title: Break-Pad:

abstract

background:

Website fingerprinting attack is an attack that uses metadata of traffic such as the size, timing and direction to identify the target websites. This can damage the user privacy provided by anonymous networks such as Tor. In the past few years, many defense algorithms against this attack have been proposed in the literature. Tor has designed and implemented a defense framework based on WTF-PAD.

problem: gap padding, hard to find optimal timing parameters

approach: In this paper, we add the break burst function to the original Tor defense framework, and design effective and efficient padding machines based on this function.

results:

[conclusion]

1. Introductiona

background: Tor, WF, WFD, subpadding system

Tor: Recently, more and more people begin to use anonymous communication systems such as Tor to hide information about personal browsing web pages. 【tor的介绍】

However, a eavesdropper, such as a Internet service provider or a entry onion router of Tor, can launch website fingerprint attacks to identify websites visited by the user despite her use of Tor.

problem(limitation & motivation) & research question: gap padding,

目前，学术界发表了多种防御方法。Tor系统设计了机遇WTF-PAD的防御框架。but have the following limitations:

propose your claim: break-burst mechanism

to solve these limitations, we propose a break-pad

results

we summarize the conditions of our paper as follows:

1. add break-burst mechanism

2. design client padding machine with break-burst mechanism

3. find optimal parameter approach.

we orgamize the rest of the paper as follows.

2. background & related work

threat model

website fingerprinting: cumul , df

CUMUL. Panchenko et al. proposed to use a support vector machine (SVM) with the cumulative summation of bytes from each direction as input features.

k-FP. Hayes and Danezis proposed the k-fingerprinting attack(k-FP). K-FP uses a random forest to extract the fingerprint of the target page, and uses a k-NN classifier to classify the fingerprint. First, Kfp feed statistical features to train the random forest classifier and obtain the fingerprint set of the training data and the trained random forest.

a website fingerprint is represented by the leaf index sequence of trees in the trained random forest.

they feed these new feature vectors to a k-NN classifier.

It compares distances between fingerprints and selects the k closest fingerprints to decide the test instance's label.

wfd

tor padding subsystem

3. tor padding framework with break-pad mechanism

3.1 motivation

3.2 break-pad scheme

4. padding machine with break-pad

1. hyperparameter tunning

5. evaluation

5.1 experimental setup

1) simulator

2) deployment details

3) dataset

4) evaluation metrics: open-world classification metrics

5.2 experimental results

6. discussion and limitations

7. conclusion

restate your claim more fully

指明新的重要意义，实际应用，提出新的研究。 point out a new significance, a practical application, or new research

acknowledgements

We thank the anonymous reviewers for their helpful feedback.Thanks for A's help on the dataset

availability

references

cumul, kfp, df, wtf-pad,

appendix

A August Padding Machines

A.1 Client-side machine

A.2 Relay-side machine

B dataset sizes