



Understanding Real-world Threats to Deep Learning Models in Android Apps

Zizhuang Deng

SKLOIS, IIE, CAS[†]

School of Cyber Security, UCAS[‡]

Beijing, China

dengzizhuang@iie.ac.cn

Kai Chen ✉

SKLOIS, IIE, CAS[†]

School of Cyber Security, UCAS[‡]

BAAI*

Beijing, China

chenkai@iie.ac.cn

Guozhu Meng ✉

SKLOIS, IIE, CAS[†]

School of Cyber Security, UCAS[‡]

Beijing, China

mengguozhu@iie.ac.cn

Xiaodong Zhang

SKLOIS, IIE, CAS[†]

School of Cyber Security, UCAS[‡]

Beijing, China

zhangxiaodong@iie.ac.cn

Ke Xu

Huawei International Pte Ltd

Singapore, Singapore

xuke64@huawei.com

Yao Cheng

Huawei International Pte Ltd

Singapore, Singapore

chengyao101@huawei.com

ABSTRACT

Famous for its superior performance, deep learning (DL) has been popularly used within many applications, which also at the same time attracts various threats to the models. One primary threat is from adversarial attacks. Researchers have intensively studied this threat for several years and proposed dozens of approaches to create adversarial examples (AEs). But most of the approaches are only evaluated on limited models and datasets (e.g., MNIST, CIFAR-10). Thus, the effectiveness of attacking real-world DL models is not quite clear. In this paper, we perform the first systematic study of adversarial attacks on real-world DNN models and provide a real-world model dataset named RWM. Particularly, we design a suite of approaches to adapt current AE generation algorithms to the diverse real-world DL models, including automatically extracting DL models from Android apps, capturing the inputs and outputs of the DL models in apps, generating AEs and validating them by observing the apps' execution. For black-box DL models, we design a semantic-based approach to build suitable datasets and use them for training substitute models when performing transfer-based attacks. After analyzing 245 DL models collected from 62,583 real-world apps, we have a unique opportunity to understand the gap between real-world DL models and contemporary AE generation algorithms. To our surprise, the current AE generation algorithms can only directly attack 6.53% of the models. Benefiting from our approach, the success rate upgrades to 47.35%.

✉ Corresponding authors.

[†] Institute of Information Engineering, Chinese Academy of Sciences.

[‡] University of Chinese Academy of Sciences.

* Beijing Academy of Artificial Intelligence.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CCS '22, November 7–11, 2022, Los Angeles, CA, USA.

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9450-5/22/11...\$15.00

<https://doi.org/10.1145/3548606.3559388>

CCS CONCEPTS

• Security and privacy → Software and application security.

KEYWORDS

Deep learning; On-device model; Adversarial attack; Android app;

ACM Reference Format:

Zizhuang Deng, Kai Chen ✉, Guozhu Meng ✉, Xiaodong Zhang, Ke Xu, and Yao Cheng. 2022. Understanding Real-world Threats to Deep Learning Models in Android Apps. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, November 7–11, 2022, Los Angeles, CA, USA. ACM, New York, NY, USA, 15 pages. <https://doi.org/10.1145/3548606.3559388>

1 INTRODUCTION

Deep learning (DL) models, as known for their comparable or even better performance than human experts in some areas, have been widely adopted in various areas such as computer vision, object detection and speech recognition [4, 11, 79], which also brings broader use of DL models in mobile applications (*apps* for short). For example, the app PayPal [18] authenticates users through face recognition; the app Google Assistant [4] identifies and executes users' voice commands through speech recognition. Both of the two apps have more than 10 million users with 50 million downloads. To reduce the heavy burden of computation on the server, DL models are often designed to be stored in client-side apps. However, at the same time, the models are exposed to end-users or attackers who may leverage state-of-the-art approaches to breach the apps' defenses and finally threaten the security and privacy of users, especially when the models are undertaking security-critical tasks, e.g., authentication through face recognition and money transfer through scanning bank cards.

Among the attacks to DL models, adversarial attacks [27, 37, 76] are considered as one of the most severe. It can fool the DL models through a crafted input. By adding a few perturbations on an original input (e.g., an image, a piece of audio), despite being unnoticed to humans, the new input can let a vulnerable model misclassify it to an arbitrary category. According to recent studies [48], deep

neural networks (DNNs) are often inevitably vulnerable to adversarial attacks according to the evaluation on popular models such as VGGNet [69], ResNet [41] and GCN [74] using open datasets (e.g., MNIST [53], CIFAR-10 [51], ImageNet [30] and COCO Dataset [56]). However, it is less known whether the real-world DNN models in mobile apps can be attacked. Nor do we know the real impact of successful attacks. **Thus, in this work, we aim to understand whether the DNN models in mobile apps are affected by such threats, and if so, the severity of the threats. Last, we provide the RWM dataset we collected and used in this work that could benefit researchers in understanding the limitations of current attacks and motivate them to design better attacks against real-world models.**

Challenges in performing real-world attacks. Quite different from previous research (e.g., DeepSec [57], RealSafe [31]) whose goals are often emphasized on evaluating the attack approaches, our research is end-to-end, which considers how to automatically extract DNN models from mobile apps, convert them into the forms that can be accepted by those attack approaches, generate AEs, and validate the results. The reason for extracting models is that dynamically analyzing all the models in apps would cost a lot of time and resources. Thus, firstly, one main challenge is to automatically extract models from mobile apps. After manually analyzing some apps, we find that the DNN models in the apps are not in fixed locations, but could be in any directories. What makes the extraction even more challenging is that the models are often with various file names, or even protected by encryption. Thus, merely searching through keywords would not work.

Secondly, even if the models are successfully extracted, they cannot be directly fed into the attacking approaches since the models' inputs and outputs, which are critical for the attacking approaches to generate reasonable AEs, are unknown. For example, in order to attack a DNN model GoogleLeNet [37], the input is an image of panda and the output (i.e., labels) is "panda", which is usually assumed to be known to attackers by default. However, when attacking real-world models in apps, such inputs/outputs are *not* known. They are not simply stored in any file in mobile apps. Instead, the information about the inputs and outputs is in the semantics of the app code. For example, an app for authentication takes a photo of a user and transforms the photo into a specific format to fit the DNN model. Only by understanding the semantics of the app code, we can correctly extract the inputs and outputs. Thus, accurately identifying the code for handling inputs and outputs and understanding the code are important to successful attacks.

Thirdly, it is challenging to automatically generate and verify AEs. For white-box models, it is necessary to translate the Java code for preprocessing (e.g., normalization) in the app to Python code for AE generation. As we know, there are no such APIs in Java that allow us to perform AE attacks or even calculate gradients. For black-box models (not using a public framework, such as Sensory [9]), we can perform a transfer-based attack by attacking a white-box substitute model. However, the challenge lies in building a suitable alternative dataset to train the substitute model. The alternative training dataset is required to only include the data with the same semantics indicated by the apps' output labels.

Our approach. To address the challenges described above, we design an approach and build a tool called AdvDroid to perform large-scale end-to-end attacks on the DNN models in mobile apps, including automatically extracting the on-device DNN models, figuring out their input formats and output labels, generating AEs through various attacking approaches and validating the generated AEs, which in turn measures the performance of various AE generation algorithms. In particular, to address the first challenge, we find that no matter how the model's filename and location are changed, the app would finally load the model through the APIs provided by DL frameworks. Even if the model is encrypted, the app would decrypt the model in memory before using it for inference. Based on this observation, AdvDroid performs a semantic-guided method to extract the model file. In particular, if the model is encrypted, AdvDroid tries to automatically trigger the code that loads the model (called *Model Inference Site* or *MIS* for short). After the app loads the model, AdvDroid dynamically extracts the decrypted model from memory through API hooking.

Then, AdvDroid infers the inputs and outputs of the model (called *model interfaces*). To achieve this goal, AdvDroid first locates the MIS, then performs data flow analysis with cross references from MIS. We also design tailored static data flow analysis to quickly determine whether there exists a path from inputs (i.e., source) to the MIS (i.e., sink), and if so, how the app preprocesses the inputs. Also, from the MIS, AdvDroid does forward slicing to locate and recognize the outputs. The extracted models are treated as being white-box if they can be loaded with known DL frameworks and their interface is recognized. Otherwise, it requires more steps to attack black-box models that cannot be loaded out of the app. Note that, we focus on the models for image classification and object detection in this study, as they occupy the majority (70.31%) of the on-devices models.

To attack a black-box model, we leverage transfer-based attacks. As we know, such attacks need to train a substitute model which requires suitable inputs and labels from the target black-box model. The inputs should be meaningful to the model; otherwise, the substitute model may not be trained closely enough to the target model, which would make the attacks less successful. To build such a dataset, we leverage the output labels extracted from the apps in the previous step. By comparing the semantics of the output labels in the app with the labels in the open-source datasets such as ImageNet [30], we can find a number of inputs with labels of similar meanings. We also leverage Google Image Search [5] and Open Images Dataset [8] to find more inputs and extend the dataset. Then we could use this dataset to train a substitute model for attacking.

Findings. After analyzing 62,583 apps, we find that 568 apps have 960 on-device DNN models. After deduplicating the extracted models, we obtain 245 unique on-device DNN models. Among them, 177 models are white-box models which use public DL frameworks; 60 models are protected through encryption; 8 models are black-box, which means that no public DL frameworks are used. Only 16 models (6.53%) of 245 models can be directly attacked by the popular attacking approaches. In contrast, using our semantic-based model interface reasoning, our approach boosts the attack success rate on model (ASR_m) from 6.53% to 47.35% (116/245). Benefiting from the unique opportunity to observe the attacks on the real-world

models, we have a set of interesting findings. We find that the success rates of adversarial attacks on real-world quantized models are generally 5-10% lower than those in corresponding unquantized versions. We also find that real-world model quantization makes on-device models more robust to adversarial attacks. According to our results, the C&W [23] method has the highest attack success rate on sample (ASR_s) among the adversarial attacks.

Contributions The contributions of this work are as follows.

- *Large-scale adversarial attacks on real-world DNN models.* We propose the first systematic study on adversarial attacks by collecting real-world DNN models and adapting them to current adversarial attacks. Particularly, we perform on-device model extraction to build a real-world model dataset RWM including 245 unique models. For each model, we build a test dataset through semantic analysis on the apps. We also adapt the models to current adversarial attacks through a suite of new techniques, including interface reasoning (i.e., model I/O analysis) and semantic-based training data generation. The RWM dataset is released at <https://github.com/AdvDroid/advdroid-pro>.

