A Critical Evaluation of Website Fingerprinting Attacks

Marc Juarez¹, Sadia Afroz², Gunes Acar¹, Claudia Diaz¹, Rachel Greenstadt³

¹ KU Leuven, Dept. of Electrical Engineering (ESAT), COSIC, iMinds
² UC Berkeley
³ Drexel University
Threat model
Motivation

- Unrealistic assumptions on:
  - Adversary capabilities (e.g., train on user data)
  - User settings (e.g., TBB version)
  - Nature of the Internet (e.g., staleness)

- M. Perry’s post in Tor blog
  - False positives matter a lot
Contributions

- Comparative evaluation
- 35K open world
- Classify-verify
- Model adversary’s cost
Results and Conclusions

- **70% accuracy drop (worst case)**
  - Still, not dismissing the attack
  - Defenses might be cheaper than expected

- **60% less false positives**
  - Verification mitigates but doesn’t solve the problem
Thanks for your attention.