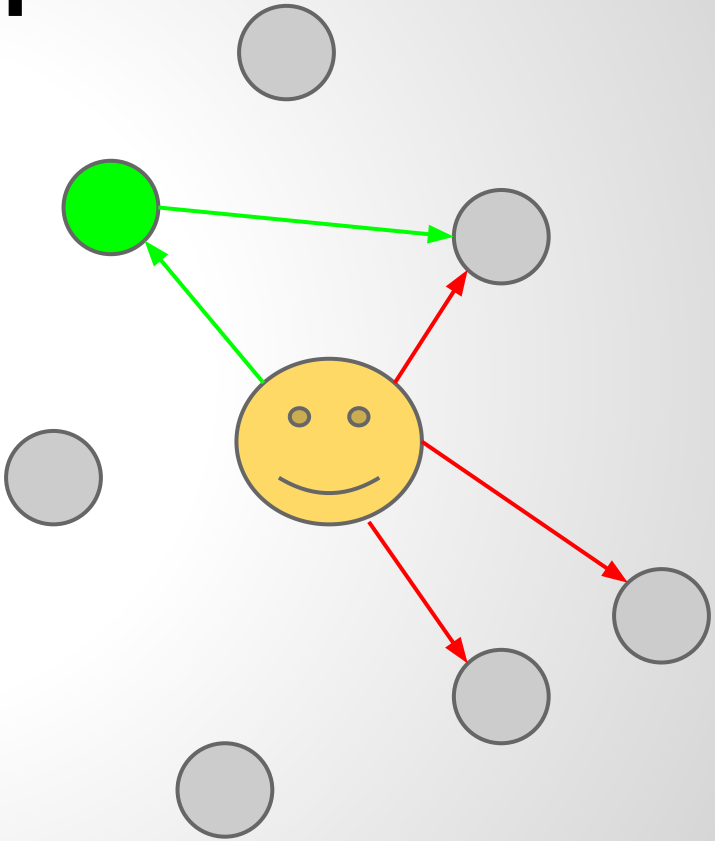
- Easily poison DNS to block services or enable a man-in-the-middle attack
- Block access to fixed servers using hostname, address or port filtering
- Disable telecommunications services

How do we guarantee our tools work when the moment of truth comes?

Unblockable Tactic #1

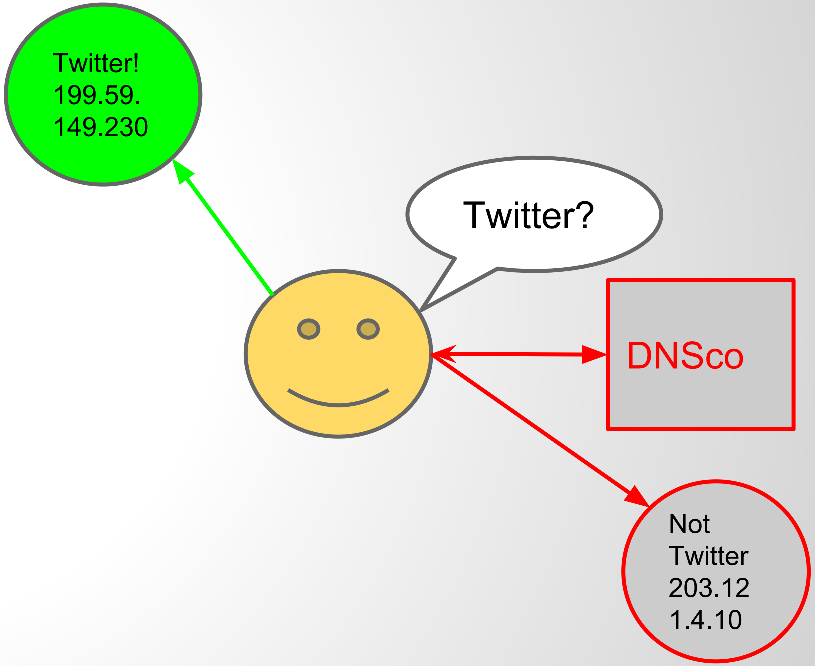
Utilize community-driven, federated server networks to create a large, diverse and dynamic network, easily accessible via one-tap.

```
"Please wait while we find a place for you somewhere out there..."
```



Unblockable Tactic #2

Don't rely on the local network DNS. Instead, utilize trustworthy domain authorities (8.8.8.8 or TorDNS) or use "hosts files" with cert pinning.

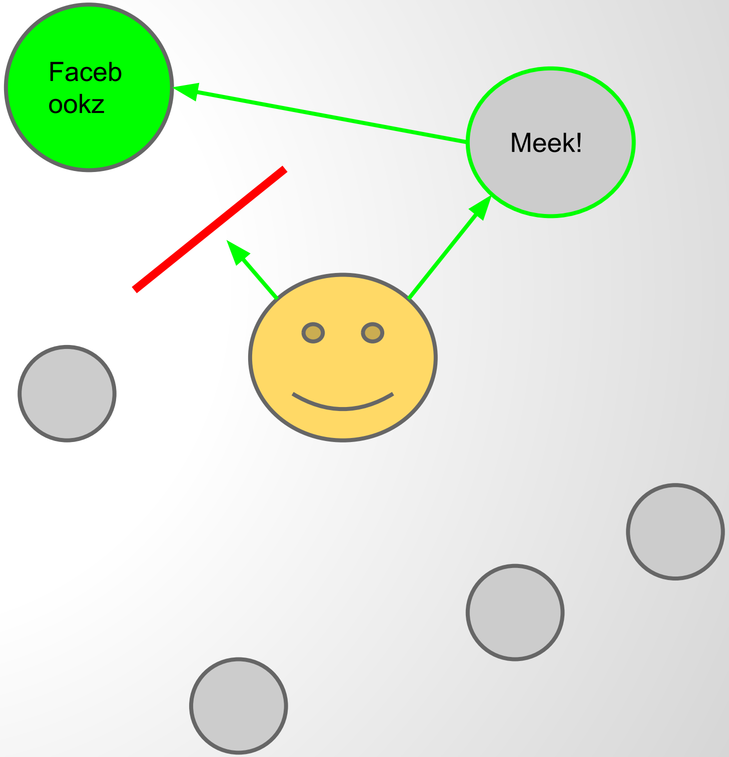


"Connecting you directly to verified servers..."

Unblockable Tactic #3

Add one-tap or automated proxy support to your apps, from basic HTTP and SOCKS, to integrated Tor and Pluggable Transport capability.

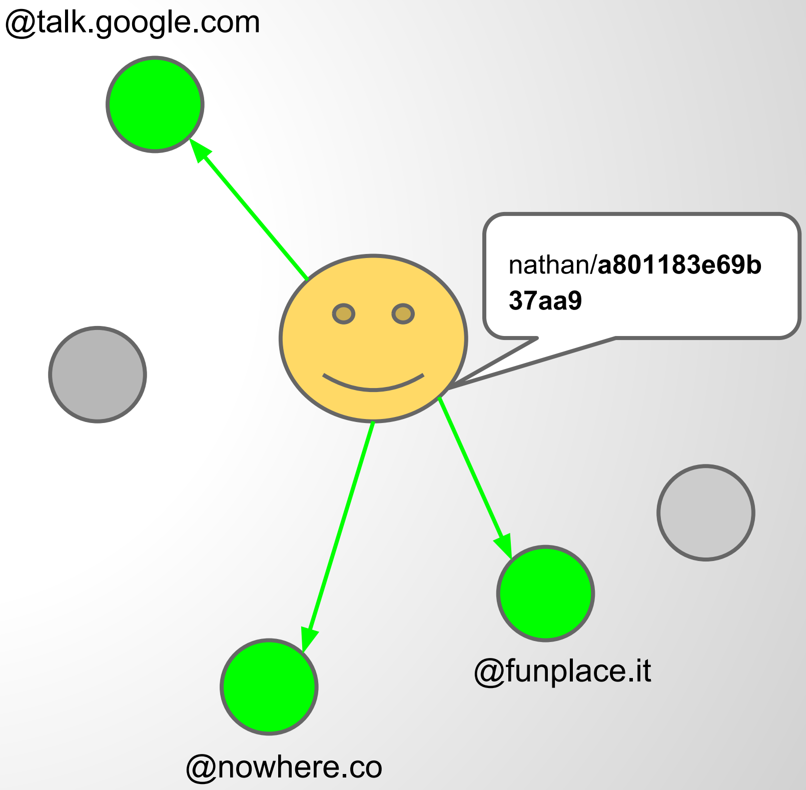
"Looks like your network is blocking us… trying an alternate route!"