- *New findings.* By analyzing the real-world models, we have the unique opportunity to understand the gap between the capability of the popularly studied adversarial attacks and the real-world situations of deployed DNN models. We find that the real-world models are more difficult to attack (with a very low attack success rate ASR_m) than the commonly-used models/datasets. Among the attacks, the C&W method has the best performance in attacking the real-world models.

2 BACKGROUND

2.1 Mobile DL Frameworks

With the growing device computational power, advanced mobile hardware accelerating techniques [25, 28, 39] and abundant RAM resource, an inference on edge devices gains its momentum nowadays. Especially due to the increasing demand of privacy protection, on-device inference is bound to be a pivot in the near future. Technically, DL models should be first quantized for fitting the low bit-width mobile platforms [49]. The quantized models are then packed into a mobile app, e.g., an APK file. On Android, the models usually locate at *assets* folders or exist as raw resource of varying file formats attributed to different DL frameworks. An app may be equipped with multiple models, even developed on different frameworks, which together perform complex functions such as identifying road conditions, including traffic lights and construction zones. On the other hand, one model may be deployed on multiple apps to accomplish the same tasks. For example, developers like to use open-source models from TFHub [10]. The model file includes the model structure and parameters, and hence there is no need to build the model in the code. After the app is installed, the model can be loaded and run as a local module using SDK or NDK libraries of the DL framework. Functions in code receive, pre-process, and feed the data into the local model which computes locally and returns the model output.

Generally, mobile DL frameworks provide essential APIs and convenient tool sets so that developers can easily train and deploy their models on mobile devices without worrying about the detailed

matrix operation or run-time optimization. Comparing to server DL frameworks, mobile DL frameworks need to enable the model with good performance, small RAM consumption, and fast model inference. It is more light-weight, which is usually achieved by optimized kernels, pre-fused activations, and fewer dependencies.

There are many open-source frameworks and proprietary frameworks, e.g., TensorFlow Lite (TFLite) from Google [11], Caffe2 from Facebook [2]. These models, with a known format, can be invoked via public APIs. Therefore, it is relatively easy for an attacker to understand the model information as well as how the model is used in the app. However, in order to protect their proprietary models, there are companies, such as DL service provider companies to whom the model is an important intellectual property, using their own proprietary mobile DL framework. The file format of these models is unknown, and hence the model information cannot be retrieved by directly analyzing model files. It increases the barrier for attackers to retrieve any information from the model.

2.2 On-device model protection

It is of great importance to protect the models deployed on mobile devices. On one hand, as model training is expensive in both data and computational power, well-trained models are always the target of attackers. On the other hand, the disclose of the exact model structure and parameters jeopardizes the model, as the information facilitates adversarial machine learning attacks. Instead of developing a proprietary mobile DL framework with unpredictable efforts, app developers are prone to using obfuscation or encryption to protect their models [71]. Obfuscation is one cost-effective approach by obscuring any meaningful text in the stored model file. Encryption is cost-heavier than obfuscation but also provides more protection by not just obscuring meaningful text but concealing all structure and parameter information into ciphertext.

3 APPROACH

Threat Model. To collect the real-world DL models for evaluating the adversarial attacks, we assume that the adversary can obtain Android apps with DL models from markets and install them on a rooted smartphone or Android emulator locally. He can freely instrument the target apps for analysis and AE generation. In the attack scenario, we assume that the adversary can only send AEs to the victim (app) without permission to modify any environment (e.g., victim's smartphone). For example, he cannot instrument the target app.

Overview. As shown in Figure 1, AdvDroid proceeds in four stages: *model extraction*, *model interface reasoning*, *dataset generation* and *attack observer*. In the model extraction module, we compile a rule list to identify the Android apps powered by deep neural networks, i.e., containing on-device models. One app may have multiple models; one model may also be deployed by multiple apps. By tracking the calling paths of model APIs, AdvDroid can locate and then extract models statically. To cope with encrypted or packed models [71], AdvDroid performs dynamic analysis to extract the plain model files. In model interface reasoning, AdvDroid utilizes semantic analysis to infer code semantics to obtain the information of model interfaces, including input format, model output, model task and preprocessing parameters. In dataset generation, AdvDroid

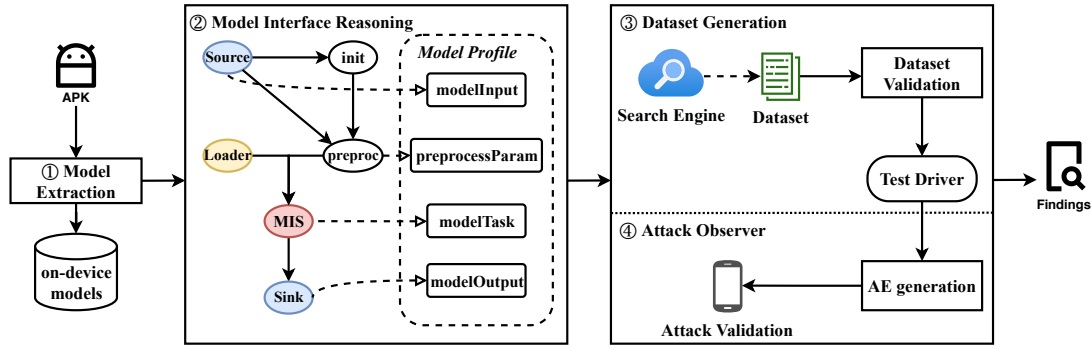


Figure 1: System overview of AdvDroid

initializes the environment for evaluating security of on-device models, which basically contains preparing drivers to load and trigger either white-box or black-box models, as well as auxiliary testing data as per model profiles. Last, we reproduce six popular white-box adversarial attacks and three black-box ones in the module of model attack observer to reveal the models' robustness and demonstrate the caused harm.

3.1 Model Extraction

Given an app, AdvDroid first checks whether the app contains an on-device DL model. If so, AdvDroid locates the model and extracts it from the app. Below we present the details.

DL App Recognition. A straightforward way to check if an app contains DL models is to check the file format of every file in the app. If the file format matches the model format, we say that a model is found. As we know, the models developed on different DL frameworks have different file formats. So we investigated the top 17 DL frameworks based on market share [75] and analyzed typical model formats in Table 4 in the Appendices¹. For example, a model developed on TFLite [11] has the format "TFL3". So if any file has the format in a given app, we can extract the file as the model file. The app containing the file is a candidate DL app.

Sometimes, apps aim to protect models by encrypting them or loading them dynamically. This makes it impossible to recognize the file format directly. To this end, we look for the code that loads the model. In most cases, the way to load models is fixed by different DL frameworks. Therefore, by identifying the code for model loading, we can ensure that the app contains the DL model. The code can also be instrumented to extract the models. We identified different file features and code features for loading models (see Table 4). With these features, we can quickly identify candidate DL apps.

Model Localization and Extraction. After obtaining candidate apps that contain on-device models, we locate the models and extract them for further analysis. We can extract the models directly if they are not protected. If a model is encrypted or dynamically loaded, we need to instrument the app for model extraction. Particularly, we divide the models into three types as follows.

- *Type A. Unprotected models using open-source frameworks.* These models are developed under open-source frameworks such as TFLite. To further verify that they can be loaded without protection, we use the loader APIs provided by the corresponding DL frameworks. For example, TFLite uses API `Interpreter.invoke` for model loading. If the target model can be loaded successfully, we say the model is Type-A.
- *Type B. Protected models using open-source frameworks.* If the model file cannot be recognized directly, the model is very likely protected (e.g., encrypted). To this end, AdvDroid hooks the code for model loading (i.e., MIS), dynamically executes the app to trigger the MIS, and then dumps the model from memory after it is loaded. The dynamic triggering of the MIS can be facilitated via constructing a sequence of UI operations that are associated with the code of model loading.
- *Type C. Models using closed source framework.* Some models may be developed with a private DL framework, so it is difficult to load them outside the apps since libraries or environmental requirements could not be satisfied. Without any details about the model, we view them as a black box and propose a dynamic approach to interact with them. More specifically, AdvDroid traces API calls during running apps, selects the APIs related to model inference, and builds a remote query service with remote procedure calls (RPCs). In such a manner, we can pass crafted data to the APIs detected during runtime to obtain model output.

Based on the above, we successfully find 960 on-device models and extract 245 distinct ones from 568 apps after deduplication by hash values. 177 (72.24%) models are of Type A, 60 (24.49%) are Type B. Besides these extracted models, 8 (3.27%) of on-device models belong to Type C.

3.2 Model Interface Reasoning

To enable security evaluation of on-device models, we need to know the model's input and output. Figure 2 illustrates how one model is loaded and executed with crafted input. First, the model is loaded from a `light_model.tflite` file via loader API "loadModel". Then the inference API "runModel" uses the loaded model for inference. It has two parameters: the model and the input "modelInput". Note that the input has been preprocessed (e.g., re-scaling). At last, the model outputs the results which are further parsed to various labels. Such input and output are important for understanding the model

¹For the content of the appendices, please refer to the released link.

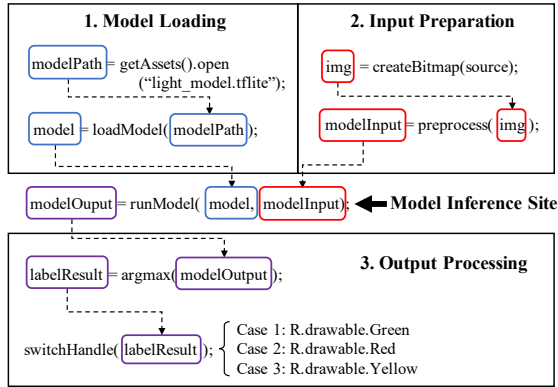


Figure 2: An example of data flow with cross references of an on-device model named “light_model.tflite”.

Algorithm 1: Model Interface Reasoning

Input: model inference site S , inter-component call graph G , and pre-defined source list I and output O

Output: model m , input i and output o

```

1  $m, i, o \leftarrow \text{parse}(S);$   $\triangleright$  initialize  $m$ ,  $i$  and  $o$  from MIS
2 while  $m \neq \text{NULL}$  do
3    $\text{nodes} \leftarrow \text{one\_step\_backward}(G, m);$   $\triangleright$  perform
   backward data flow analysis within one jump
4   if any  $n \in \text{nodes}$  points to a file then
5      $m \leftarrow n;$   $\triangleright$  find the location of model file
6     break;
7    $m \leftarrow \text{nodes};$ 
8 while  $i \neq \text{NULL}$  do
9    $\text{nodes} \leftarrow \text{one\_step\_backward}(G, i);$ 
10  foreach  $n \in \text{nodes}$  do
11    if  $n \in I$  then
12       $i \leftarrow n;$   $\triangleright$  identify the input for models
13      break;
14   $i \leftarrow \text{nodes};$ 
15 while  $o \neq \text{NULL}$  do
16   $\text{nodes} \leftarrow \text{one\_step\_forward}(G, o);$ 
17  foreach  $n \in \text{nodes}$  do
18    if  $n \in O$  then
19       $o \leftarrow n;$   $\triangleright$  identify the output for models
20      break;
21   $o \leftarrow \text{nodes};$ 
22 return  $m, i, o$ 

```

and also vital for further attacks. Therefore, we perform model interface reasoning to obtain the input and output.

