PERCIVAL: Making in-browser perceptual ad blocking practical with deep learning

Zainul Abi Din, Panagiotis Tigas, Samuel T. King, Benjamin Livshits
Web pages compose content and ads from multiple domains
Web pages compose content from multiple domains

[Diagram showing the process of web pages composing content from multiple domains, with requests for ad content from adnetwork.com and ad content serving from nytimes.com.]
Ad network can sell the ad space to another network [Li et al.]
Why ad blocking?

INTRUSIVE ADS AFFECT USER EXPERIENCE AND PERFORMANCE ON EDGE DEVICES. [SHAO ET AL.]
Why ad blocking?

INTRUSIVE ADS AFFECT USER EXPERIENCE AND PERFORMANCE ON EDGE DEVICES. [SHAO ET AL.]
Why ad blocking?

- Intrusive ads affect user experience and performance on edge devices. [Shao et al.]
- Ad distribution channels have been used to distribute malware. [Xing et al.]
Why ad blocking?

- Intrusive ads affect user experience and performance on edge devices. [Shao et al.]
- Ad distribution channels have been used to distribute malware. [Xing et al.]
- Advertisers track users to identify them across websites. [Lerner et al.]
Existing Ad blocking solutions use handcrafted, crowd-sourced filter-lists like EasyList.
Existing Ad blocking solutions use handcrafted, crowd-sourced filter-lists like EasyList.
Existing Ad blocking solutions use handcrafted, crowd-sourced filter-lists like EasyList.
Existing Ad blocking solutions use handcrafted, crowd-sourced filter-lists like EasyList.
Existing Techniques fall short

Filter-list based blocking can easily be broken – by changing the URL or page markup

There are a lot of redundant un-matched rules [Snyder et al.]

Updating the rules takes a lot of time [Iqbal et al.]
Perceptual Ad Blocking [Storey et al.]

Looks at the content of the ad
Perceptual Ad Blocking

Looks at the content of the ad

And not at the markup
Perceptual ad blockers examine content from a user’s perspective

The intended audience for advertisements are humans and not the browser
Perceptual ad blockers examine content from a user’s perspective

The intended audience for advertisements are humans and not the browser.

Operate on rendered content.
Existing perceptual ad blockers also fall short

AD BLOCKERS ONLY LOOK AT HIGH LEVEL FEATURES LIKE AD CHOICES LOGO OR TEXT IN THE IMAGE [STOREY ET AL.]
Existing perceptual ad blockers also fall short

- AD BLOCKERS ONLY LOOK AT HIGH LEVEL FEATURES LIKE AD CHOICES LOGO OR TEXT IN THE IMAGE [STOREY ET AL.]
- OTHERS ARE PROHIBITIVELY LARGE AND SLOW FOR PRODUCTION DEPLOYMENT [SENTINEL ET AL.]
Existing perceptual ad blockers also fall short

AD BLOCKERS ONLY LOOK AT HIGH LEVEL FEATURES LIKE AD CHOICES LOGO OR TEXT IN THE IMAGE [STOREY ET AL.]

OTHERS ARE PROHIBITIVELY LARGE AND SLOW FOR PRODUCTION DEPLOYMENT [SENTINEL ET AL.]

WORK AT THE EXTENSION LAYER [AD HIGHLIGHTER, STOREY ET AL.]
PERCIVAL looks at the entire ad and non-ad content (images, videos, animations etc.) through the lens of a convolution neural network to filter ad content.
PERCIVAL looks at the entire ad and non-ad content (images, videos, animations etc.) through the lens of a convolution neural network to filter ad content.
PERCIVAL looks at the entire ad and non-ad content through the lens of a convolutional neural network (CNN) to filter ads.
Overall Architecture of PERCIVAL in the browser.

PERCIVAL runs in the rendering engine of the browser.
PERCIVAL intercepts all visual content obtained during page execution and blocks ad content.
Outline

- Challenges
- Design principles
- Design
- Evaluation
- Demo
- Conclusion
Deep CNNs can beat humans on ILSVRC

Error rate vs Year

Deep Learning

Human Error rate = 5.1
However

![Error rate vs Year](image-url)
Slow inference times

On 16 core Arm Cortex-A72 CPU

Error rate vs Year

275ms [Liu et al.]
575ms [Liu et al.]
351ms [Liu et al.]
Running deep CNNs in the browser in real time is non-trivial. Need smaller models with high-accuracy. All the visual content must go through the CNN, so need to keep the browser responsive with efficient design.
PERCIVAL: Design Principles

- Run in the browser
- Run at a choke point
- Run in parallel
- Run fast and be small
Browser: Has two main processes.

