Censorship Arms Race: Research vs. Practice

Sadia Afroz

In collaboration with:
David Fifield, Michael Carl Tschantz, Vern Paxson, J.D. Tygar

Censorship

forbidden.com

forbidden.com

Censorship

forbidden.com

forbidden.com

Censorship

forbidden.com

Public Tor relay

forbidden.com

Censorship

forbidden.com

Public Tor relay

forbidden.com

Censorship

forbidden.com

Public Tor relay

Non-public Tor relay

forbidden.com

Censorship

forbidden.com

Public Tor relay

Non-public Tor relay

forbidden.com

Censorship

forbidden.com

Public Tor relay

Non-public Tor relay

forbidden.com

We want to know

- How well a circumvention system works in practice?
- How does it compare to other systems?

Practical attacks on Tor

1. Using properties of the endpoints

Domain name
IP : Port

Does not possess

Practical attacks on Tor

1. Using properties of the endpoints

Domain name
IP : Port

Does not possess

Happened in: Iran, China, Syria, Saudi Arabia, …

15 of the 32 known cases

Practical attacks on Tor

2. Using properties of the protocol

Cipher suite
SSL certificate lifetime
Is this SSL?

Does not possess

Practical attacks on Tor

2. Using properties of the protocol

Cipher suite
SSL certificate lifetime
Is this SSL?

Does not possess

Happened in: Iran, China, Syria, UAE, …

14 of the 32 known cases

Practical attacks on Tor

3. By unplugging the Internet

Happened in: Egypt 2011, Libya 2011, Syria 2012.