To start with model interface reasoning, we define the Model Inference Site (MIS) as follows.

DEFINITION 1. A model inference site S is a concrete execution of on-device models and can be characterized as $S = \{m, i, o\}$, where m is executed model, i is the input for the model and o is the output result.

Generally, MIS associates the input and output to on-device models, which is our starting point for model interface reasoning.

Take TFLite model in Figure 2 as an example. The API “runModel” is treated as an MIS and glues the model’s input, output, and the model instance. Other DL frameworks have their own MISs, we manually summarize them in Table 5 in the Appendices. From an MIS, we adopt context-sensitive data flow analysis to track the arguments and return values as stated in Algorithm 1. In particular, considering an MIS (m, i, o) , we perform backward data flow analysis from its parameter m (i.e., model), which can finally locate the file “light_model.tflite” (Line 2-7 in Algorithm 1). From parameter i (i.e., modelInput), we are diverted to the statement “img=createBitmap(source)” and learn that the model’s input is an image (Line 8-14 in Algorithm 1). Similarly, model output can be determined by a forward data flow analysis, where we infer the output details, e.g., pre-defined labels for a classifier (Line 15-21 in Algorithm 1). Below we detail how to locate the model together with the corresponding inputs and outputs.

Model Loading. Starting from an MIS, we first need to know what model m it loads. An app may contain multiple MISs and models, which should be connected correspondingly. Data flow analysis is used here to ensure the connection. For example, in Figure 2, using the method proposed in Section 3.1, we only know that the app uses the model “light_model.tflite”. For further analysis, we locate the MIS at the statement “runModel”. Its parameter indicates the model is “model”. By backtracking from the parameter, we further locate the API loadModel and identify the model as “light_model.tflite”.

Input Preparation. We intend to infer the semantics of parameter I in MIS, which is either an image, audio file or text in deep learning tasks. We first construct an inter-component call graph (ICCG) via class hierarchy analysis [29] and perform a backward data flow analysis to determine where the parameter I comes from. The analysis is terminated upon pre-defined sources are detected. These pre-defined sources are Android APIs that we have summarized in Table 6 in the Appendices. For example, we take methods “createBitmap” and “createScaledBitmap” as the source for creating an image, and “AudioRecord” for an audio file. Oftentimes, input data needs to be transformed for suiting the model. For example, image resizing and normalization are conventional operations before being passed to a model. AdvDroid infers the resizing configuration from model input layer, where for example, (1, 224, 224, 3) denotes that the model accepts a three channel 224×224 sized image. As for image normalization, we list a number of commonly-used APIs in image processing libraries for normalization and determine the key parameters—mean and standard deviation (see “input preproc method” in Table 6 in the Appendices). Then AdvDroid performs a code search in the current class to identify the possible values. It is worth mentioning that the analysis of input transformation is usually unnecessary for a protected model as the code is dynamically triggered with the original input.

Output Processing. Here we aim to learn what results come from the model so as to prepare the necessary information for our test data. Take a classification task for example. We need to learn what types of objects (i.e., labels) the model can classify and then select well-suited data to feed. It cannot be known from viewing model structure, but instead, we can find clues from the processing code like colors in Figure 2.

Similar with input reasoning, AdvDroid identifies from the ICCG where the result generated from MIS flows to. For example, as shown in Figure 2, the app calls `switchHandle()` with model outputs as parameters and the model output is interpreted with three possible labels for a classification model. Therefore, `switch-case` and `if-else` serve as the termination condition for our forward flow analysis. Besides classification, there are other types of tasks as well as outputs for a model, e.g., segmentation, style transfer and optical character recognition. Therefore, we summarize three types of processing handlers in terms of mainstream model tasks used in our static analysis: ❶ n -dimensional array of floating-point probabilities. It usually occurs in a classification task where one element of the array represents the probability of being an object. ❷ 4-tuple of floating-point numbers. It is common in object detection to outline the boundaries of the recognized object. ❸ a matrix of floating-point numbers. It appears in a segmentation task where each element indicates what class the corresponding pixel is associated with. For a style transfer task, it represents an image and each element is the pixel value. More details about output examples can be found in Table 6.

As our AE attacks focus on image classification and object detection, we retain these two kinds of models recognized as above and determine the literal labels of their output. Sometimes, one file like “labelmap.txt” that records the label information resides in the same folder as the model. It is observed from the experiments that 50.31% (483/960) of models have such files. Otherwise, we strip the values in `switch-case` and `if-else` statements and build the label mapping accordingly. Additionally, we find that 43 apps use the labels mapping of public datasets, e.g., the output value “1” means label “Person” in dataset COCO. If all the trials fail, AdvDroid will use random initial samples for adversarial attacks.

3.3 Dataset Generation

Besides the model itself, we also need to form a dataset to evaluate the attacks. Since our adversarial attacks are mainly targeting classification tasks, sample inputs with the correct labels are required. Then by varying the input with different perturbation levels, we can evaluate the effectiveness of different attack methods. More inputs with various labels can better help evaluate attack methods.

Recall that we have already known the labels of the models. So the dataset can be automatically generated by searching for the corresponding inputs using the labels. We take inputs from popular datasets (e.g., ImageNet, Microsoft COCO) and search engines. Firstly, given a model that outputs different labels, we collect inputs with the same labels from popular datasets. For example, if a label is “cat”, AdvDroid can get inputs from the open datasets. Secondly, AdvDroid also uses search engines (e.g., Google image and Bing image) to obtain sufficient inputs. In addition to the image corpora, we also choose AudioSet [36] as audio corpora and Metatext [14] as text corpora.

However, the generated data may be not qualified for the attacks with either wrong or inaccuracy labels. For example, search engines may return a “banana” with the keyword “apple”, and images associated with “elephant” may have refined labels like “African elephant” and “tusker” in ImageNet. Therefore, we perform data

Algorithm 2: Dataset Validation on Model Outputs

Input: Dataset $D = \{(X_i, Y_i)\} (0 \leq i < N)$ contains top- N closest classes, *model* with M classes ($M \leq N$), threshold α_1 and α_2 .
Output: *labelmap*.

```

1 // cand is a 2-dimensional list to store valid samples for each index.
2 cand  $\leftarrow \emptyset$ ;
3 labelmap  $\leftarrow \emptyset$ ;
4 m  $\leftarrow \text{loader}(\text{model})$ ;
5 for sample  $\in D$  do
6   model_output  $\leftarrow \text{run\_model}(m, \text{sample})$ ;
7   index, max_conf  $\leftarrow \text{argmax}(\text{model\_output})$ ;
8   // we only count the samples with high confidence ( $> \alpha_1$ )
9   if max_conf  $> \alpha_1$  then
10    cand[index].append(sample's origin label  $Y'$ );
11 for index  $\in \text{len}(\text{cand})$  do
12   // count is a temporary dictionary that stores the number of
13   // times the label appears.
14   count  $\leftarrow \emptyset$ ;
15   for item  $\in \text{cand}[\text{index}]$  do
16     count{ $Y'$ }  $++$ ;
17   // we choose the label with the most occurrences.
18   sort(count);
19   top_label, top_cnt  $\leftarrow \text{top}_1(\text{count})$ ;
20   // we calculate the number of all samples in cand[index].
21   tot_cnt  $\leftarrow \text{sum}(\text{count})$ ;
22   // we map index to the label that occurs most frequently. Note
23   // that the number of occurrences should reach the threshold.
24   if  $\frac{\text{top\_cnt}}{\text{tot\_cnt}} > \alpha_2$  then
25     labelmap[index]  $\leftarrow \text{top\_label}$ ;
26 return labelmap

```

validation to get more quality data based on Algorithm 2. The inputs to Algorithm 2 are top- N closest classes, the model with M classes, and two thresholds α_1 and α_2 . The output is a *labelmap* that maps model labels (numeric values) to strings describing the label. In particular, we first feed the data into the model and get the inference result (Line 5-10). Note that we only count the samples with high confidence value ($> \alpha_1$, Line 9). AdvDroid then maps a label (returned by the model) to a string. We assume that the string appearing most frequently should better describe the label (Line 11-23). Also, note that we require that the number of occurrences should reach a threshold (Line 22). In this way, we obtain a suitable dataset for the on-device model.

3.4 Attack Observer

AdvDroid provides a platform to measure the effectiveness of different attack methods against a given on-device model. The platform accepts a model as input. It also needs to know the input and output of the model. Regarding the inputs, AdvDroid supports a template and fills the template with the resizing and normalization arguments extracted from the app. AdvDroid also fills the index-label mapping into a dictionary in the template, e.g., `labelmap<index, label>`. We also define a successful attack to an on-device model. In particular, AdvDroid randomly selects 50 samples as inputs for each class from the dataset generated in Section 3.3. If one method

can generate AEs on 80% of them, we say that the model is defeated by this attack method [23]. We implemented nine state-of-the-art adversarial attack methods (including six white-box methods and three black-box methods). Untargeted attack can satisfy our measurement requirements, and targeted attack is generally lower in ASR_s than untargeted attack. Details of the attack methods are shown in Table 3. On this platform, AdvDroid automatically mutates an input and generates adversarial samples with different levels of perturbation. In this way, the on-device models can be evaluated uniformly.

4 IMPLEMENTATION

We implement AdvDroid with more than 5,000 lines of Python code and around 500 lines of JavaScript code. AdvDroid employs and extends FlowDroid [19] to accomplish model extraction and interface reasoning. During data flow analysis, we encounter errors for 183 apps including “timeout”, “out-of-memory” and “no-sink-found”. The average size of these failed apps is 52MB. 163 of them have multiple DEX files, and the average DEX code size is around 19MB. See Appendix E for details. By debugging and fixing these errors like considering implicit call in `java.util.concurrent.Future`, we successfully reduce the number of errors to 12. For the models that cannot be directly loaded, we apply DroidBot [54] to dynamically run them, and involve manual efforts if apps are authenticated and protected via registration.

