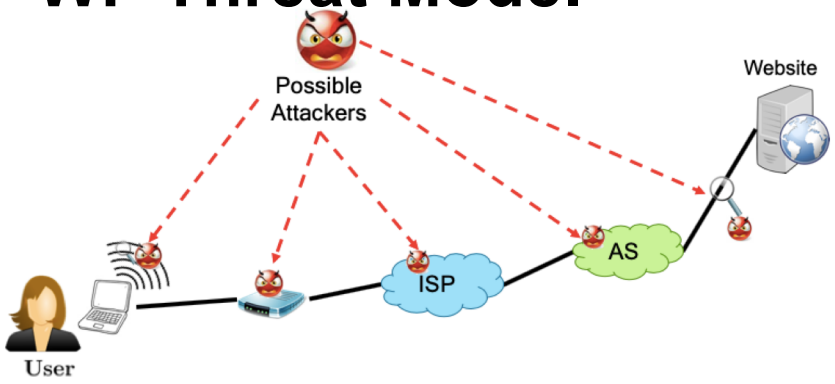
Website Fingerprinting (WF) Attacks and Defenses with Deep Learning

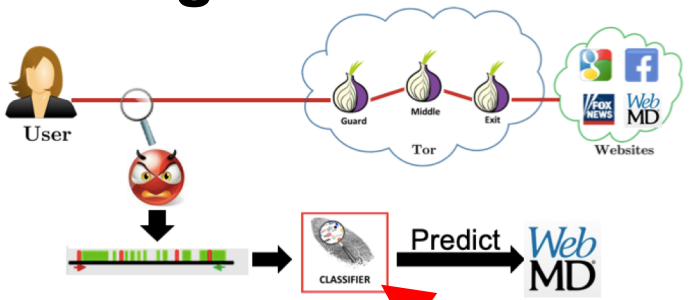
Matt Wright matthew.wright@rit.edu

WF Threat Model



Impact: Many types of attackers can use WF to harm privacy by watching users' online activity

WF against Tor

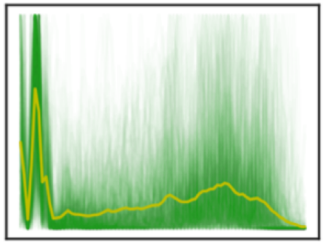


Our result [CCS '18]: ***98%*** *accuracy*

(deep learning goes here)

Novel Defenses

- Use *adversarial examples*
- Insights from visualizations of what deep learning "sees"



RIT | Rochester Institute of Technology

1816851