<table>
<thead>
<tr>
<th>Browser Process</th>
<th>Main Thread</th>
<th>IO Thread</th>
</tr>
</thead>
<tbody>
<tr>
<td>Renderer Process</td>
<td>Main Thread</td>
<td>IO Thread</td>
</tr>
</tbody>
</table>

Rendering Engine: BLINK runs in the renderer process

Principle 1: Run in the browser
BLINK: Converts code to pixels on screen
BLINK: Converts code to pixels on screen

• Parse the HTML to create the DOM tree
BLINK: Converts code to pixels on screen

• Parse the style sheets to determine how to display content
BLINK: Converts code to pixels on screen

- Use the DOM and CSS to create the layout tree.
BLINK: Converts code to pixels on screen

- Other operations like paint operations, encode draw commands etc. to create display items.
BLINK: Converts code to pixels on screen

- Layout and paint stages create display items, which can have images that need decoding
BLINK: Converts code to pixels on screen

- Turn display items into bitmaps
BLINK: Converts code to pixels on screen

- Low level GPU primitives using SKIA
Finally: pixels on screen
With PERCIVAL: pixels on screen

PERCIVAL intercepts every image and blocks rendering of images classified as ads

Principle 2: Run at a choke point
Blink creates many worker threads to decode and raster in parallel

<table>
<thead>
<tr>
<th>Worker thread 1</th>
<th>Image Decode Task</th>
<th>Raster Task</th>
<th>PERCIVAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worker thread 2</td>
<td>Image Decode Task</td>
<td>Raster Task</td>
<td>PERCIVAL</td>
</tr>
</tbody>
</table>

In PERCIVAL, model inference is thread safe.
PERCIVAL: Implementation

```c++
#include<percival.h>

int callPercival(void* pixels){
    return model.predict(pixels);
}

void processImage(void* pixels){
    //………..
    //………..
    //………..
}
```
PERCIVAL: Implementation

We use SqueezeNet[landola et al.] as our base network. We refine the network to remove parameter heavy later layers as we gather and train with more data.

We use a singleton design pattern, where the model is loaded on the first invocation only.

The model inference is thread safe.

Principle 4: Be small and fast
Evaluation: Performance

Mean render time impact on Alexa top 5000 URLs.
Evaluation: Performance

Mean render time impact on Alexa top 5000 URLs.

Percival adds 4.55% or 178.23 MS to Chromium and 19.07% or 281.85 MS overhead to Brave.
Evaluation: Performance

Mean render time impact on Alexa top 5000 URLs.

Percival adds 4.55% or 178.23 MS to Chromium and 19.07 % or 281.85 MS overhead to Brave.

CDF of mean render time
Evaluation: with a microbenchmark

First meaningful paint: Time it takes to display content on the user’s screen.
Evaluation: with a microbenchmark

First meaningful paint: Time it takes to display content on the user’s screen.

We measure first meaningful paint on a static html page with 100 images.
Evaluation: with a microbenchmark

First meaningful paint: Time it takes to display content on the user’s screen.

We measure first meaningful paint on a static html page with 100 images.

PERCIVAL adds 120ms to Chromium and 140ms to Brave
Evaluation: Accuracy on Facebook ads

Facebook has ads on the right-side column and sponsored content embedded in the feed.
Evaluation: Accuracy on Facebook ads

Facebook has ads on the right-side column and sponsored content embedded in the feed.

Metrics:
- TP: No of ads in right-side column or sponsored content blocked
- FP: No images in the remaining portion of the web page that PERCIVAL incorrectly blocks
- TN: No of images rendered in the remaining content
- FN: No of ads not blocked
Evaluation: Accuracy on Facebook ads

Facebook has ads on the right-side column and sponsored content embedded in the feed.

We browse the Facebook website for 35 days with PERCIVAL and report the results.
Evaluation: Accuracy on Facebook ads

Facebook has ads on the right-side column and sponsored content embedded in the feed.