As for model testing, we set $\alpha_1 = 0.7$ and $\alpha_2 = 0.8$ typically for Algorithm 2. When performing AE attacks, AdvDroid adapts from projects Foolbox [68] and AdvBox [33] six white-box adversarial attacks, i.e., Fast Gradient Sign Method (FGSM), Projected Gradient Descent (PGD), Deepfool, Basic Iterative Method (BIM) [52], Momentum Iterative Method (MIM) [32] and C&W, and three black-box attacks, i.e., boundary attack [22], NES attack [47] and substitute model transfer attack [32, 64]. We use a large model ResNet152 as the substitute model following [31, 40]. It is pre-trained on ImageNet with 75.4% accuracy and has 60.4M parameters. For these models whose gradient information can be calculated, AdvDroid uses white-box methods. Otherwise, AdvDroid uses black-box methods, which are usually harder than white-box methods [64]. For example, although the TFLite framework is open-source, its model in our dataset lacks operators to compute gradients (see Section 8). It is known to be impossible so far to reverse TFLite to its Tensorflow model. It is because model quantization (Tensorflow to TFLite) uses int values (e.g., INT8) or low-precision floating points (e.g., FP16) to approximate and replace original full-precision floating weights that is irreversible [3]. Besides, there are no official TensorFlow APIs to support the conversion from TFLite to Tensorflow. We then re-implement the existing transfer attack methods and build our own adversarial attack toolbox which is compatible with TFLite models.

5 EVALUATION

App Dataset. We collect 62,583 apps from Google Play Store and alternative markets from May 2020 to October 2021, aiming to draw more comprehensive conclusions and identify new threats and defenses over time. From the Google play store, we crawl the top 1,000 apps at most for all of 24 categories and obtain 22,632 apps

Table 1: Distribution of different frameworks of models. Many apps use identical models so that the numbers in parentheses are counts of models after deduplication.

| Framework | Type A | Type B | Type C | Total |
|--------------|------------------|-----------------|----------------|------------------|
| Tensorflow | 153 (32) | 3 (1) | 0 | 156 (33) |
| TFLite | 271 (98) | 66 (30) | 0 | 337 (128) |
| Caffe | 26 (12) | 28 (6) | 0 | 54 (18) |
| Caffe2 | 6 (3) | 13 (4) | 0 | 19 (7) |
| PyTorch | 13 (1) | 0 | 0 | 13 (1) |
| PaddleLite | 33 (12) | 21 (5) | 0 | 54 (17) |
| NCNN | 22 (10) | 19 (9) | 0 | 41 (19) |
| MNN | 20 (7) | 14 (3) | 0 | 34 (10) |
| MindSpore | 8 (2) | 6 (2) | 0 | 14 (4) |
| SenseTime | 0 | 0 | 106 (2) | 106 (2) |
| Megvii | 0 | 0 | 110 (2) | 110 (2) |
| Sensory | 0 | 0 | 19 (1) | 19 (1) |
| -Others- | 0 | 0 | 3 (3) | 3 (3) |
| Total | 552 (177) | 170 (60) | 238 (8) | 960 (245) |

in total. Similarly, we crawl the top apps from alternative markets and obtain 39,951 apps which are deduplicated by app hash values.

Environment. The experiments are conducted on three Ubuntu 18.04 Linux servers. One with five NVIDIA Titan X GPUs, 32 cores CPU, and 128 GB RAM is used for model attack experiments, the other two both have 128 cores CPU and 256 GB RAM for Android app analysis and on-device models extraction. The attack validation experiments are conducted on a Google Pixel 2 smartphone.

Here we conduct experiments to evaluate AdvDroid and conduct comprehensive analysis of the results, in order to answer the following research questions:

- RQ1.** How effective and efficient of AdvDroid in extracting and analyzing on-device models? (see Section 5.1)
- RQ2.** How are the on-device models protected from physical theft during deployment in mobile devices? (see Section 6.1)
- RQ3.** How robust of on-device models with regards to state-of-the-art adversarial attacks? (see Section 6.2)

5.1 Effectiveness and Efficiency (RQ1)

We evaluate the effectiveness of AdvDroid for each phase.

Model extraction. AdvDroid identifies 5,573 candidate DL apps from 62,583 apps. From the 5,573 apps, AdvDroid further recognizes 568 apps containing DL models, and extracts 991 models. After a two-week manual examination, we find that 31 models are false positives. For example, some apps contain files with the extension “*.pb”. However, the file is not a model but a “protobuf” file with the same file extension as models. So our model recognition found 960 real models and yielded a false positive rate of 3.13%. Furthermore, these fake models are actually configure files: `feat.params` (12 occurrences), `METADATA.pb` (10), `ClientInfo.pb` (2), and others (7). As for false negatives, we randomly sampled 100 apps from those without DL characteristics and found no DL apps.

Model interface reasoning. We successfully identify 902 MISs, 880 input sources and 562 output labels from the extracted models. To validate the correctness, we feed specific samples into models and examine whether models return the consistent output labels. The reasoning is correct and accurate if the model to test accepts

the offered input and has the consistent output labels as inferred. Based on that, it is found that 853 (96.93%) of the input sources and 509 (90.57%) of the output handlers are correct. Additionally, apps may preprocess the input for models like resizing and normalization. AdvDroid identifies 94 such operations as well as their key parameters (e.g., mean and standard deviation in normalization).

Dataset generation. To further evaluate the quality of the generated data for models, we just feed them into our extracted models and the original in apps, and then obtain their inference results. By computing the l_2 -norm distance of two inference results, we show how consistent of the extracted models with the original. We repeat this evaluation for 10 times. In such a manner, 475 (98.55%) of models exhibit a high consistency under the threshold 0.1.

Runtime of AdvDroid. Overall, AdvDroid spends about 26 hours on extracting and attacking the models in 568 DL apps. On average, it takes AdvDroid 9.58 minutes to attack one model in white-box attacks and 69.28 minutes in black-box attacks. We also evaluate the time spent on each step. For each app, it takes about 1.25 minutes to find and extract the on-device models. The time spent on inferring inputs/outputs is 5.60 minutes. For white-box AE generation, the average time is 2.73 minutes. For black-box AE generation², the average time is 62.43 minutes.

5.2 Statistics of on-device Models

We remove the replicates from 960 extracted models via hash code and obtain 245 distinct on-device models. Here we characterize these models from the following aspects.

Model Frameworks & Accessibility. We present the frameworks used by the models as well as their accessibility in Table 1. It is observed that Tensorflow and TFLite contribute the most (16.25% and 35.10%, respectively) in the collected models. Models with Caffe2 and NCNN frameworks are only available through the native APIs, and a higher percentage of models with these frameworks (68.42% for Caffe2 and 46.34% for NCNN) have lower model accessibility (i.e., Type B models). Through our experiment, we find that 170 models are protected to some extent. Although AdvDroid extracts 960 models, only 587 (61.15%) of them can be loaded from an external loader with the model files, which contain 552 models of Type A and 35 ones of Type B. For the left, i.e., 135 models of Type B and 238 ones of Type C, we need to dynamically load and execute models in apps. In this study, AdvDroid successfully runs 41 such on-device models in the apps.

Model Task. Here we focus on what tasks the models can perform and the data types of model input. As shown in Table 2, the image-based models account for the largest share (70.31%), compared to audio-based (13.13%) and text-based (8.23%) models. There are 465 image classification models, 168 object detection models including OCR models, 29 style transfer models, and 13 pose detection models among 675 image-based models. One DL app may use several models (e.g., bank card recognition model) while one model would be used by several DL apps (e.g., NSFW detection model). On the other hand, not all models in apps will be executed during runtime. For example, some SDKs (e.g., Google Firebase) have integrated on-device models for special use. Therefore, one app that relies

Table 2: Model input types in apps of different categories

| Category | Image | Audio | Text | UNKNOWN | Total |
|---------------|------------|------------|-----------|-----------|------------|
| Photo/Video | 274 | 34 | 2 | 12 | 322 |
| Entertainment | 95 | 20 | 6 | 14 | 135 |
| Beauty | 87 | 32 | 3 | 8 | 130 |
| Tools | 27 | 10 | 21 | 14 | 72 |
| Finance | 43 | 2 | 10 | 0 | 55 |
| Communication | 32 | 5 | 2 | 9 | 48 |
| Education | 23 | 4 | 19 | 1 | 47 |
| Medical | 12 | 0 | 3 | 1 | 16 |
| -Others- | 82 | 19 | 13 | 21 | 166 |
| Total | 675 | 126 | 79 | 80 | 960 |

on the SDK may not demand the DL service, and thereby will not execute the models.

App category is associated with these models to show what types of apps are more prone to using on-device models. It is observed that *Photo/Video* apps exhibit the most interest as object detection, optical character recognition (OCR) [16], and VR/AR [15] are the more mature areas in deep learning. After manually vetting these 245 model tasks, we find that security-critical tasks account for about 20-30%. Top security-critical tasks include face recognition (23), identity card recognition (14), road condition recognition (3), malware detection (2), and so on. The models in Finance category are mainly used for face recognition, and the models in category *Communication* are mainly used for speech recognition. Besides, the apps in *Education* usually use models for OCR and keyboard typing, and the apps in *Tools* use models usually for translation to provide accessibility service.

Model Optimization. In order to reduce the size of models and raise inference efficiency, most mobile deep learning frameworks quantify numerical representation in parameters and reduce fused operators used in the training process. In the 587 loadable models that can be peeked into for network internals, there are 261 models with optimization characteristics, including quantization (238) and pruning (23). Additionally, there are 200 (84.03%) quantized models using the TFLite framework, 196 quantized models use the 8-bit uint quantization method, and the rest 42 models use 16-bit uint quantization method and else. Quantization parameters can be directly obtained from model files, for example, by calling TFLite API `interpreter.get_input_details()[0][‘quantization’]`. The most used quantized parameters are (`zero_point = 0.0078125, scale = 128`). We consider that a model pruning exists if the ratio of zero weights and biases is larger than a certain threshold (e.g., 40% [58]). As such, we find that 23 models are pruned.

6 MEASUREMENT AND FINDINGS

In this section, we conduct an empirical analysis of physical theft threat and evaluate the robustness of on-device models under adversarial attacks.

6.1 Threats of Physical Theft (RQ2)

Intellectual property infringement becomes a severe threat for deep learning models and has yet to be solved [43]. Prior research has paved a way to unveil the possibilities of stealing models through

²The iteration threshold for substitute model training is 100,000 queries.

authorized APIs [42, 50]. However, this threat is significantly worse when offline models are deployed in mobile devices where the models may be physically accessed and stolen by attackers. It shows that on-device models have already performed limited measures to protect their weights [71]. In this section, we investigate the host apps for the extracted 960 models, introduce the existing protection measures that are being used in reality and unveil the flaws threatening these models. Below we compile a list of model protection techniques from two perspectives.

