TTP: Defending Against Website Fingerprinting in Tor

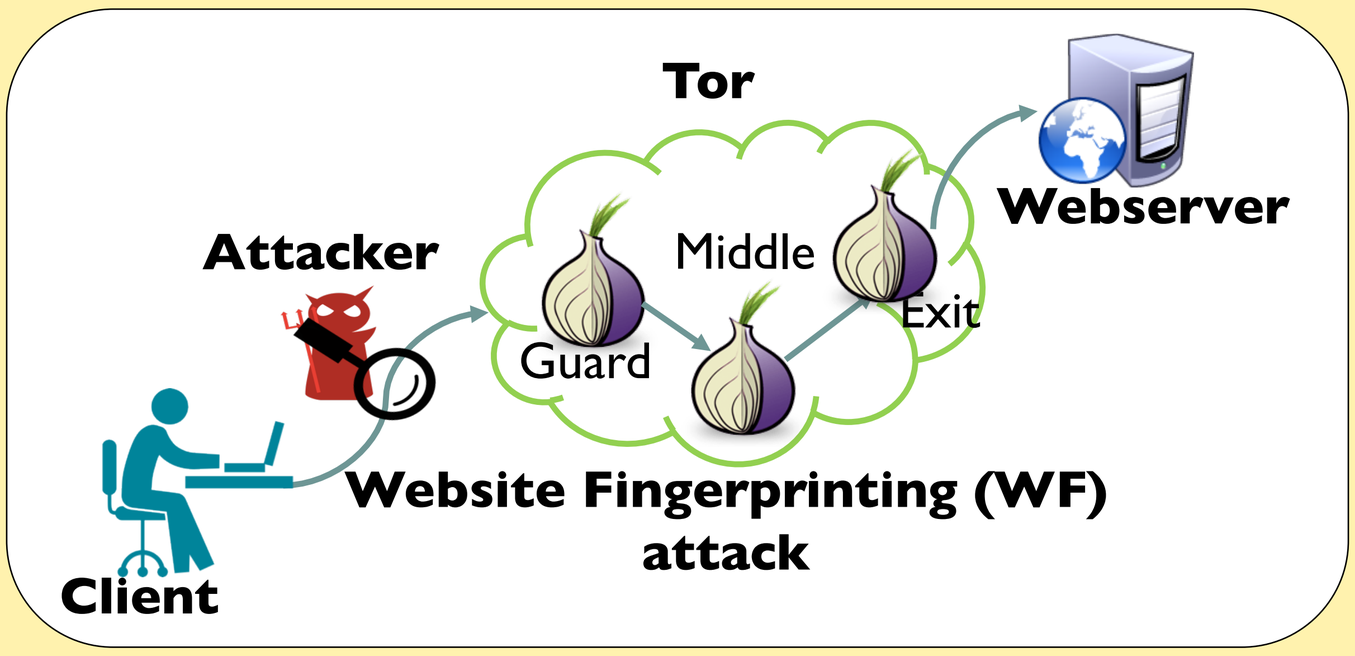
PIs: Roger Dingledine, The Tor Project
Matthew Wright, Rochester Institute of Technology

Website Fingerprinting

Website Fingerprinting (WF) attacks reveal a user's web browsing activity to an eavesdropper, even when using Tor.

Goals:

- Prevent the attack
- Cost as little overhead as possible
- Provide a good user experience



Approach

State-of-the-art attacks

- ML classifiers: k-NN, SVM
- Key features: Bursts of traffic
- 90+% accuracy
- Even in the 'open-world' setting

Other Defenses

- Add delays: 2-3x
- Heavy bandwidth costs
- Require a large DB of websites

Adaptive Padding (AP)

- Profile 'typical' web activity
- Look for surprising gaps in traffic
- Fill the gaps with padding

AP Histograms

- Training: Profile delays between cells
- Monitor traffic: BURST histogram
  - Draw a token, wait for traffic
  - No traffic? Surprising gap!
  - Switch into Gap mode
- Add a Fake Burst: GAP histogram