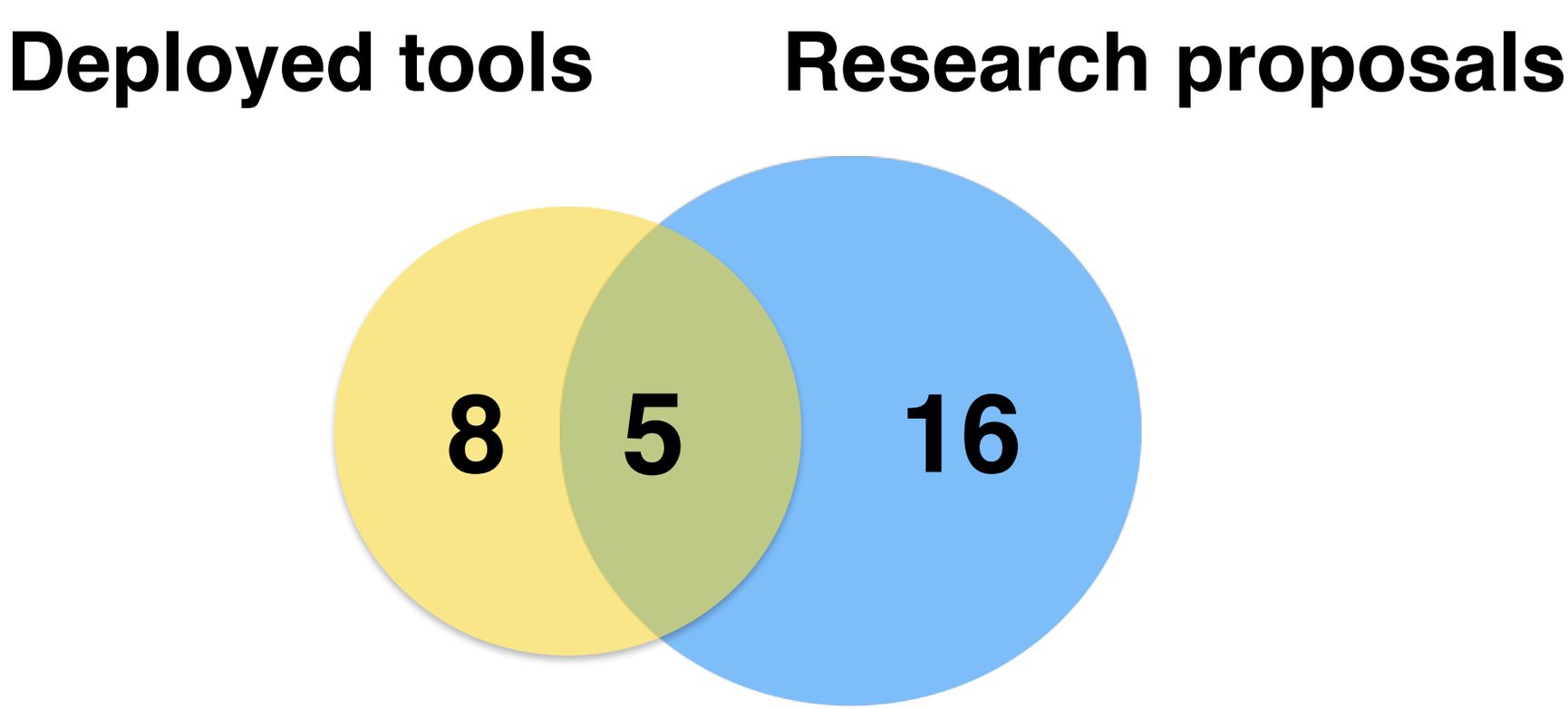
3 of the 32 known cases

Censor in real attacks

- Looks for the simplest features for blocking
    - scalable
    - low operational cost
    - low collateral damage
- Discovering the feature needs manual effort

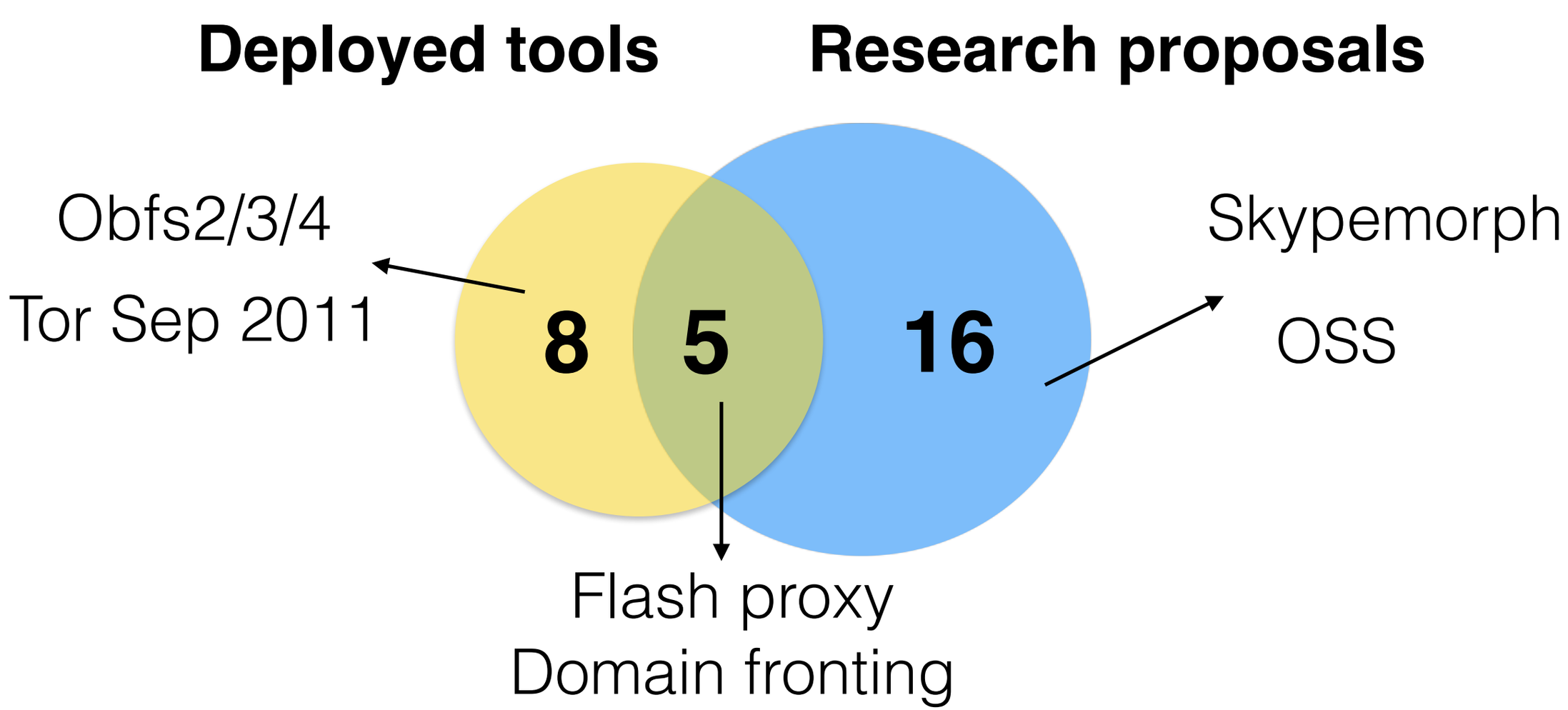
Research in censorship circumvention

- Surveyed 34 academic and practical censorship circumvention approaches



Research in censorship circumvention

- Surveyed 34 academic and practical censorship circumvention approaches



Research in censorship circumvention

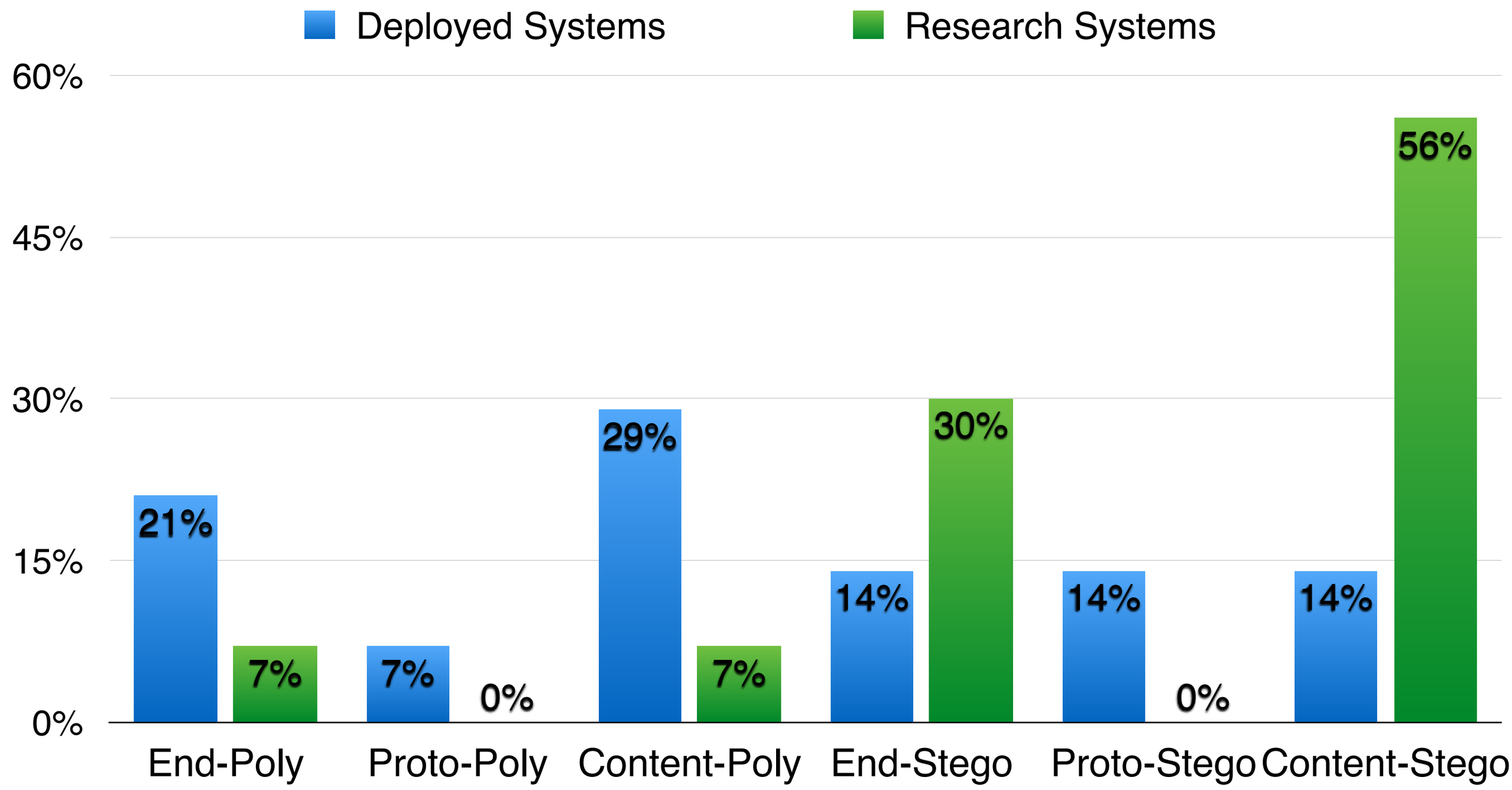
- What kind of attacks it defends?

- How?

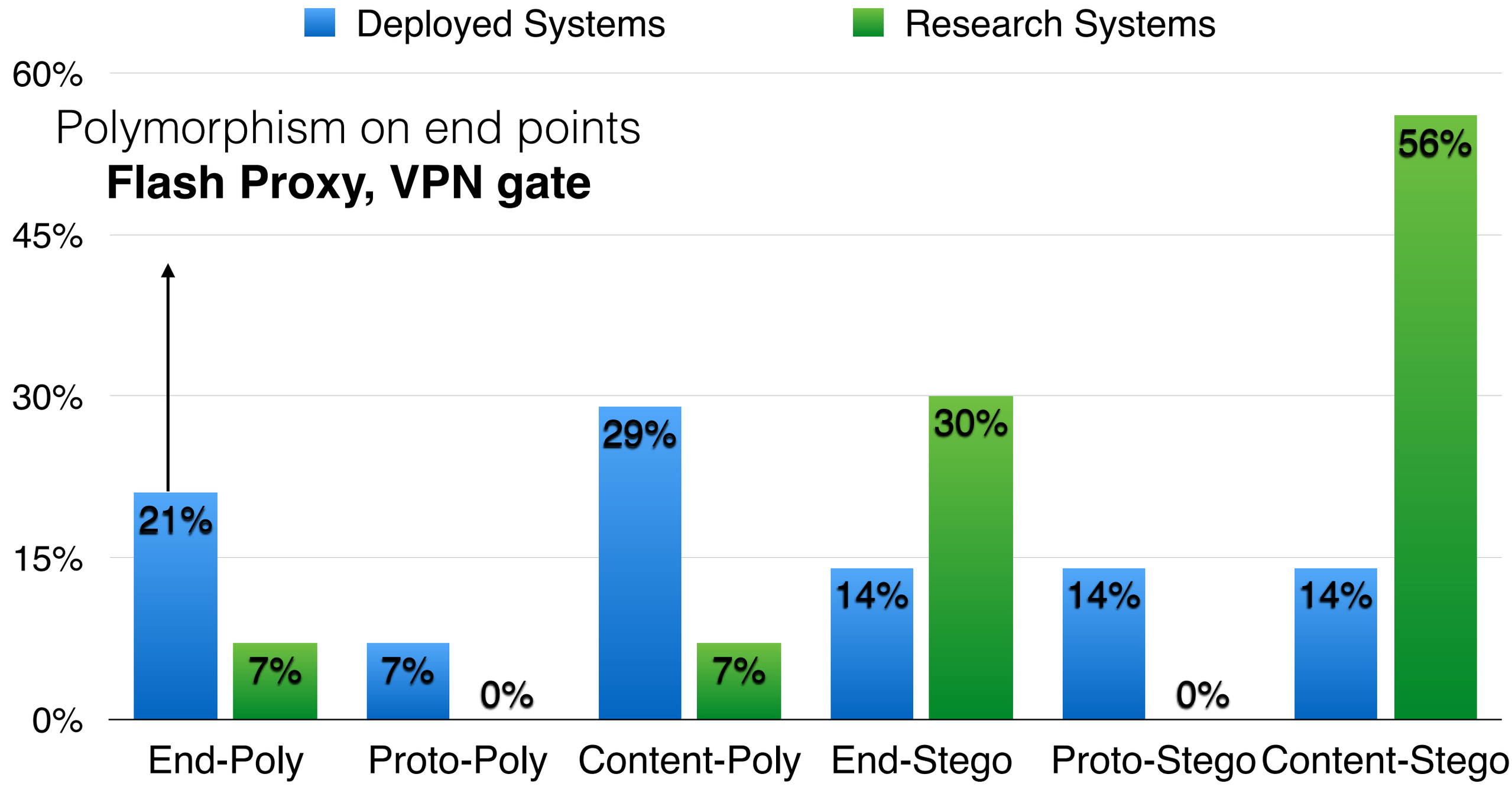
Research in censorship circumvention

- What kind of attacks it defends?
    - end points, protocol, content
- How?
    - Polymorphism: Looking different
    - Steganography: Looking like something

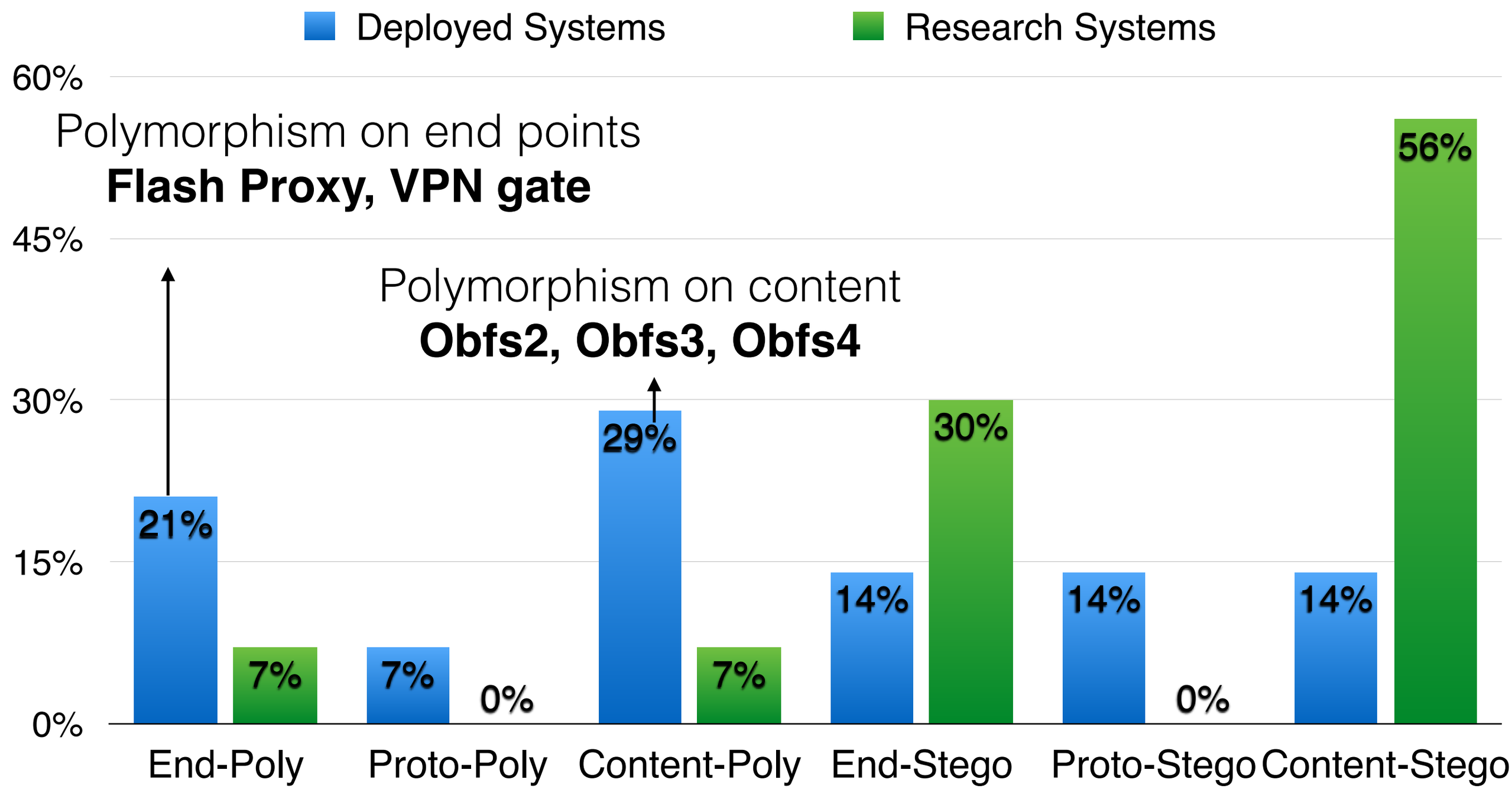
Research Vs. Practice



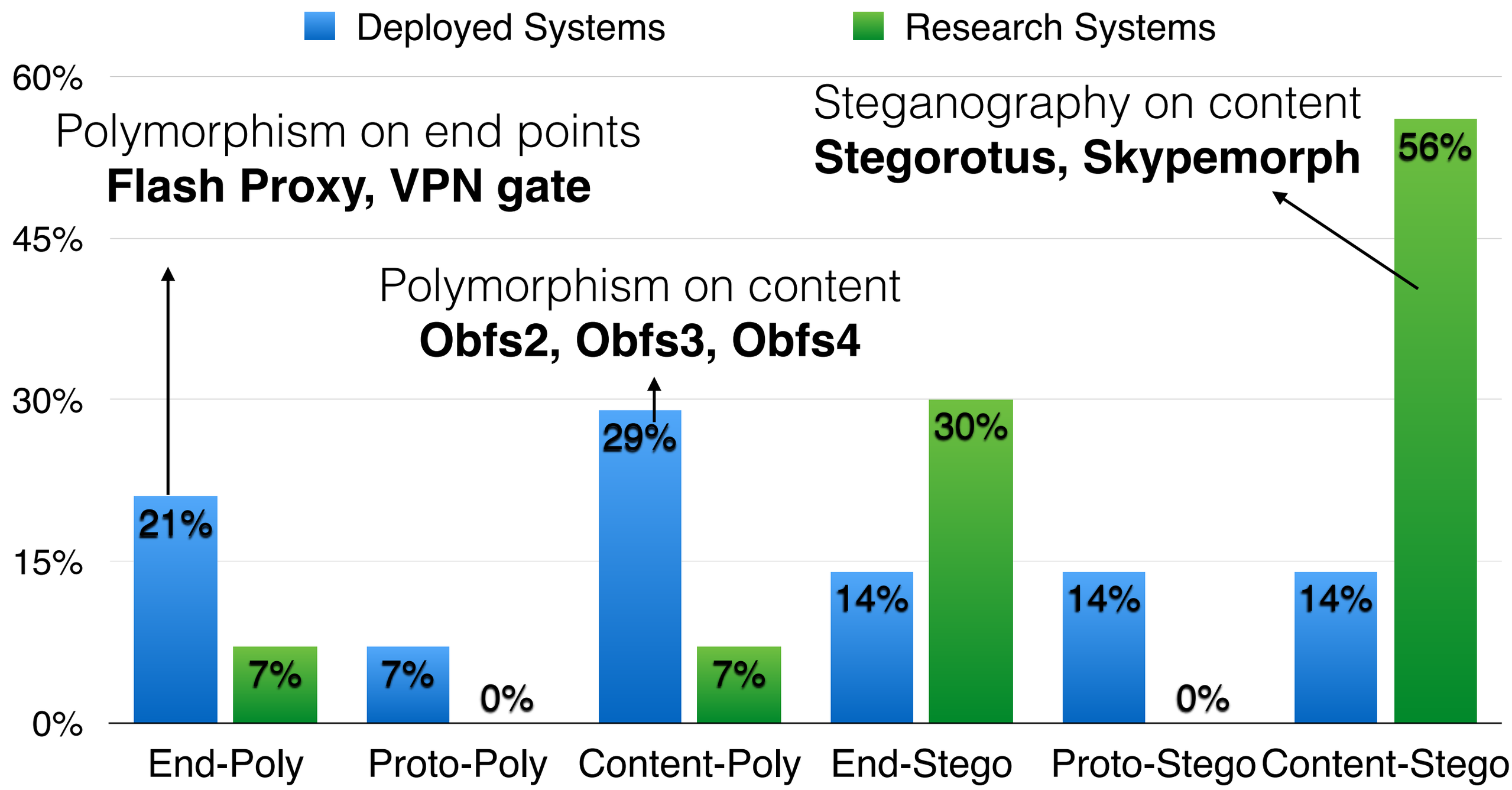
Research Vs. Practice



Research Vs. Practice



Research Vs. Practice



Research Vs. Practice

- Development cost
- End game

- Operational cost
- Arms race

How to mitigate this gap?

- Practical evaluation criteria
- We found 60 different evaluation criteria
- Different papers use different evaluation criteria

Current evaluation criteria

The criteria fall under the following broad categories:

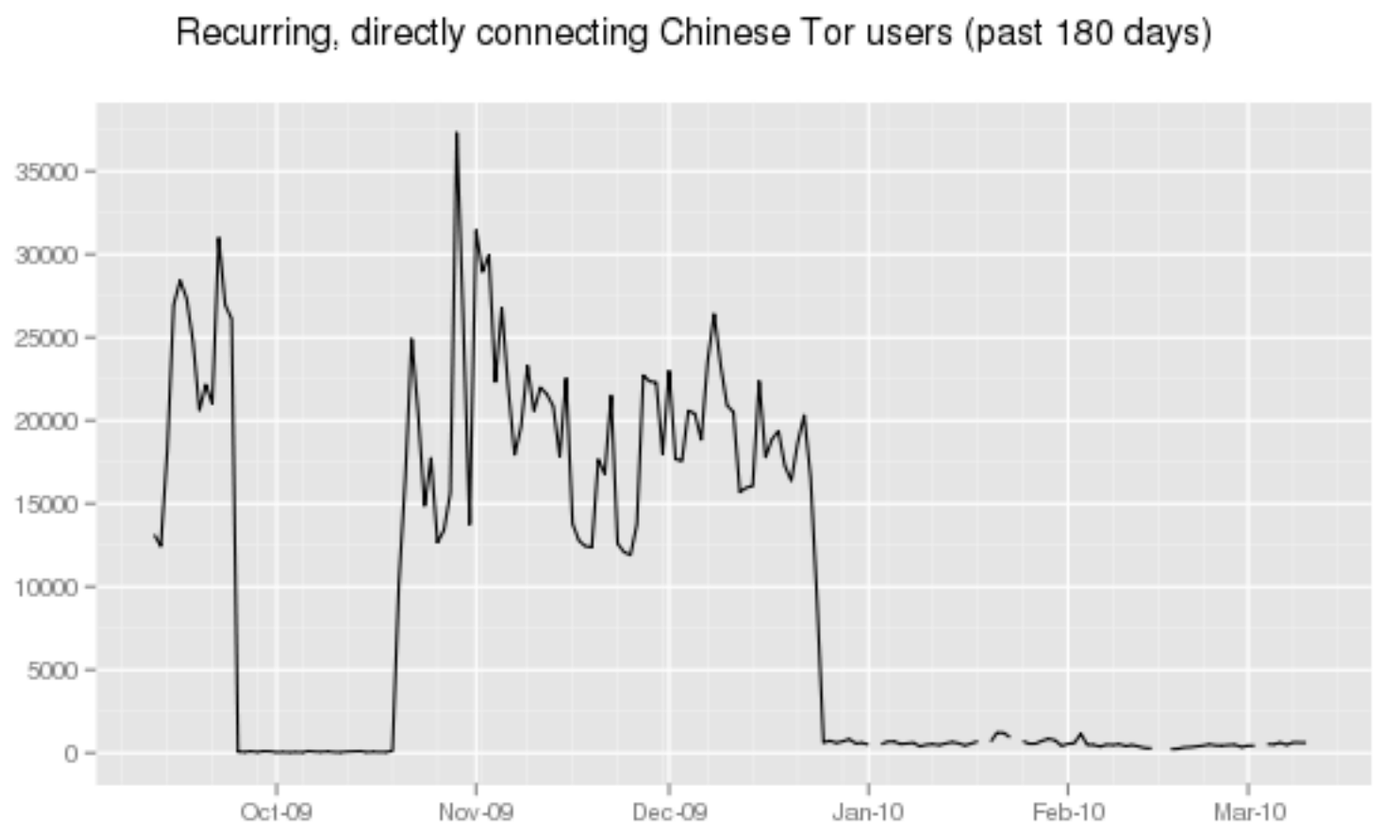
1. resistance to known attacks (e.g., address blocking, active probing),
2. cost of the evaders
3. collateral damage of the censor
4. performance,
5. traffic analysis,
6. usage.

New evaluation criteria

- **Total cost** of a system:
    - censor's cost, user's cost, system maintainer's
- **Goodput**, how much productive traffic it enables

How to find censor's cost?

- Check how long it takes to discover how to block a system



Blocking happens either before some major events or as soon as an event occurs

Discussion

- What should be the effective evaluation criteria?
- Any known blocking events that we missed?
- List of attacks:

  http://eecs.berkeley.edu/~sa499/tor_timeline.pdf

- Researchers: expect email from us!