System-level protection. Apps treat on-device models as a sensitive component and protect them in conventional manners.

- **Remote loading.** Models are not stored in apps so that static analysis and code viewing cannot find them. Otherwise, models are dynamically loaded from the remote during runtime and perform inference for one time. As observed, there are 4 apps that behave in such a way in our dataset. For example, we find that one app contains a DL native library and MIS “MgFaceLab:Miguface”, but the size of the associated model file “thin.tflite” is zero. By monitoring its execution, we identify that the model content comes from HTTP requests, and the model is used to extract features of face images and then upload them to one server for further detection and recognition.
- **Model encryption.** Alike other key components, on-device models are often encrypted and the ciphertext is stored locally. Apps need to decrypt ciphertext and load the model in memory for use. We find that 23 apps have taken this measure to protect their models. The popular encryption methods include simple bitwise computation (5), TEA [17] (2), AES (10), etc.
- **Model packing.** As described by the document of MACE framework [13], models can be converted to native C++ code that is much harder for parsing. That is, one model is stored as native code rather than a plain file. It is common in reality and 16 models cannot be extracted.
- **Identity authentication.** Models are only granted to specific users for use. Therefore, some apps authenticate whether the current user owns a valid authorization token. The token is generally distributed during app execution by a remote server for the registered users. For example, we find that an app requires users to register first to use the model for liveness detection.
- **Integrity verification.** It is used to verify whether models are stolen and apps are repackaged. More specifically, models may be replaced with a poisoned one, or code is changed to bypass authentication by attackers. To handle this problem, apps can compute the hash code for the model and app itself in advance. On-device inference is only conducted if integrity is verified successfully. We find 3 cases that have verified model integrity.

Model security enhancement. System-level protections can be hacked by mature techniques like instrumentation, debugging, and simulation. It is intriguing to explore the measures to enhance the security of on-device models from physical theft. In this study, we identify the following three out-of-the-box techniques.

- **Layers obfuscation.** Layers are commonly assigned with lucid names in model design. For example, “Conv2D” is a 2D convolution layer while “AvgPool2D” implies a layer of performing average pooling. We find some apps obfuscating model layer

name in our dataset, e.g., “7cff058686c711e9a0ac4ccc6ac78afa:2”. Although ineffective in protecting models from theft and misuse, it can increase the difficulty of model interpretation and further model development.

- **Weights transformation and protection.** Weights are vital for a model and should be protected as well. Prior studies have proposed several methods, e.g., placing parts of the model in TEE [20] and masking model weights during deployment and unmasking them during runtime [70]. Although we find no apps with this type of protection, it exhibits a superior efficacy in model protection and will be widely applied once the additional overhead is significantly reduced.
- **Custom operators.** Model developers may create their own operators with DL frameworks, seeking for more flexible and powerful computations beyond built-in operators (e.g., convolution, relu, pooling, normalization). These operators, in the meantime, raise the difficulty of misusing the models. Unless the attackers learn how operators compute, they cannot load and use these models. In our dataset, we find 20 models with custom operators that are defined in native libraries. For example, in app Google AR [15], an operator “MaxPoolingWithArgmax2D” is designed to perform max pooling and output the pooling indices.

Through an analysis of these protection techniques, we identify some development flaws, as described in Table 7 in the appendices. We have reported these issues to the affected vendors and received one confirmation. We also find that four issues are fixed in the newer versions. As shown in Table 7, we do find an app that applies more defenses to protect models in its new version. But it does not necessarily imply that on-device models become more secure over time. We also provide some suggestions in Section 7.

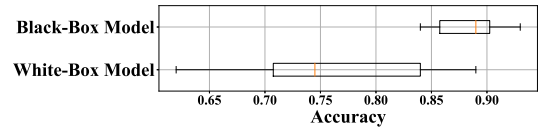


Figure 3: The accuracy of different models tested on our generated test dataset.

6.2 Threats from Adversarial Attacks (RQ3)

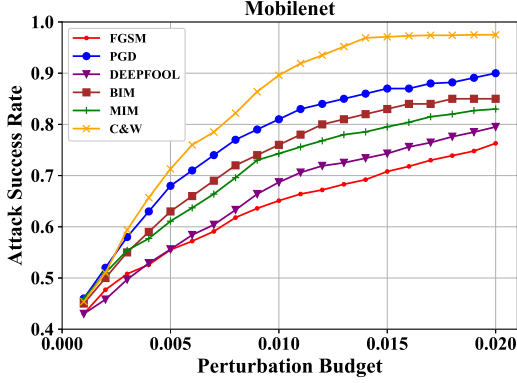
In this section, we explore how robust on-device models considering adversarial examples. Note that, we only test image-based models since the models of other types are too few to draw convincing conclusions. Even so, our attacking approach can be easily adapted to them by employing proper AE generation algorithms.

Test dataset. For each model to test, we prepare a dataset for adversarial attacks from public datasets (e.g., ImageNet [30], Open Images [8]) and Google Image. As such, we obtain 46 datasets in total for these models that contain 251,765 samples. We manually evaluate the accuracy of semantic-based training data generation. In total, 20 datasets are generated with 320 labels during white-box attacks, and 26 datasets are generated with 620 labels during black-box attacks. The accuracy of 245 models tested on our datasets is shown in Figure 3.

Table 3: Untargeted attack results with $\epsilon = 0.06$ (16/255) under the l_∞ norm

| Model Type | Test Difficulty | Num ¹ | White-box method | | | | | | Black-box method | | | Succ Num ¹ |
|------------|--------------------|------------------|------------------|-----|----------|-----|-----|-----|------------------|----------|----------|-----------------------|
| | | | FGSM | PGD | Deepfool | BIM | MIM | C&W | NES | Boundary | Transfer | |
| A | direct test | 21 | 14 | 16 | 14 | 13 | 15 | 14 | 9 | 8 | / | 16 |
| | interface adaption | 156 | 63 | 52 | 56 | 51 | 45 | 66 | 22 | 12 | / | 80 |
| B | dynamic extraction | 27 | 3 | 6 | 5 | 5 | 5 | 6 | 5 | 3 | 5 | 7 |
| | black-box query | 33 | / | / | / | / | / | / | 4 | 9 | 4 | 9 |
| C | black-box query | 8 | / | / | / | / | / | / | 3 | 1 | 3 | 4 |
| Total | | 245 | 80 | 74 | 75 | 69 | 65 | 86 | 43 | 33 | 12 | 116 |

¹ “Num” indicates the number of models, “Succ Num” indicates the number of models successfully attacked by any one method.

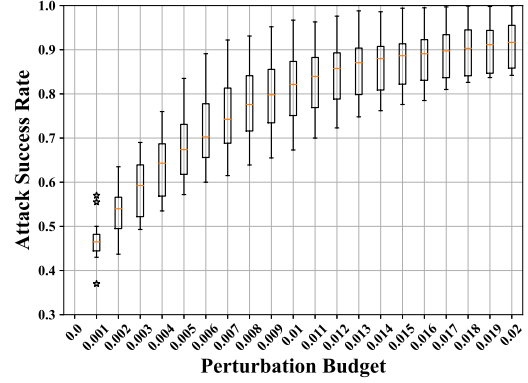
**Figure 4: Performance comparison on the most-used real-world model MobileNet against untargeted white-box algorithms under l_∞ norm.**

Test difficulties. Models are varying from test difficulties considering protection measures. Here we define four types of test difficulties to launch an adversarial attack.

- Direct test means that we can run adversarial attacks to evaluate models with no adaptations.
- Interface adaption denotes that it needs to provide any input preparation to adapt the models, like normalizing input images.
- Dynamic extraction means that the plain models need to be extracted in advance for loading outside the app.
- Black-box query necessitates an app trigger to dynamically send input samples to the model and then get the attack results, amounting to 41 models (33 Type-B and 8 Type-C models).

As shown in Table 3, 116 of 245 tested models can be successfully attacked by AEs. Except 16 Type A models of “direct test” difficulty, 100 (86.21%) of them are benefited from interface reasoning. We also find that white-box attack methods can attack more models than black-box methods.

White-box adversarial attacks. For white-box models, AdvDroid performs six different white-box attacks. The results are shown in Table 3. In terms of the number of successful attacks, i.e., ASR_m , C&W has the best performance. For the FGSM method, we draw a box plot in Figure 5 to show the distribution of ASR_s of white-box models with different perturbation budgets. We find that the distribution of ASR_s of different models gradually diverges as perturbation budget increases. Additionally, the models with high ASR_s are generally those with a large number of classes (e.g., > 10) and complicated model structures (e.g., over 100 model layers and

**Figure 5: Distribution of ASR_s of white-box models over the l_∞ perturbation budgets in untargeted FGSM attack.**

20,000 model neurons). Thus, providing real-world models is of great value to security researchers.

Using these 6 attack algorithms with best-practice parameters described in RealSafe [31] and DeepSec [57], we make a performance comparison on the same real-world model using different attack algorithms. For instance, we choose the most-used real-world model MobileNet as our target and the results are shown in Figure 4. We also select three popular DNNs for testing—ResNet, MnasNet, and InceptionNet. For each model, we compute the ASR_s of six attack algorithms on the same dataset from ImageNet. We find that the most effective algorithm against real-world models is method C&W, but it is slower compared to other algorithms.

Since 40.55% (238/587) of models have been quantized before being deployed on edge devices, we conduct another experiment to quantify the influence of model quantization and determine the main reason for the ASR_m gap. We randomly select 20 unquantized models and also convert them into 20 quantized ones to perform 6 white-box attacks. The models are all from the real world and the results are shown in Figure 6. We attack each model at different perturbation budgets, ranging from 0 to 0.02 with a stride of 0.001, and find that the ASR_s of the quantized models is lower than that of the unquantized models. At the perturbation budget 0.02, the ASR_s difference between the quantized model and the unquantized model can be 5–10%. The root cause of this problem is that quantized models have a certain degree of gradient masking [64].