Unblockable Tactic #4

Using verifiable public key cryptography, create an identity that is portable across different servers and contexts.

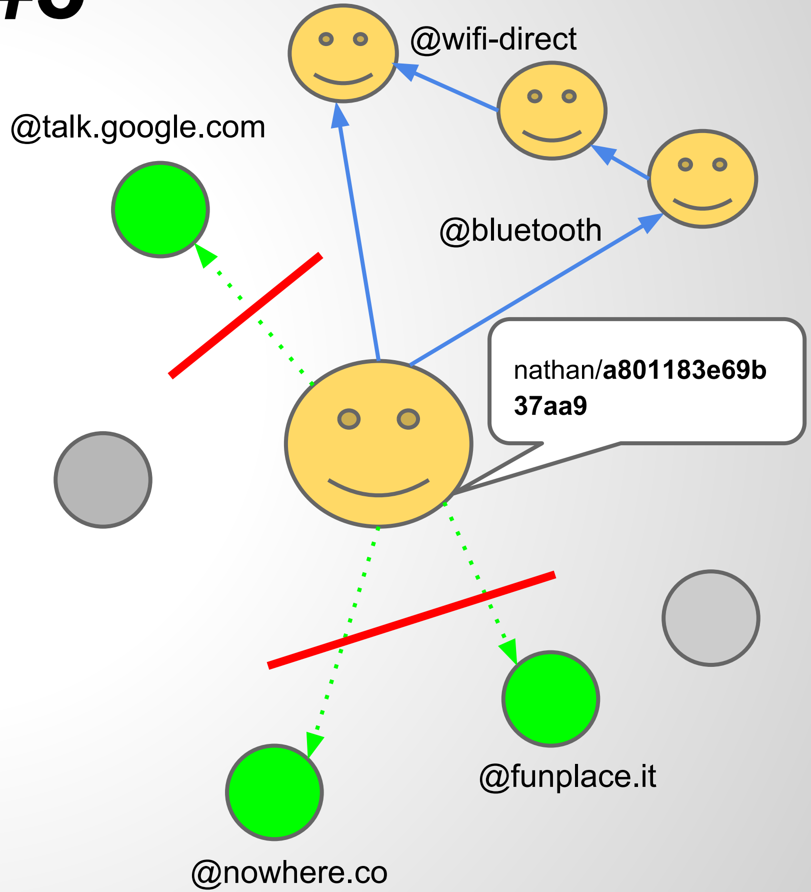
"Looks like your server is blocked or gone… moving you to a new one!"



Unblockable Tactic #5

Support non-Internet "Nearby" communication methods (Bluetooth, Bonjour, WifiDirect) as a default feature of your app.

```
"There are people nearby to
connect with - want to share
with them?"
```



The Unblockable Five

1. Use **diverse** network infrastructure
2. Only use **trustworthy** domain authorities
3. Integrate easy and **automatic** proxy support
4. Allow **verifiable** identities to be portable
5. Make **nearby** mode a default feature