INRIA

# One Bad Apple Spoils the Bunch

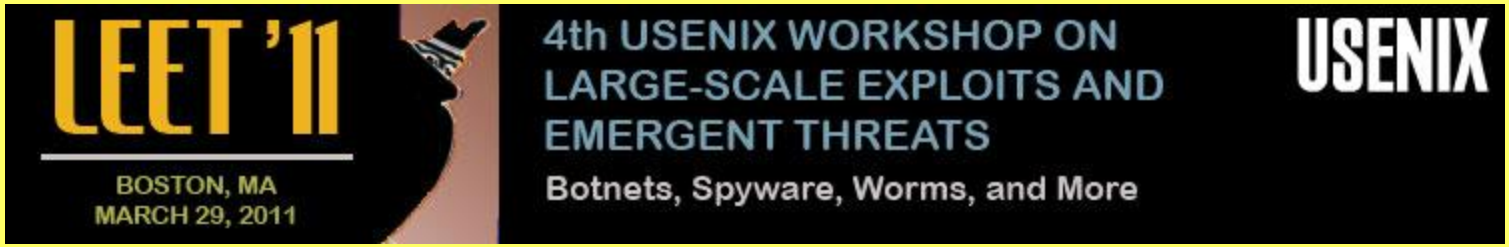
**Stevens Le Blond** Pere Manils Abdelberi Chaabane

Dali Kaafar Claude Castelluccia Arnaud Legout Walid Dabbous

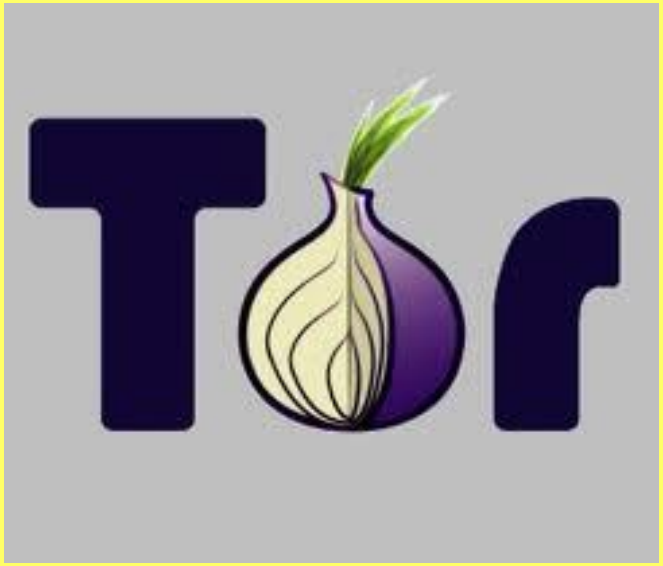

LEET '10
SAN JOSE, CA
APRIL 27, 2010
3rd USENIX WORKSHOP ON
LARGE-SCALE EXPLOITS AND
EMERGENT THREATS
Botnets, Spyware, Worms, and More
USENIX


BitTorrent™

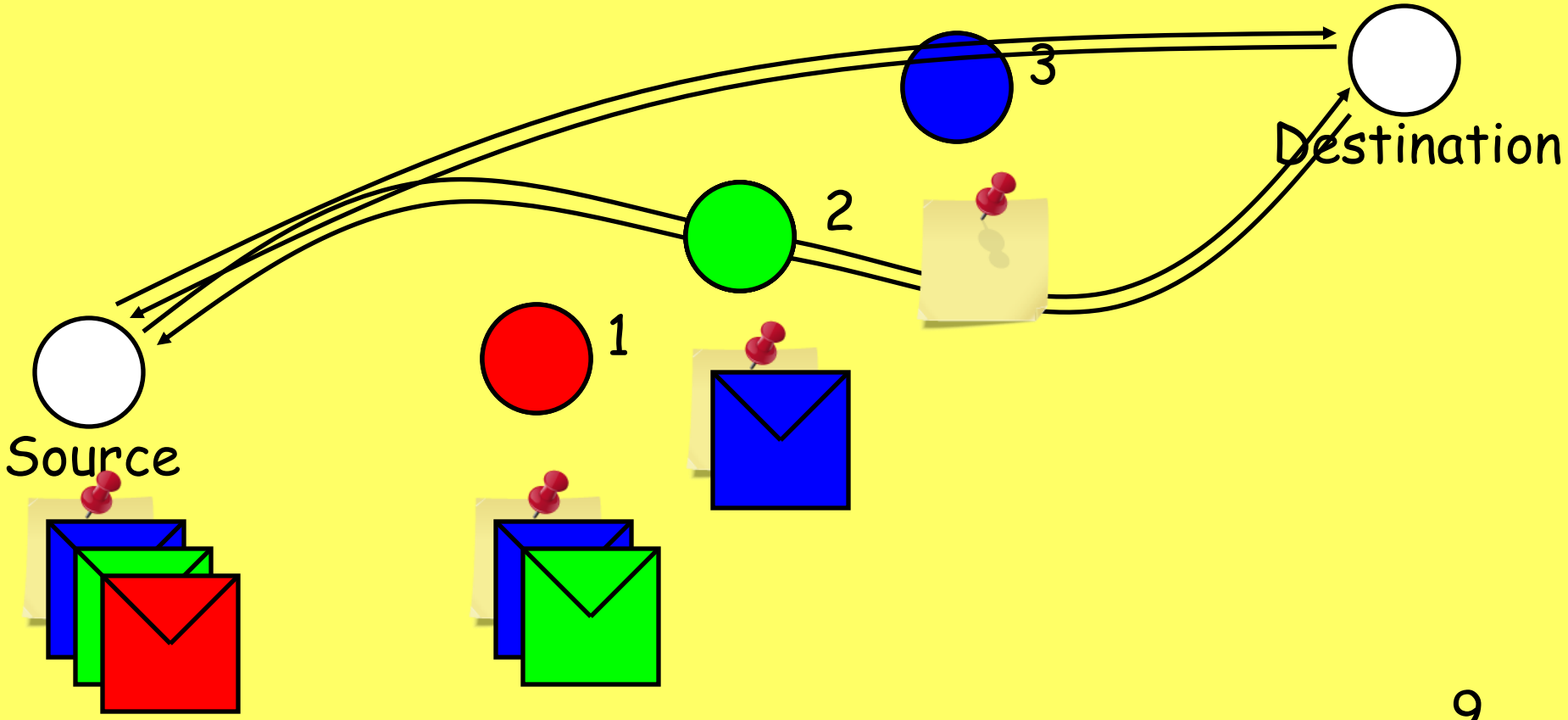
# IP address?


LEET '11
BOSTON, MA
MARCH 29, 2011
4th USENIX WORKSHOP ON
LARGE-SCALE EXPLOITS AND
EMERGENT THREATS
Botnets, Spyware, Worms, and More
USENIX

"I am not going to be around this year... sorry for missing out on the beer..."


Tor

# Background

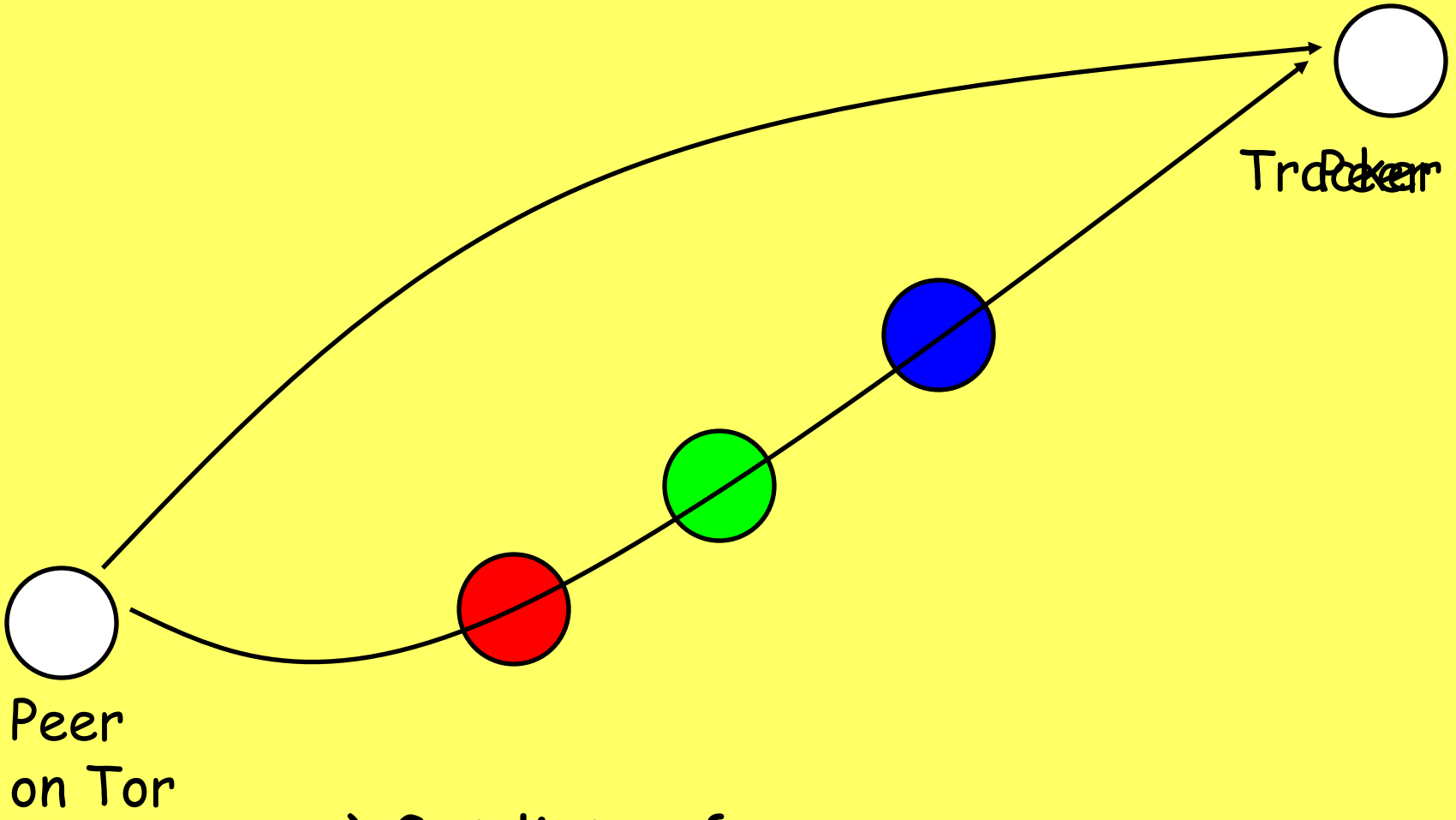


# Roadmap

1) 2 attacks against Tor

2) BitTorrent usage on Tor

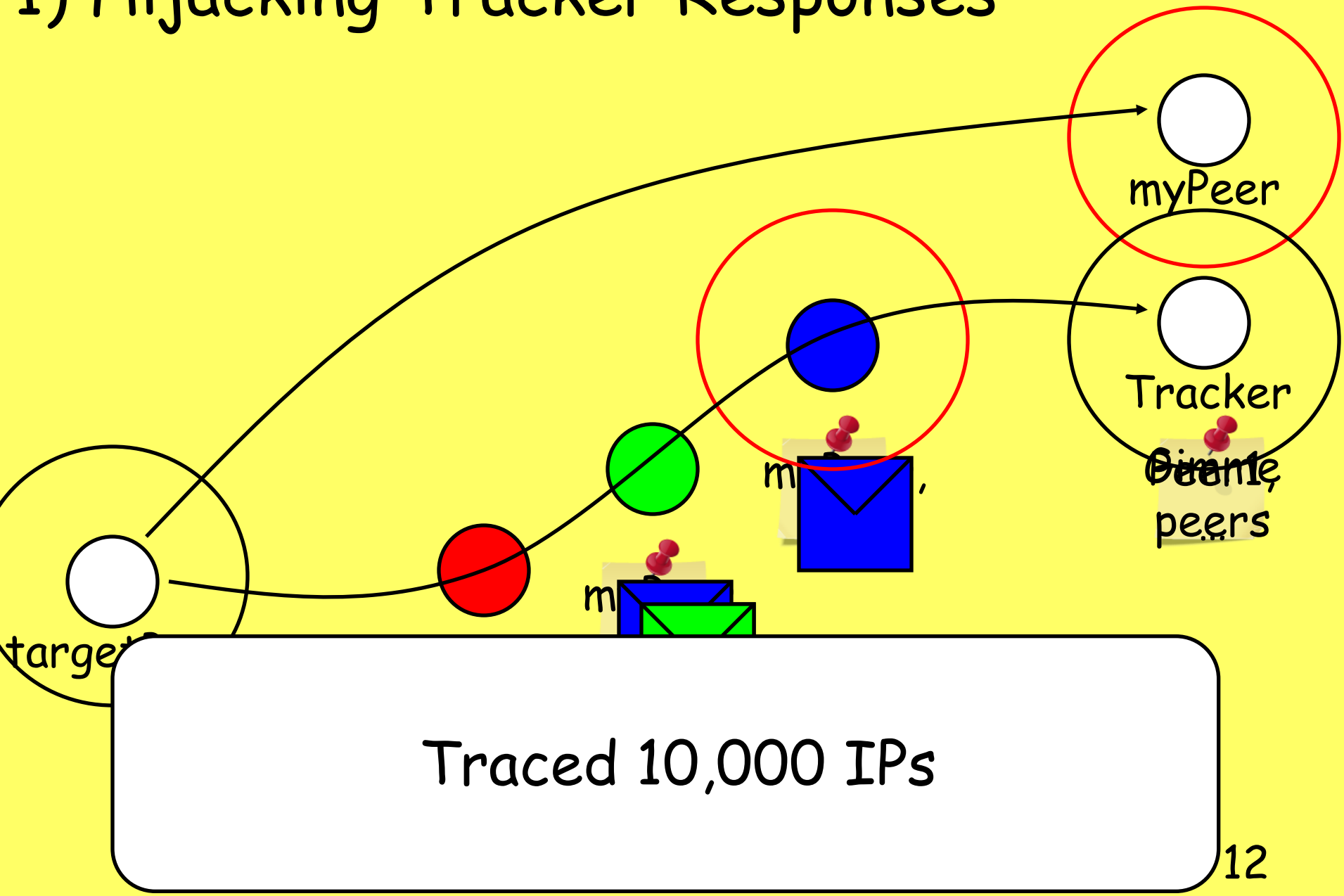
# BitTorrent on Tor



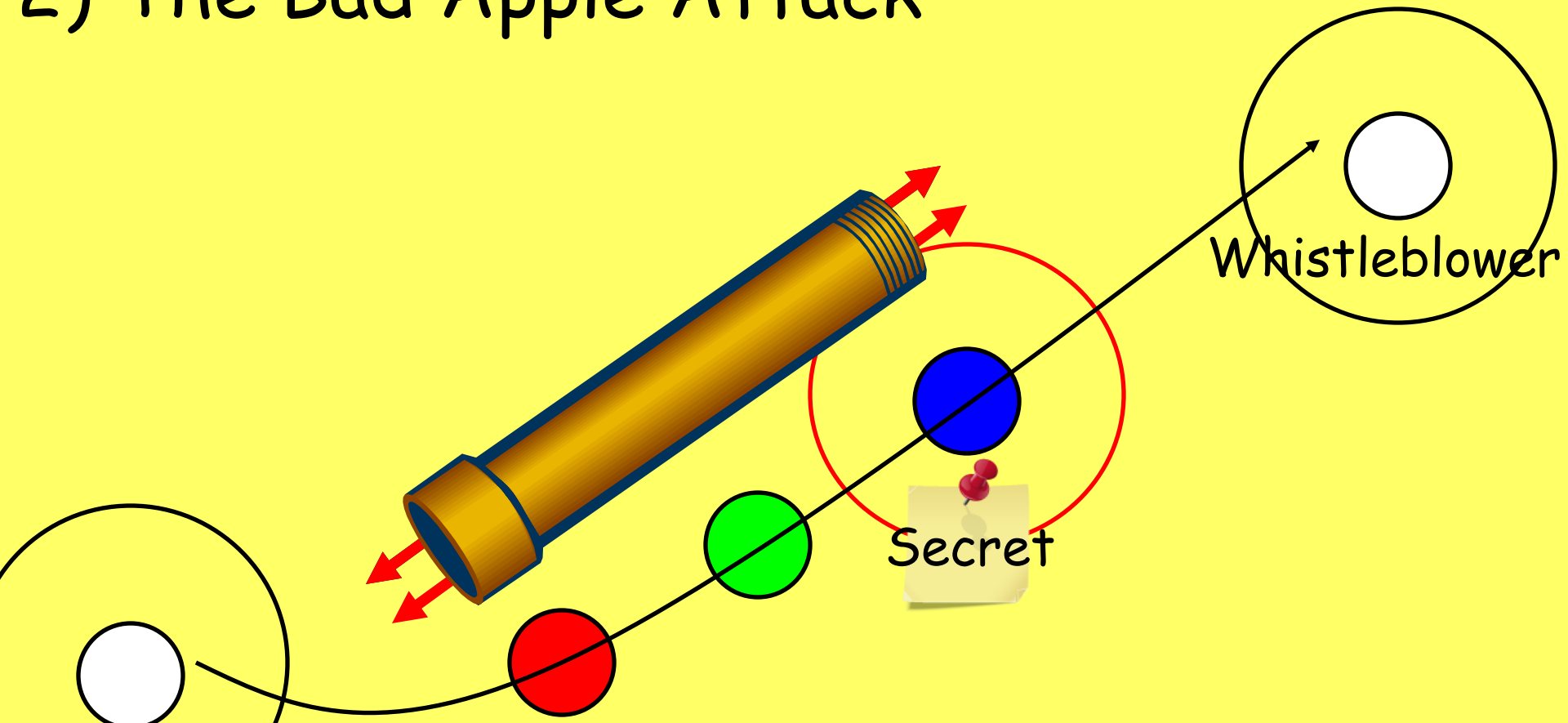

a) Get lists of peers (Tracker, DHT)

b) Content distribution

# 1) Hijacking Tracker Responses



# 2) The Bad Apple Attack




For each BitTorrent stream,
traced 2 additional streams
(9% of *all* streams)

# Roadmap

1) 2 attacks against Tor

2) BitTorrent usage on Tor

# Over-representation per Country

| Rank | # | % | Over | Country |
|---|---|---|---|---|
| 1 | 958 | 14 | 0.9 | US |
| 2 | 937 | 13 | 5.6 | Japan |
| 3 | 887 | 13 | 2.8 | Germany |
| 4 | 369 | 5 | 1.3 | France |
| 5 | 354 | 5 | 1.8 | Poland |
| 6 | 236 | 3 | 0.9 | Italy |
| 7 | 232 | 3 | 0.6 | UK |
| 8 | 231 | 3 | - | China |

BitTorrent on Tor

14% US peers

⇨ Over = 1

14% Japanese peers

⇨ Over = 5

BitTorrent outside Tor

14% US peers

2.5% Japanese peers

Why some countries
are over-represented?

# BitTorrent Usage in the US

# BitTorrent Usage in Japan

# BitTorrent Usage in Germany


Over-representations
likely due to sociological reasons

# Take Home Messages

1) P2P filesharing apps
   kill privacy on Tor

2) Bad Apple attack
   can be severe

3) Significant fraction of Tor traffic
   can be traced with app-level attacks