Moreover, quantized models have poor transferability with AEs generated from unquantized models. This phenomenon is consistent with prior studies. For example, Galloway et al. [35] point

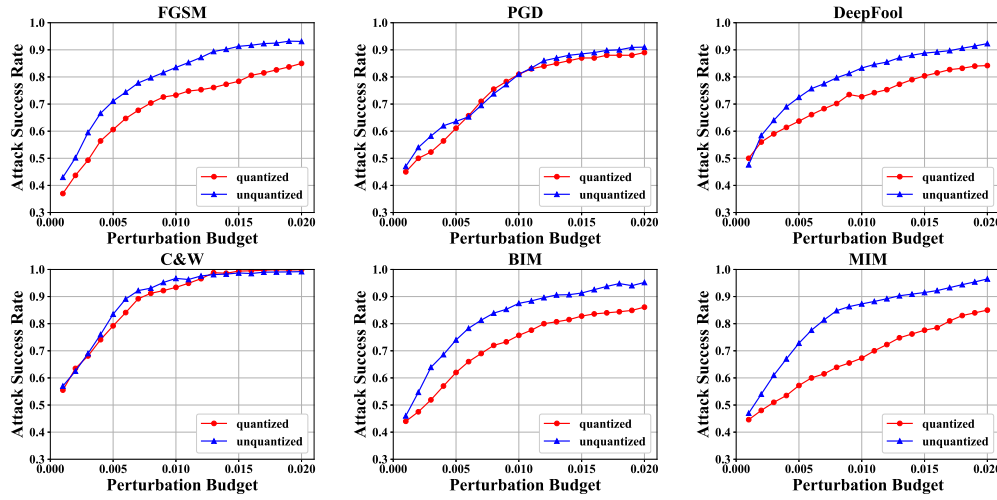


Figure 6: Comparison between quantized and unquantized models with different perturbation budgets against untargeted white-box attacks under the l_{∞} norm.

out that quantized networks have better robustness against adversarial attacks. Bernhard et al. [21] state that quantized models have a quantization shift phenomenon which ruins the adversarial effect. Although [55] draws a different conclusion from us, their work is mainly based on only two models (i.e., VGG-16 and Wide ResNet) with AE attack setting (ϵ ranges from 1/255 to 9/255), and it only takes into account activation quantization. Additionally, based on our findings, real-world quantized models mostly adopt the post-training 8-bit integer quantization method [12] which is parameter-quantized. It is observed that the C&W algorithm performs the best with regard to quantization, causing about 1-2% ASR_s loss. Because the C&W method essentially turns the generation of AEs into an optimization problem, there is little dependence on the gradient information of the original model.

Summary. It is concluded that model quantization can to some extent raise the robustness of a DL model, which results in a lower ASR_s in real-world models.

Black-box adversarial attacks. AdvDroid performs three types of attacks—transfer-based, score-based and decision-based attacks on black-box models. Table 3 shows that 43 models are vulnerable to NES attack, 33 models are vulnerable to boundary attack, and 12 models to transfer attack. Finally, we find that 48.86% (43/88) of successful black-box attacks use NES, which is most effective. The transfer attack of the black-box model has two requirements to train a substitute model, suitable dataset, and model query. We have no limit on the number of queries. In most cases, the internal structure and parameters of the model are not clear.

We find that black-box quantized models need more queries to train a transfer model to reach the same ASR_s on unquantized models. As well known, it is difficult to train a substitute model, because we do not know what model architecture to train with. With more queries, the substitute model may have more abilities to learn the original model’s feature. We choose three different white-box algorithms to attack substitute models, and the results are shown in Figure 7. When the query number reaches 32,500, the model accuracy decreases as the same level as the unquantized

model with 13,333 queries, additional 19,167 queries bring extra time and resource consumption. The upper bound of ASR_s reflects the consistency of the substitute model with the original. With fewer queries, the substitute model is more consistent with unquantized models so the generated AEs exhibit stronger transferability. Over the number of queries, the consistencies of the unquantized and quantized model reach a similar upper bound and thereby the gap decreases.

White-box Case Study. “Nsfw.pb” is found in 19 social and video apps, e.g., an app named HOLLA with 10+ million installs. It is a not-suitable-for-work (NSFW) image classifier with two labels (non-NSFW or NSFW). By using AdvDroid, we change a dog image’s label from the non-NSFW to NSFW using DeepFool with $\epsilon = 0.14$ under the l_{∞} norm. This kind of attack is applicable in many scenarios, like bypassing the detection of received images on victim’s phone. On the contrary, if the app user acts as an attacker, it is more practical to upload the AEs of NSFW images rather than real NSFW images by intentionally disabling NSFW detection in app. It is because NSFW images can be likely blocked by either the server or the receivers’ detectors. Besides, many apps have adopted app integrity check (e.g., SafetyNet [1]) that makes it harder to manipulate one app nowadays [44].

Black-box Case Study. We test a black-box model which is developed with NanoNet [6]. Its usage is to detect the traffic lights and construction zones from the pictures captured by the dash-cam app, a popular app called Nexar [7], with about 1 million downloads. Its task is to identify and classify traffic lights in real-time scenarios. It has four output labels: empty, red, green, and yellow. We generate a training dataset from Internet, and train a substitute model with MobileNet after 50,000 queries. After that, we use targeted white-box method to generate 10 AEs, and find that 8 of them have the same attack effects in the original model. This kind of AEs can bring considerably severe consequences. Supposing there are two cars on the road, the attacker can put an adversarial stop sign or red light sign on the front car. So that the rear car, the victim who is using this dash-cam app, will make wrong driving decisions.

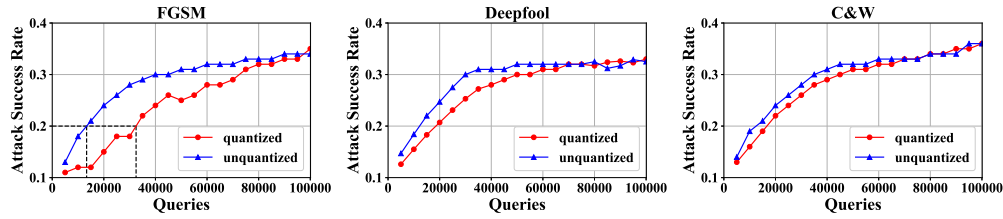


Figure 7: Comparison between quantized and unquantized models with the number of queries against untargeted transfer-based attacks with $\epsilon = 0.06$ (16/255) under the l_∞ norm.

7 SUGGESTIONS FOR DEVELOPERS

On-device models are important intellectual properties to app developers and model providers. On one hand, improper protection of on-device models may attract attackers to launch attacks against legitimate app function, leading to various consequences. On the other hand, the misuse of such on-device models may cause damage to the revenue of the model providers, as attackers can plagiarize the model through infinite queries and building a substitute model. However, it is well recognized that the arms race between attack and defense never ends. It is appealing for defenders to raise the barrier for attackers so that the benefit from the attack cannot offset the attack cost. Here we provide three suggestions against model stealing, misuse and AE attacks.

1. Avoid clear text on-device models. Our analysis tool relies on a lot of useful information provided by the clear text on-device models. Therefore, to avoid being analyzed, the straightforward way is to well protect on-device model files. Obfuscation is one cost-effective approach by obscuring any meaningful text in the stored model files. Encryption can even make the model exist only in memory, and users cannot identify the model by looking at the storage. We found that 70 apps take the defense. In these apps, we can only extract models from 18.57% (13/70) of them. In contrast, for unprotected apps, 97.80% (241/246) of them can be successfully analyzed for model extraction, demonstrating the defense's effectiveness. We further analyzed the failed apps and found that 23 apps use obfuscation to make plaintext unrecognizable. While we cannot directly use string matching to locate the code for model loading, we can still use dynamic analysis to find the code. However, for the rest of the 34 apps using encryption, it is really hard for us to extract the models. So heavy-weight encryption/obfuscation can make the analysis very difficult. A developer can even split the model into two parts and encrypt them [72]. When using the model, users dynamically decrypt the two parts and combine them to form a whole DL model, which can increase the difficulty of model extraction. Obfuscation and encryption are two common techniques for protecting apps. Developers only need to follow standard methods to deploy the two techniques.

2. Prevent the misuse of on-device models. On-device models are valuable assets, and hence the approaches of protecting assets can be applied directly, e.g., authentication. Authentication ensures that only authenticated users/apps are permitted to use the on-device models. This requires the collaboration between app developers and model providers. For app developers, this can be performed by requiring login and user token before the use of their

on-device models. For model providers, secure license distribution from server side and proper license management from client side are necessary before the use of their models. According to our evaluation, 47 apps take advantage of this defense, and they are all Type-C. Recall that the Type-C model uses closed source frameworks. That is to say, even if we successfully extract the models, we cannot directly load them for white-box analysis. So the only choice is to treat the apps as black-box and query the models using various input/output pairs. However, for 35 apps that use the defense, we cannot obtain proper licenses or tokens and cannot execute queries. For other Type-C models without the defense, we can successfully conduct black-box attacks. For example, the AppLock app with about 1 million downloads, uses Sensory's face liveness detection model. This model lacks a license manager to verify user access to the model. An attacker can just copy the model and the library to steal this closed source model and rebuild another face detection app. One challenge of deploying the defense is securing licenses well. Once the license is compromised, malicious users can query the model and perform black-box attacks. Therefore, it is recommended to store licenses on the cloud and update authentication credentials regularly. Besides, recent studies use TEE to protect mobile models from AE attacks by concealing model loading and execution (e.g., OMG [20]).

3. Build more robust on-device models. Last but not the least, it is important for both app developers and model providers to bear in mind the necessity of enhancing the robustness of the on-device model itself. It is shown that the robustness can be achieved using various techniques, such as adversarial training [60, 77] and input transformation [38]. There are also approaches [34, 59] to detect whether the input is an AE. To evaluate the efficacy of these three defenses, we randomly select 20 real-world models and compare the attack success rates (ASR_s) before and after the defenses. Specifically, we employ PGD-AT [60] and TRADES [77] for adversarial training. The ASR_s drops by 37.5% on average, indicating that 37.5% of adversarial examples cease to be effective. As for input transformation, we use JPEG compression [38] and Pixel Deflection (PD) [67], which reduces the ASR_s by 17.0% on average. For AE detection, we take two popular methods—Local Intrinsic Dimensionality (LID) [59] and Kernel Density Estimation (KDE) [34] with the default settings. The average detection ROC-AUCs are 82.1% and 71.5%, respectively. Detailed experiment settings and results are shown in Appendix D.

We also compare the time cost of the three defenses. For adversarial training, the average training time is 2.8 hours. Input

transformation does not require additional time to retrain the models. Its cost is mainly from dynamic execution, which on average takes about 0.03 seconds to process an image. AE detection usually requires to extract features of AEs and models and train a detector for recognizing abnormal input, which takes us 1.2 hours on average. The extra time comes from detectors' inference of the given input, which averagely takes about 0.5 seconds.

The main challenge of deploying the defenses is to minimize the impact on normal inputs. Adversarial training requires updating the model, which may affect the model's accuracy; input transformation requires changing the inputs, which may make the original input unrecognizable; AE detection can also classify normal inputs as adversarial examples. Therefore, developers should deploy defenses carefully so as not to affect the normal requests of users.

8 DISCUSSION

Real-world vs. Academic models. After extracting and evaluating these on-device models, we make a comparison between real-world models and conventional models. Real-world models exhibit significant differences from those in academia based on our study. Specifically, real-world models are prone to employing: ❶ cost-efficient network architectures like MobileNets, EfficientNet, which negatively impact prediction accuracy (see Figure 3). In the RWM dataset, these models' average file size is 4.35 MB. In particular, there are 84 MobileNets, 18 SqueezeNets, 13 EfficientNets in the RWM dataset. ❷ layers obfuscation or custom operators designed for edge devices and hardware accelerators (e.g., TPU, NPU) in Section 6.1. There are 12 kinds of custom operators found in the RWM dataset, e.g., MaxPoolingWithArgmax2D, MaxUnpooling2D, StrSim, and TextEncoder3. ❸ model quantization (40.55% as stated in Section 6.2), model compression and pruning for optimization. Such differences could inspire interesting research questions.

Limitations. During the model extraction in Section 3.1, there may be some false negatives due to the model protection adopted by app developers. For example, for the app that adopts obfuscation techniques, AdvDroid based on semantic search may not be able to find any model-related strings in the app's bytecode or lib export functions. Moreover, the file formats of protected models in some apps are with suffixes like *.bin* or *.data* instead of common model file format like *.tflite*.

Future work. In this work, we only try several mainstream attacks which are experimentally effective. There are more and more powerful attacks being proposed. To keep up with the arm race, we will experiment with more new attack methods in the future, e.g., recently proposed optimized boundary attack [22]. It is an interesting extension to our work to study models with more diverse functions, such as audio recognition and natural language processing, other than image-related functions. Even so, we believe AdvDroid, which facilitates model extraction, interface reasoning and automated testing, can benefit the security assessment of mobile DL models.

9 RELATED WORK

On-device model evaluation. As the on-device inference has been practically adopted on mobile devices, it is of great significance to analyze and understand the potential security threats in these on-device models [73]. Ignatov et al. [45, 46] evaluate different

mobile hardware accelerators for on-device model inference and present the first real-world benchmark performance of different mobile SoCs. Xu et al. [75] give a glance at how DL techniques are deployed in smartphone apps. Their work uses statistical methods to provide insightful results, for example, how many top apps use DL techniques, what these apps use DL for, what is the average size of on-device models, and whether the apps are using any optimization techniques, etc. Based on the revealed results, they provide implications for multiple stakeholders of the mobile DL ecosystem. However, it is worth noting that though plenty of toolboxes, such as cleverhans [63] and ART [62], are developed for practically evaluating DL models using traditional DL framework, few of work has been done to evaluate on-device models that are built upon mobile DL frameworks. *Different from their work, our study is to understand the gap between real-world adversarial attacks and academic attacks on DL models, and show robustness and threats in real-world models.*

Attacks on DL apps. Deep learning has been witnessed to be suffering from many attacks, for example adversarial attacks [23, 24, 37, 61, 64, 65]. Attacks aim to find AEs to force a machine learning system to produce erroneous outputs. This type of attacks can be done in both white-box manner [23, 37, 61, 65] and black-box manner [24, 64]. More specifically, white-box attacks can be categorized into gradient-based methods [37, 65] and optimization-based methods [23, 61]. Due to the lack of sufficient model information, black-box attacks are achieved using scored-based methods to estimate the gradient [24], or using the transferability feature of the adversarial input between an accessible model and the victim black-box model [64]. In addition, there are attacks against specific critical DL apps, such as biometric authentication system [26], liveness detection system [78] and malware detection [66].

10 CONCLUSION AND OUTLOOK

This work is the first measurement work looking at security risks of learning models deployed in mobile apps. We have found that 5,573 (8.90%) of 62,583 apps from the market have been equipped with DL technology to enhance their performance, while 568 (10.19%) of them have local on-device models inside the APK files. Many on-device models are unprotected and vulnerable to adversarial attacks. We proposed a novel method to get model interface of DL models and build model testing environment to generate the AEs. Benefiting from our model analysis, 47.35% of the models can be successfully attacked by current AE generation algorithms. We also found that real-world models with quantization are more robust than academic ones. In the end, we provided insightful suggestions on deploying DL models and defending AE attacks for developers.

ACKNOWLEDGEMENTS

We thank all the anonymous reviewers for their constructive feedback. IIE authors are supported in part by the National Key R&D Program of China (2020AAA0140001), NSFC (U1836211, 61902395), Beijing Natural Science Foundation (No.M22004), the Anhui Department of Science and Technology under Grant 202103a05020009, Youth Innovation Promotion Association CAS, Beijing Academy of Artificial Intelligence (BAAI) and a research grant from Huawei.

REFERENCES

- [1] 2020. Android SafetyNet. <https://developer.android.com/training/safetynet/attestation>.
- [2] 2020. Caffe2. <https://research.fb.com/downloads/caffe2/>.
- [3] 2020. Convert from TFLite. <https://stackoverflow.com/questions/59559289-is-there-any-way-to-convert-a-tensorflow-lite-tflite-file-back-to-a-keras-fil>.
- [4] 2020. Google Assistant. <https://assistant.google.com>.
- [5] 2020. Google Image. <https://images.google.com>.
- [6] 2020. NanoNet. <https://nanonets.com>.
- [7] 2020. Nexar - AI Dash Cam for Peace of Mind on the Road. <https://play.google.com/store/apps/details?id=mobi.nexar.dashcam&hl=en>.
- [8] 2020. Open Images Dataset. g.co/dataset/open-images.
- [9] 2020. Sensory. <https://www.sensory.com>.
- [10] 2020. TensorFlow Hub. <https://tfhub.dev>.
- [11] 2020. TensorFlow Lite example apps. <https://www.tensorflow.org/lite/examples>.
- [12] 2020. TensorFlow Lite model optimization. https://www.tensorflow.org/lite/performance/model_optimization.
- [13] 2021. Convert model(s) to C++ code. https://mace.readthedocs.io/en/latest/user_guide/advanced_usage.html#convert-model-s-to-c-code.
- [14] 2021. Curated NLP Database. <https://metatext.io/datasets>.
- [15] 2021. Google Play Services for AR. <https://play.google.com/store/apps/details?id=com.google.ar.core&hl=en>.
- [16] 2021. Google Translate. <https://play.google.com/store/apps/details?id=com.google.android.apps.translate&hl=en>.
- [17] 2021. Tiny Encryption Algorithm. https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm.
- [18] 2022. PayPal. <https://play.google.com/store/apps/details?id=com.paypal.android.p2pmobile&hl=en&gl=US>.
- [19] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Oteanu, and Patrick McDaniel. 2014. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. *Acm Sigplan Notices* 49, 6 (2014), 259–269.
- [20] Sebastian P Bayerl, Tommaso Frassetto, Patrick Jauernig, Korbinian Riedhammer, Ahmad-Reza Sadeghi, Thomas Schneider, Emmanuel Stapf, and Christian Weinert. 2020. Offline model guard: Secure and private ML on mobile devices. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 460–465.
- [21] Remi Bernhard, Pierre-Alain Moellic, Jean-Max Dutertre, and France Gardanne. 2019. Adversarial Robustness of Quantized Embedded Neural Networks. *Computer & Electronics Security Applications Rendezvous* (2019), 1–33.
- [22] Wieland Brendel, Jonas Rauber, and Matthias Bethge. 2017. Decision-based adversarial attacks: Reliable attacks against black-box machine learning models. *arXiv preprint arXiv:1712.04248* (2017).
- [23] Nicholas Carlini and David Wagner. 2017. Towards evaluating the robustness of neural networks. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 39–57.
- [24] Pin-Yu Chen, Huan Zhang, Yash Sharma, Jinfeng Yi, and Cho-Jui Hsieh. 2017. Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models. In *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*. 15–26.
- [25] Tianshi Chen, Zidong Du, Ninghui Sun, Jia Wang, Chengyong Wu, Yunji Chen, and Olivier Temam. 2014. Diannao: A small-footprint high-throughput accelerator for ubiquitous machine-learning. *ACM SIGARCH Computer Architecture News* 42, 1 (2014), 269–284.
- [26] Yu Chen and H. C. Ma. 2019. Biometric Authentication Under Threat : Liveness Detection Hacking. In *Black Hat USA*.
- [27] Yuxuan Chen, Xuejing Yuan, Jiangshan Zhang, Yue Zhao, Shengzhi Zhang, Kai Chen, and Xiaofeng Wang. 2020. Devil's Whisper: A General Approach for Physical Adversarial Attacks against Commercial Black-box Speech Recognition Devices.. In *USENIX Security Symposium*. 2667–2684.
- [28] Yu-Hsin Chen, Joel Emer, and Vivienne Sze. 2016. Eyeriss: A spatial architecture for energy-efficient dataflow for convolutional neural networks. *ACM SIGARCH Computer Architecture News* 44, 3 (2016), 367–379.
- [29] Jeffrey Dean, David Grove, and Craig Chambers. 1995. Optimization of object-oriented programs using static class hierarchy analysis. In *European Conference on Object-Oriented Programming*. Springer, 77–101.
- [30] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Fei-Fei Li. 2009. ImageNet: A Large-Scale Hierarchical Image Database. In *CVPR09*.
- [31] Yinpeng Dong, Qi-An Fu, Xiao Yang, Tianyu Pang, Hang Su, Zihao Xiao, and Jun Zhu. 2020. Benchmarking Adversarial Robustness on Image Classification. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 321–331.
- [32] Yinpeng Dong, Fangzhou Liao, Tianyu Pang, Hang Su, Jun Zhu, Xiaolin Hu, and Jianguo Li. 2018. Boosting adversarial attacks with momentum. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 9185–9193.
- [33] Goodman Dou, Xin Hao, Yang Wang, Yuesheng Wu, Junfeng Xiong, and Huan Zhang. 2020. Advbox: a toolbox to generate adversarial examples that fool neural networks. *arXiv:2001.05574* [cs.LG].
- [34] Reuben Feinman, Ryan R. Curtin, Saurabh Shintre, and Andrew B. Gardner. 2017. Detecting Adversarial Samples from Artifacts. *ArXiv abs/1703.00410* (2017).
- [35] Angus Galloway, Graham W Taylor, and Medhat Moussa. 2017. Attacking binarized neural networks. *arXiv preprint arXiv:1711.00449* (2017).
- [36] Jort F Gemmeke, Daniel PW Ellis, Dylan Freedman, Aren Jansen, Wade Lawrence, R Channing Moore, Manoj Plakal, and Marvin Ritter. 2017. Audio set: An ontology and human-labeled dataset for audio events. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 776–780.
- [37] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. 2015. Explaining and harnessing adversarial examples. In *ICLR*.
- [38] Chuan Guo, Mayank Rana, Moustapha Cisse, and Laurens van der Maaten. 2018. Countering Adversarial Images using Input Transformations. In *International Conference on Learning Representations*. <https://openreview.net/forum?id=SyJ7CIWCB>.
- [39] Song Han, Xingyu Liu, Huizi Mao, Jing Pu, Ardavan Pedram, Mark A Horowitz, and William J Dally. 2016. EIE: efficient inference engine on compressed deep neural network. *ACM SIGARCH Computer Architecture News* 44, 3 (2016), 243–254.
- [40] Jamie Hayes and George Danezis. 2018. Learning universal adversarial perturbations with generative models. In *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 43–49.
- [41] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 770–778.
- [42] Yingzhe He, Guozhu Meng, Kai Chen, Jinwen He, and Xingbo Hu. 2021. DRMI: A Dataset Reduction Technology based on Mutual Information for Black-box Attacks. In *Proceedings of the 30th USENIX Security Symposium (USENIX)* (Vancouver, B.C., Canada).
- [43] Yingzhe He, Guozhu Meng, Kai Chen, Xingbo Hu, and Jinwen He. 2022. Towards Security Threats of Deep Learning Systems: A Survey. *IEEE Transactions on Software Engineering (TSE)* 48, 5 (2022), 1743–1770. <https://doi.org/10.1109/TSE.2020.3034721>.
- [44] Muhammad Ibrahim, Abdullah Imran, and Antonio Bianchi. 2021. SafetyNOT: on the usage of the SafetyNet attestation API in Android. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 150–162.
- [45] Andrey Ignatov, Radu Timofte, William Chou, Ke Wang, Max Wu, Tim Hartley, and Luc Van Gool. 2018. Ai benchmark: Running deep neural networks on android smartphones. In *Proceedings of the European Conference on Computer Vision (ECCV)*. 0–0.
- [46] Andrey Ignatov, Radu Timofte, Andrei Kulik, Seungsoo Yang, Ke Wang, Felix Baum, Max Wu, Lirong Xu, and Luc Van Gool. 2019. AI Benchmark: All About Deep Learning on Smartphones in 2019. *arXiv preprint arXiv:1910.06663* (2019).
- [47] Andrew Ilyas, Logan Engstrom, Anish Athalye, and Jessy Lin. 2018. Black-box adversarial attacks with limited queries and information. *arXiv preprint arXiv:1804.08598* (2018).
- [48] Andrew Ilyas, Shibani Santurkar, Dimitris Tsipras, Logan Engstrom, Brandon Tran, and Aleksander Madry. 2019. Adversarial examples are not bugs, they are features. In *Advances in Neural Information Processing Systems*. 125–136.
- [49] Benoit Jacob, Skirmantas Kligys, Bo Chen, Menglong Zhu, Matthew Tang, Andrew Howard, Hartwig Adam, and Dmitry Kalenichenko. 2018. Quantization and training of neural networks for efficient integer-arithmetic-only inference. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2704–2713.
- [50] Hengrui Jia, Christopher A. Choquette-Choo, Varun Chandrasekaran, and Nicolas Papernot. 2021. Entangled Watermarks as a Defense against Model Extraction. In *Proceedings of the 30th USENIX Security Symposium (USENIX)* (Vancouver, B.C., Canada).
- [51] Alex Krizhevsky, Geoffrey Hinton, et al. 2009. Learning multiple layers of features from tiny images. (2009).
- [52] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. 2016. Adversarial machine learning at scale. In *ICLR*.
- [53] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. 1998. Gradient-based learning applied to document recognition. *Proc. IEEE* 86, 11 (1998), 2278–2324.
- [54] Yuanchun Li, Ziyue Yang, Yao Guo, and Xiangqun Chen. 2017. DroidBot: A Lightweight UI-Guided Test Input Generator for Android. IEEE Press.
- [55] Ji Lin, Chuang Gan, and Song Han. 2019. Defensive quantization: When efficiency meets robustness. *arXiv preprint arXiv:1904.08444* (2019).
- [56] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C Lawrence Zitnick. 2014. Microsoft coco: Common objects in context. In *European conference on computer vision*. Springer, 740–755.
- [57] Xiang Ling, Shouling Ji, Jiaxu Zou, Jiannan Wang, Chunming Wu, Bo Li, and Ting Wang. 2019. Deepsec: A uniform platform for security analysis of deep learning model. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 673–690.
- [58] Zhuang Liu, Mingjie Sun, Tinghui Zhou, Gao Huang, and Trevor Darrell. 2019. Rethinking the Value of Network Pruning. In *International Conference on Learning Representations*. <https://openreview.net/forum?id=JlInB3C5Ym>.

- [59] Xingjun Ma, Bo Li, Yisen Wang, Sarah M. Erfani, Sudanthi Wijewickrema, Grant Schoenebeck, Michael E. Houle, Dawn Song, and James Bailey. 2018. Characterizing Adversarial Subspaces Using Local Intrinsic Dimensionality. In *International Conference on Learning Representations*. <https://openreview.net/forum?id=B1gj1L2aW>
- [60] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. 2018. Towards Deep Learning Models Resistant to Adversarial Attacks. In *International Conference on Learning Representations*. <https://openreview.net/forum?id=rjzIBfZAb>
- [61] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, and Pascal Frossard. 2016. Deepfool: a simple and accurate method to fool deep neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2574–2582.
- [62] Maria-Irina Nicolae, Mathieu Sinn, Minh Ngoc Tran, Beat Buesser, Ambrish Rawat, Martin Wistuba, Valentina Zantedeschi, Nathalie Baracaldo, Bryant Chen, Heiko Ludwig, Ian Molloy, and Ben Edwards. 2018. Adversarial Robustness Toolbox v1.2.0. *CoRR* 1807.01069 (2018). <https://arxiv.org/pdf/1807.01069>
- [63] Nicolas Papernot, Fartash Faghri, Nicholas Carlini, Ian Goodfellow, Reuben Feinman, Alexey Kurakin, Cihang Xie, Yash Sharma, Tom Brown, Aurko Roy, Alexander Matyasko, Vahid Behzadan, Karen Hambardzumyan, Zhishuai Zhang, Yi-Lin Juang, Zhi Li, Ryan Sheatsley, Abhibhav Garg, Jonathan Uesato, Willi Gierke, Yinpeng Dong, David Berthelot, Paul Hendricks, Jonas Rauber, and Rujun Long. 2018. Technical Report on the CleverHans v2.1.0 Adversarial Examples Library. *arXiv preprint arXiv:1610.00768* (2018).
- [64] Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z Berkay Celik, and Ananthram Swami. 2017. Practical black-box attacks against machine learning. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*. 506–519.
- [65] Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z Berkay Celik, and Ananthram Swami. 2016. The limitations of deep learning in adversarial settings. In *2016 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 372–387.
- [66] Fabio Pierazzi, Feargus Pendlebury, Jacopo Cortellazzi, and Lorenzo Cavallaro. 2020. Intriguing Properties of Adversarial ML Attacks in the Problem Space. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 1308–1325. <https://doi.org/10.1109/SP40000.2020.00073>
- [67] Aaditya Prakash, Nick Moran, Solomon Garber, Antonella DiLillo, and James A. Storer. 2018. Deflecting Adversarial Attacks with Pixel Deflection. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition* (2018), 8571–8580.
- [68] Jonas Rauber, Wieland Brendel, and Matthias Bethge. 2017. Foolbox: A Python toolbox to benchmark the robustness of machine learning models. In *Reliable Machine Learning in the Wild Workshop, 34th International Conference on Machine Learning*. <http://arxiv.org/abs/1707.04131>
- [69] Karen Simonyan and Andrew Zisserman. 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).
- [70] Zhichuang Sun, Ruimin Sun, Changming Liu, Amrita Roy Chowdhury, Somesh Jha, and Long Lu. 2020. Shadownet: A secure and efficient system for on-device model inference. *arXiv preprint arXiv:2011.05905* (2020).
- [71] Zhichuang Sun, Ruimin Sun, Long Lu, and Alan Mislove. 2021. Mind Your Weight(s): A Large-scale Study on Insufficient Machine Learning Model Protection in Mobile Apps. In *30th USENIX Security Symposium (USENIX Security 21)*. 1955–1972.
- [72] Florian Tramèr and Dan Boneh. 2019. Slalom: Fast, Verifiable and Private Execution of Neural Networks in Trusted Hardware. In *ICLR*.
- [73] Dianlei Xu, Tong Li, Yong Li, Xiang Su, Sasu Tarkoma, and Pan Hui. 2020. A Survey on Edge Intelligence. *arXiv preprint arXiv:2003.12172* (2020).
- [74] Han Xu, Yao Ma, Hao-Chen Liu, Debayan Deb, Hui Liu, Ji-Liang Tang, and Anil K. Jain. 2020. Adversarial attacks and defenses in images, graphs and text: A review. *International Journal of Automation and Computing* 17, 2 (2020), 151–178.
- [75] Mengwei Xu, Jiawei Liu, Yuanqiang Liu, Felix Xiaozhu Lin, Yunxin Liu, and Xuanzhe Liu. 2019. A First Look at Deep Learning Apps on Smartphones. In *The World Wide Web Conference (San Francisco, CA, USA) (WWW '19)*. Association for Computing Machinery, New York, NY, USA, 2125–2136. <https://doi.org/10.1145/3308558.3313591>
- [76] Mingming Zha, Guozhu Meng, Chaoyang Lin, Zhe Zhou, and Kai Chen. 2019. RoLMA: A Practical Adversarial Attack Against Deep Learning-Based LPR Systems. In *Information Security and Cryptology (Inscrypt)*. 4701–4708.
- [77] Hongyang Zhang, Yaodong Yu, Jiantao Jiao, Eric P. Xing, Laurent El Ghaoui, and Michael I. Jordan. 2019. Theoretically Principled Trade-off between Robustness and Accuracy. In *International Conference on Machine Learning*.
- [78] Benjamin Zi Hao Zhao, Hassan Jameel Asghar, and Mohamed Ali Kaafar. 2020. On the Resilience of Biometric Authentication Systems against Random Inputs. *arXiv preprint arXiv:2001.04056* (2020).
- [79] Zhong-Qiu Zhao, Peng Zheng, Shou-tao Xu, and Xindong Wu. 2019. Object detection with deep learning: A review. *IEEE transactions on neural networks and learning systems* 30, 11 (2019), 3212–3232.