We browse the Facebook website for 35 days with PERCIVAL and report the results.

```
<table>
<thead>
<tr>
<th>Ads</th>
<th>No-Ads</th>
<th>Accuracy</th>
<th>FP</th>
<th>FN</th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>354</td>
<td>1,830</td>
<td>92.0%</td>
<td>68</td>
<td>106</td>
<td>78.4%</td>
<td>70.0%</td>
</tr>
</tbody>
</table>
```
Evaluation: Accuracy on Facebook ads

Facebook has ads on the right-side column and sponsored content embedded in the feed.

We browse the Facebook website for 35 days with PERCIVAL and report the results.

<table>
<thead>
<tr>
<th>Ads</th>
<th>No-Ads</th>
<th>Accuracy</th>
<th>FP</th>
<th>FN</th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>354</td>
<td>1,830</td>
<td>92.0%</td>
<td>68</td>
<td>106</td>
<td>78.4%</td>
<td>70.0%</td>
</tr>
</tbody>
</table>

Training a customized user model achieved a precision of 88.04% and a recall of 97.25%
Evaluation: Accuracy on non-English languages

- We tested on multiple non-English languages.

<table>
<thead>
<tr>
<th>Language</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic</td>
<td>81.3%</td>
<td>83.3%</td>
<td>82.5%</td>
</tr>
<tr>
<td>Spanish</td>
<td>95.1%</td>
<td>76.8%</td>
<td>88.9%</td>
</tr>
<tr>
<td>French</td>
<td>93.9%</td>
<td>77.6%</td>
<td>90.4%</td>
</tr>
<tr>
<td>Korean</td>
<td>76.9%</td>
<td>54.0%</td>
<td>92.0%</td>
</tr>
<tr>
<td>Chinese</td>
<td>80.4%</td>
<td>74.2%</td>
<td>71.5%</td>
</tr>
</tbody>
</table>

Side benefit of Deep learning, it generalizes well.

PERCIVAL blocking Portuguese ads.
Adversarial attacks against PERCIVAL and defenses.

Recently Tramèr et al. showed Perceptual Ad blockers including PERCIVAL are vulnerable to adversarial attacks.
Adversarial attacks against PERCIVAL and defenses.

Recently Tramèr et al. showed Perceptual Ad blockers including PERCIVAL are vulnerable to adversarial attacks.

However, only one attack from this work evades PERCIVAL
Adversarial attacks against PERCIVAL and defenses.

Recently Tramèr et al. showed Perceptual Ad blockers including PERCIVAL are vulnerable to adversarial attacks.

However, only one attack from this work evades PERCIVAL.

To address this, we updated the model from SqueezeNet to MobilenetV2 and re-trained with original data. The updated model was able to correctly classify all the images. ~ 9 minutes to train
Adversarial attacks against PERCIVAL and defenses.

Recently Tramèr et al. showed Perceptual Ad blockers including PERCIVAL are vulnerable to adversarial attacks.

However, only one attack from this work evades PERCIVAL.

To address this, we changed the model from SqueezeNet to MobilenetV2 and re-trained with original data. The updated model was able to correctly classify all the images. ~ 9 minutes to train

PERCIVAL is smaller than the average web-page size and regular updating is not an issue.
More defenses and Future work

Client-Side Training:
If model is trained client side, every user has a different version of the model.
More defenses and Future work

Client-Side Training:
If model is trained client side, every user has a different version of the model.

Recent research on adversarial training is promising.
Madry et al.’s min-max optimization adversarial training demonstrates a strategy to deal with adversarial samples with security guarantees.
Conclusion

Existing ad blocking and perceptual ad blocking falls short
Conclusion

Existing ad blocking and perceptual ad blocking falls short

With PERCIVAL, it is practical to run deep learning based ad blockers directly in the rendering engine
Conclusion

Existing ad blocking and perceptual ad blocking falls short

With PERCIVAL, it is practical to run deep learning based ad blockers directly in the rendering engine

PERCIVAL,
- has minor impact on browser performance,
Conclusion

Existing ad blocking and perceptual ad blocking falls short

With PERCIVAL, it is practical to run deep learning based ad blockers directly in the rendering engine

PERCIVAL,
- has minor impact on browser performance,
- can block first-party ads,
Conclusion

Existing ad blocking and perceptual ad blocking falls short

With PERCIVAL, it is practical to run deep learning based ad blockers directly in the rendering engine

PERCIVAL,

- has minor impact on browser performance,
- can block first-party ads,
- generalizes to other locales as well.
Thank you. Please direct your questions to zdin@ucdavis.edu