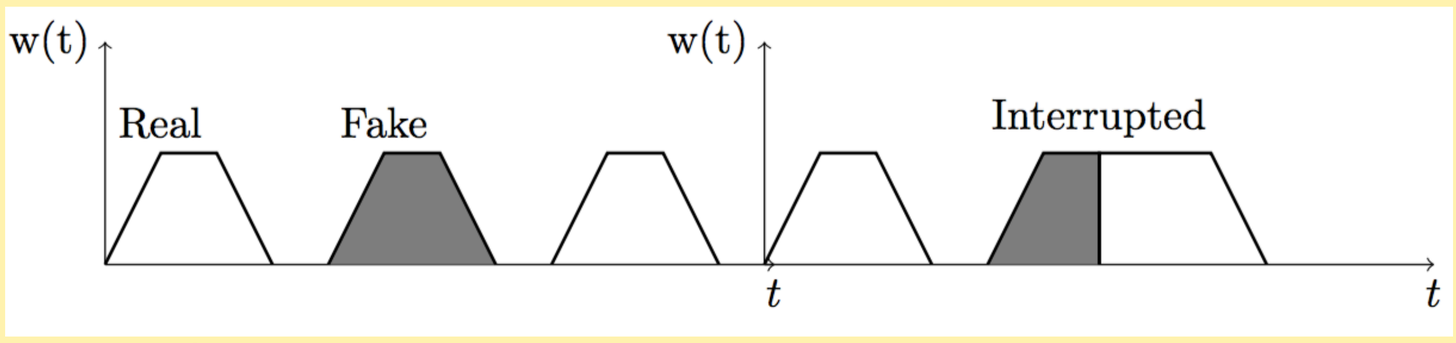


Diagram of how AP works. Time is on the x-axis and instantaneous bandwidth is on the y-axis. Real bursts (white) are used in WF to identify a website, so we add fake bursts (grey), which can be interrupted by real traffic as shown on the right. The BURST histogram is used during real bursts, while the GAP histogram is used to generate a fake burst.

WTF-PAD

- Engineering AP for Tor
- Receive histograms
- Control messages
- Stopping condition
- Measuring inter-arrival distributions
- Tuning bandwidth versus security

Results

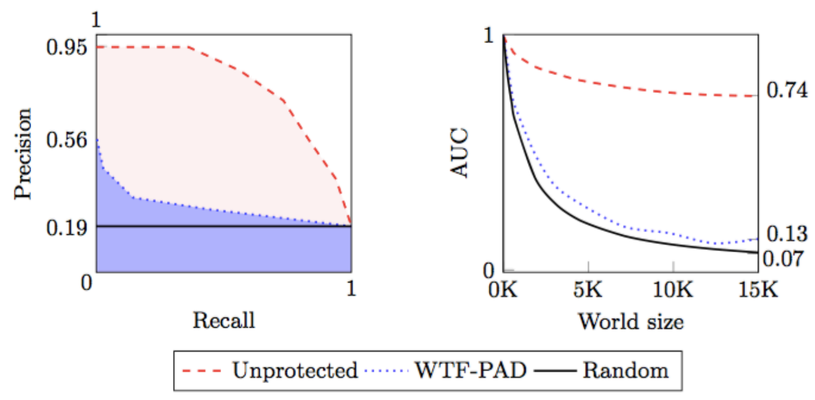


Fig. 8: The figure on the left shows the P-ROC curves for the k-NN attack on the protected and unprotected datasets for 5,000 pages. On the right, a comparison of P-ROC AUC with respect to the world size.

TTP Goals

- Develop experimental platform in Tor
- Test WTF-PAD and more attacks
- Pick parameters, histogram selection
- Account for overheads in relay selection
- Deploy in Tor

Personnel

- Marc Juárez and Claudia Diaz, KU Leuven (COSIC)
- Mike Perry, The Tor Project

Publication

- ESORICS 2016
- Best Student Paper Award

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN