

# Hermes Attack: Steal DNN Models with Lossless Inference Accuracy

Yuankun Zhu\*

*The University of Texas at Dallas*  
yuankun.zhu@utdallas.edu

Yueqiang Cheng\*

*Baidu Security*  
chengyueqiang@baidu.com

Husheng Zhou

*VMware*  
zhusheng@vmware.com

Yantao Lu

*Syracuse University*  
ylu25@syr.edu

## Abstract

Deep Neural Network (DNN) models become one of the most valuable enterprise assets due to their critical roles in all aspects of applications. With the trend of privatization deployment of DNN models, the data leakage of the DNN models is becoming increasingly severe and widespread. All existing model-extraction attacks can only leak parts of targeted DNN models with low accuracy or high overhead. In this paper, we first identify a new attack surface – unencrypted PCIe traffic, to leak DNN models. Based on this new attack surface, we propose a novel model-extraction attack, namely *Hermes Attack*<sup>1</sup>, which is the first attack to fully steal the *whole* victim DNN model. The stolen DNN models have the same hyper-parameters, parameters, and semantically identical architecture as the original ones. It is challenging due to the closed-source CUDA runtime, driver, and GPU internals, as well as the undocumented data structures and the loss of some critical semantics in the PCIe traffic. Additionally, there are millions of PCIe packets with numerous noises and chaos orders. Our Hermes Attack addresses these issues by massive reverse engineering efforts and reliable semantic reconstruction, as well as skillful packet selection and order correction. We implement a prototype of the Hermes Attack, and evaluate two sequential DNN models (i.e., MINIST and VGG) and one non-sequential DNN model (i.e., ResNet) on three NVIDIA GPU platforms, i.e., NVIDIA GeForce GT 730, NVIDIA GeForce GTX 1080 Ti, and NVIDIA GeForce RTX 2080 Ti. The evaluation results indicate that our scheme can efficiently and completely reconstruct ALL of them by making inferences on any one image. Evaluated with *Cifar10 test dataset* that contains 10,000 images, the experiment results show that the stolen models have the same inference accuracy as the original ones (i.e., lossless inference accuracy).

## 1 Introduction

Nowadays, Deep Neural Networks (DNNs) have been widely applied in numerous applications from various aspects, such as Computer Vision [9, 57], Speech Recognition [20, 22], Natural Language Processing [11], and Autonomous Driving, such as Autoware [28], Baidu Appolo [3], Tesla Autopilot [49], Waymo [52]. These applications indicate the principle role of DNNs in both industry and academic areas. Compared to other machine learning technologies, DNN stands out for its human-competitive accuracy in cognitive computing tasks, and capabilities in prediction tasks [35, 45]. The accuracy of a DNN model is highly dependent on internal architecture, hyperparameters, and parameters, which are typically trained from a TB datasets [16, 56] with high training costs. For instance, renting a v2 Tensor processing unit (TPU) in the cloud is \$4.5 per hour, and one full training process would cost \$400K or higher [17, 42]. Therefore, the importance of protecting DNN models is self-evident.

Over the last few years, privatization deployments [2, 26] are becoming a popular trending for giant AI providers. The AI providers have private high-quality DNN models, and would like to sell them to other companies, organizations and governments with a license fee, e.g., million dollars per year. This privatization-deployment situation further exacerbates the risk of model leakage. There have been many DNN extraction works proposed in the literature [18, 23, 24, 38, 46, 50, 51, 53, 55, 58]. All of them use either a search or prediction method to recover DNN models. For the search based schemes [24, 58], they can only obtain existing models but not customized models. Besides, the performance of their searching processes is particularly low. The prediction based schemes [18, 23, 55] result in a significant drop in inference accuracy. Most importantly, all of these attacks are *not* able to reconstruct the whole DNN model. Thus, until now, most people still have the illusion that the model is safe enough or at least the leakage is limited and acceptable.

In this paper, we first observed that the attacker in the model privatization deployment has physical access to GPU devices,

\*This work was mainly done during the internship at Baidu.

<sup>1</sup>Hermes is the master of thieves and the god of stealth [54].

making the PCIe bus between the host machine and the GPU devices become a new attack surface. Even if the host system and the GPU are well protected individually (e.g., using Intel SGX protect DNN model on the host and never sharing GPU with others), the attacker still has the chance to snoop the unencrypted PCIe traffic to extract DNN models. Based on this critical observation, we propose a novel black-box attack, named Hermes Attack, to entirely steal the whole DNN model, including the architecture, hyper-parameters, and parameters.

It is challenging to fully reconstruct DNN models from PCIe traffic even if we can intercept and log all PCIe packets due to the following three aspects. First, the CUDA runtime, GPU driver, and GPU internals are all closed source, and the critical data structures are undocumented. The limited public information makes the reconstruction extremely difficult. Second, some critical model information, such as the information about layer type, is lost in the PCIe traffic. Without this critical information, we cannot fully reconstruct the whole DNN model. At last, there are millions of PCIe packets with numerous noises and chaos orders. Based on our experiments, only 1% to 2% of all captured PCIe packets are useful for our model extraction work.

To address the above challenges, we design our Hermes Attack into two phases: offline phase and online phase. The main purpose of the offline phase is to gain domain knowledge that is not publicly available. Specifically, we recover the critical data structures, e.g., GPU command headers, using a large number of reverse engineering efforts to address challenge 1. We address challenge 2 based on a key observation: *each layer has its own corresponding unique GPU kernel*. Thus, we identify the mapping relationship between the kernel (binaries) and the layer type in the offline phase with known layer type and selected white-box models. We put all these pair information into a database, which will benefit the runtime reconstruction. In the online phase, we run the victim model and collect the PCIe packets. By leveraging the PCIe specification and the pre-collected knowledge in the database, we correct the packet orders, filter noises, and fully reconstruct the whole DNN model, to address challenge 3.

To demonstrate the practicality and the effectiveness of Hermes Attack, we implement it on three real-world GPU platforms, i.e., NVIDIA Geforce GT 730, NVIDIA Geforce GTX 1080 Ti, and NVIDIA Geforce RTX 2080 Ti. The PCIe snooping device is Teledyne LeCroy Summit T3-16 PCIe Express Protocol Analyzer [33]. We choose two sequential DNN models - MNIST [36] and VGG [47], and one non-sequential model - ResNet [21]. These three pre-trained victim models are used for interference by Keras framework [29] with Tensorflow [1] as the backbone. The attack experiments indicate that Hermes Attack is effective and efficient: (1) randomly given one image, we can completely reconstruct the whole victim model within 5 – 17 minutes; and (2) the reconstructed models have the same hyper-parameters, parameters, and semantically identical architecture as the original ones.

In the inference accuracy experiments, we test each reconstructed model with 10,000 images from public available test datasets [31, 36]. The results show that the reconstructed models have exactly the same accuracy as the original ones (i.e., lossless inference accuracy).

**Contributions.** In summary, we make the following contributions in this paper:

- We are the first to identify the PCIe bus as a new attack surface to steal DNN models in the model-privatization deployments, e.g., smart IoT, autonomous driving and surveillance devices.
- We propose a novel Hermes Attack, which is the first black-box attack to fully reconstruct the *whole* DNN models. *None* of the existing model extraction attacks can achieve this.
- We disclose a large number of reverse engineering details in reconstructing architectures, hyper-parameters, and parameters, benefiting the whole community.
- We have demonstrated the Hermes Attack on three real-world GPU platforms with sequential and non-sequential models. The results indicate that the Hermes Attack can handle MNIST, VGG and ResNet DNN models and the reconstructed models have the same inference accuracy as the original ones.

## 2 Background

### 2.1 DNN Background

Deep Neural network (DNN) is a sub-area of machine learning in artificial intelligence that deals with algorithms inspired from the biological structure and functioning of a brain. DNN is used to model both linear and non-linear relationships between the input  $x$  and the output  $y$ , learning to approximate an unknown function  $f(x) = y$ . A DNN model is represented as a hierarchical organization of connected layers with a certain level of complexity between the input data and resultant output. DNNs are used in two phases, i.e., training and inference. The training process is computationally heavy and needs a large amount of data. With a series of feed-forward matrix computations on given input data, the resultant output is computed through a loss function against ground truth. The weights of the network are updated accordingly based on error back-propagation. The training is done once passing through all of the training samples. The inference is the phase in which a trained model is used to infer real-world data. Terminologies used in the rest of this paper are described as follows.

**Architecture:** Neural network architecture consists of a number of layers, types/dimensions for each layer, and connection topology among layers. The connections between layers can be either sequential or non-sequential. Sequential connection

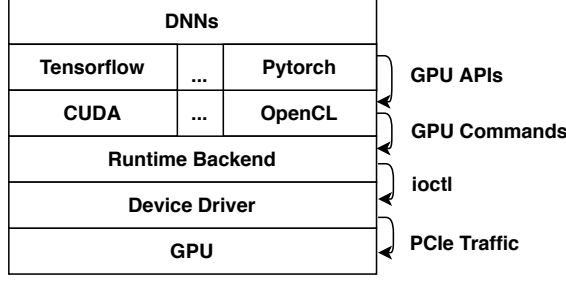


Figure 1: **Typical DNN System Stack.** DNNs are usually implemented with deep learning frameworks, e.g., Tensorflow, Pytorch, and Caffe. These frameworks invoke the GPU runtime frontend like CUDA by calling APIs. The runtime frontend converts these APIs to GPU commands and sends them to the runtime backend, which then sends the received commands to the device driver through *ioctl*. The device driver submits these commands to GPU hardware via PCIe.

means layers are stacked and every layer take the only output of the previous layer as the input. Non-sequential connection denotes the model may include shortcuts, branches, or shared layers [29, 58].

**Hyper-parameters:** Hyper-parameters are the parameters used to control the training process, which do not belong to the trained model and cannot be estimated from training data. There are many hyper-parameters such as learning rate, regularization factors, momentum coefficients, number of epochs, batch size, etc.

**Parameters:** Parameters are configuration variables of the trained model, whose values are derived via training. Model parameters includes weights and bias in DNNs. Throughout the paper, when we mention “parameters”, we mean DNN model parameters instead of “arguments”.

## 2.2 GPU Working Mechanism

Adding sufficient DNN layers to guarantee high inference accuracy may easily explode the computation demand [15]. Currently, major DNN frameworks mainly rely on employing GPUs to satisfy the need, since GPUs enable orders of magnitude acceleration and more energy-efficient execution for many DNN related computations. According to their architecture, modern GPUs can be divided into integrated GPUs that lie on the same die of CPUs and discrete GPUs which are connected to CPU via PCIe. Integrated GPUs are more energy-efficient but less powerful, which is often seen in embedded systems and mobile devices. In this paper, we focus on discrete GPUs since they dominate the markets of AI and machine learning for their computation powers. Some terminologies used in this paper are described as follows.

**CUDA** is a parallel computing architecture provided by NVIDIA for GPUs [37], which includes compilers, user space

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0				
0	Fmt		Type			0	TC		0			TDEP				Attr		0		Length															
Requester ID																Tag						Last BE				First BE									
Address[63:32]																Address[31:2]																0			

Figure 2: **Example of Memory Read Request TLP.** The Tag field can be used to identify the corresponding completion TLP. The address field is the targeted reading address.

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
0			Fmt		Type			0		TC		0			TD/EP			Attr		0			Length									
Completer ID																Status			0			Byte Count										
Requester ID																Tag						Last BE				First BE						
Reserved																																
Payload																														0		

Figure 3: **Example of Completion TLP.** The Tag field can be used to identify the corresponding request TLP. The payload field includes the reading data from the targeted address.

libraries, and kernel space drivers. Employing CUDA for a very simple GPU accelerated program usually involves three procedures: copying input data from main memory to GPU memory, launching computations on GPU, and transferring back the resultant output from GPU memory to main memory.

**Kernel** is a piece of code that is compiled into hardware-specific executable and runs on GPU hardware to do the actual computation. Throughout the paper, when we mention “kernel” we mean “GPU kernel” instead of OS kernel. In CUDA, kernels are compiled by nvcc compiler [12] into CUDA Fatbin and embedded into a dedicated section of host executable file. During runtime, sets of GPU instructions are loaded onto GPU and launched when specific CUDA APIs are called (e.g., `cudaLaunchKernel`).

**Commands** are encoded using distinct instruction sets with kernels, which are used to control data copy, kernel launch, initialization, synchronization, etc. In this paper, we use “GPU command” to indicate a set of GPU hardware instructions that complete an atomic CUDA operation. Each GPU command consists of two parts: the header and the data. The header contains the type of this command and the data size. The data field comprises values passed to this command. We named the data movement command as *D* command and the kernel launch command as *K* command in the rest of the paper.

**GPU Accelerated DNN Platform** is depicted as Figure 1, which includes DNN frameworks, user space libraries, kernel space drivers, and the hardware. High level computation tasks of DNN are finally converted to low level PCIe packets, which is the attack surface we are targeting in this paper.

## 2.3 PCIe Protocol

PCIe is a high-speed motherboard interface for I/O devices, such as graphics cards, SSDs, Wi-Fi, etc. The communication of PCIe takes the form of packets transmitted over these

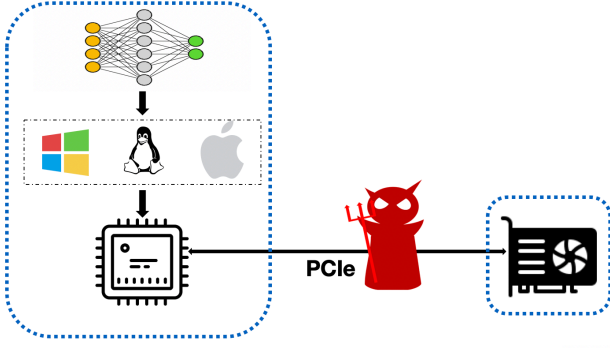


Figure 4: **Threat Model.** We consider the model privatization environment, where the host and the GPU device are well protected individually, and the PCIe bus is the new attack surface. The adversary can snoop the PCIe traffic using a bus snooping device, e.g., a PCIe protocol analyzer.

dedicated lines, with flow control, error detection and re-transmissions. The underlying communications mechanism of PCIe protocol is composed of three layers: Transaction Layer, Data Link Layer, and Physical Layer. Figure 2 and Figure 3 show the formats of memory read request Transaction Layer Packet (TLP) and completion TLP with 64-bit addressing. The header of each TLP is four double words (DWs) long, and the maximum payload size is 128 DWs.

When a CPU writes data into a peripheral, the chipset generates a memory write packet which consists of a 32-bit header and a payload containing the data to be written. The packet is then transmitted to the chipset’s PCIe port. The peripheral can be connected directly to the chipset or connected to a switch network.

When a CPU reads data from a peripheral, there are two packets involved in the read operation. One is read request TLP that is sent from CPU to the peripheral, asking the latter to perform a read operation, as shown in Figure 2. The other one is completion TLP which comes back with data in the payload, as shown in Figure 3. The completion TLP and request TLP can be identified by the same Tag value.

### 3 Attack Design

#### 3.1 Overview

**Threat Model.** In this paper, we consider an AI model privatization deployment environment (e.g., smart IoT, surveillance devices, autonomous driving), where service providers pack their private AI models into heterogeneous CPU-GPU devices and sell them to third-party customers with subscription or perpetual licensing. The end-users are able to physically access the hardware, especially, the PCIe interface. The threat model is depicted as Figure 4, where the GPU is attached to the host

via an unencrypted PCIe connection. We assume the host and the GPU device are well protected individually, e.g., AI models are protected with existing software-hardening techniques on the host side, such as secure boot, full disk encryption, and trusted execution environment (e.g., Intel SGX [14]). It leaves the PCIe bus as a new attack surface for attackers. This assumption is reasonable in the privatization deployment environments because: (1) attackers (e.g., insiders within the third-party company) have the motivation to extract the AI model for saving the per-year license fee, and (2) attackers have physical access to the host machine, and thus they can install a PCIe bus snooping device (e.g., PCIe protocol analyzer) between the host and GPU to monitor and log the PCIe traffic. The victim model is considered a black-box. The victim can be either an existing model or a customized model. It can be implemented with arbitrary deep learning frameworks.

**Challenges.** It is challenging to fully reconstruct DNN models from PCIe traffic even if we can intercept and log all PCIe packets. We summarize the challenges as follows:

1. **Closed-source Code and Undocumented Data Structures.** The CUDA runtime, driver, and NVIDIA GPU hardware are all closed-source, and the critical data structures involved in data transfer and GPU kernel launch are undocumented. The closed-source code and per-architecture instruction set make fully disassembling impractical. Moreover, GPU kernels and commands are encoded with different instruction sets, making reverse engineering more difficult.
2. **Semantic Loss in PCIe Traffic.** Some critical semantic information of a DNN model is lost at the level of PCIe traffic. For instance, DNN layer types can not be obtained directly from PCIe traffic because it is resolved on the CPU side. The loss of critical information makes it challenging to recover the whole model fully.
3. **PCIe Packets with Numerous Noises and Chaotic Orders.** There are millions of packets generated for a single image inference, in which only 1% to 2% are useful for our DNN model reconstruction. The rest “noises” packets should be carefully eliminated. Moreover, numerous completion packets, which indicate operation completion, often arrive out-of-order compared to DNN level semantics, due to the CUDA features that pipeline asynchronous operations. This situation is even worse in the more advanced GPU architectures (e.g., NVIDIA GeForce RTX 2080 Ti) because of introducing new features to unify GPU device and host memory.

**Attack Overview.** The methodology of our attack can be divided into two phases: offline phase and online phase. During the offline phase, we use white-box models to build a database with the identified command headers, the mappings between GPU kernel (binaries) and DNN layer types, and



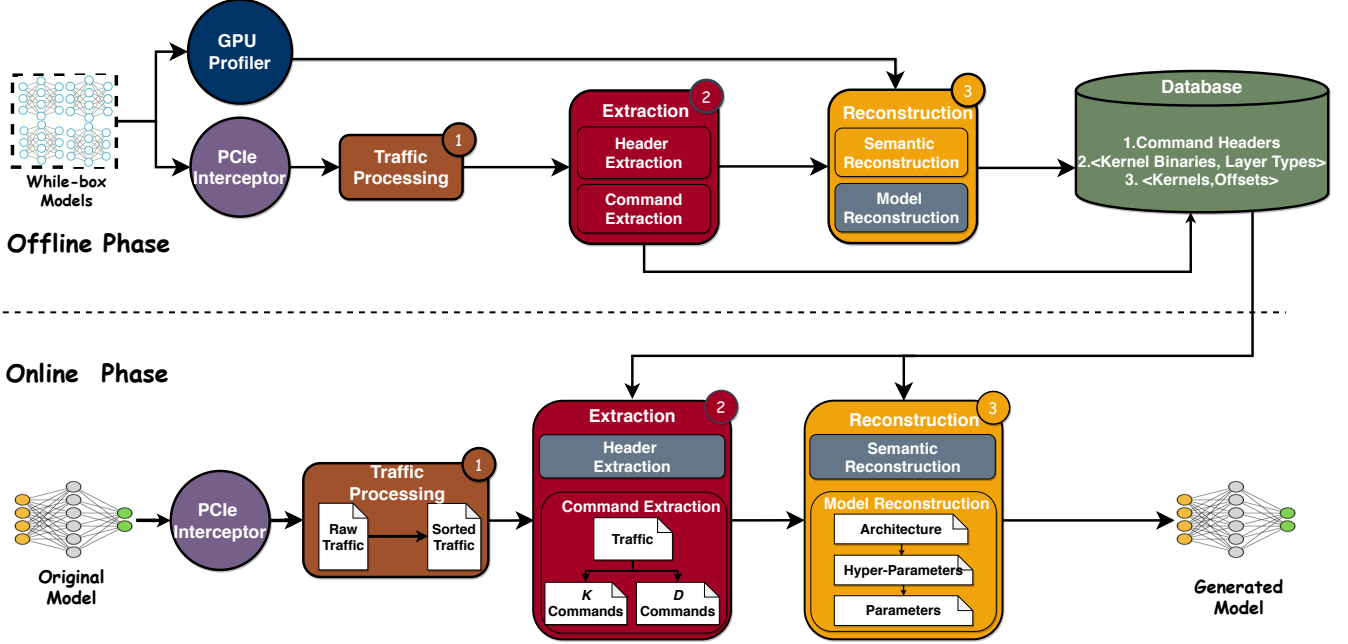


Figure 5: **Attack Overview.** The offline phase builds a knowledge database by identifying GPU command headers of interest, the mappings between GPU kernel (binaries) and DNN layer types, and the mappings between GPU kernels and offsets of hyper-parameters. The online phase is the actual deployed attack to steal the victim model during inference. Three major modules are used in both phases but with different sub-components activated (grey diagrams indicate inactivity): The traffic processing module ① sorts out-of-order PCIe packets; The extraction module ② extracts and filters GPU commands of interest; The reconstruction module ③ fully reconstructs the semantics, architecture, hyper-parameters, and parameters.

the mappings between GPU kernels and offsets of hyper-parameters. Specifically, the traffic processing module (① in Figure 5) sorts the out-of-order PCIe packets intercepted by PCIe snooping device. The extraction module (②) has two sub-modules: header extraction module and command extraction module. The header extraction module extracts command headers from the sorted PCIe packets (Section 3.3.1). The extracted command headers will be stored in the database, accelerating command extraction in the online phase. The command extraction module in the offline phase helps get the kernel binaries (Section 3.3.2). The semantic reconstruction module within the reconstruction module (③) takes the inputs from the command extraction module and the GPU profiler to create the mappings between the kernel (binary) and the layer type, as well as the mappings between the kernel and the offset of hyper-parameters, facilitating the module reconstruction in the online phase (Section 3.4.1).

During the online phase, the original (victim) model is used for inference on a single image. The victim model is a black-box model and thoroughly different from the white-box models used in the offline phase. PCIe traffics are intercepted and sorted by the traffic processing module. The command extraction module (②) extracts  $K$  (kernel launch related) and  $D$  (data movement related) commands as well as the GPU kernel binaries, using the header information profiled from the

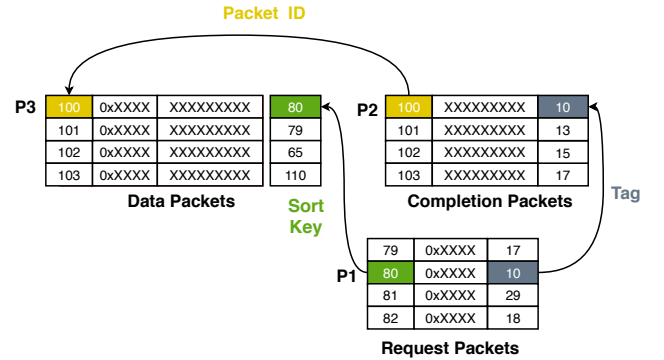


Figure 6: **Process of Sorting PCIe Traffic.** We sort the packets using *packet ID* and *tags*, instead of the capture order.

offline phase (Section 3.3.2). The entire database are feed to the model reconstruction module (③) to fully reconstruct architecture, hyper-parameters, and parameters (Section 3.4.2). All these steps need massive efforts of reverse engineering.

## 3.2 Traffic Processing

The intercepted traffic is composed of TLPs with unique packet IDs. Thanks to the oriented interception, the inter-

cepted traffic is only formed by packets transmitted between CPU and GPU. These packets are arranged increasing ID values in order of arrival. Packets can be classified into upstream packets and downstream packets based on the transmitting direction. The upstream packets represent packets that are sent from GPU to CPU, e.g., GPU read request packets, or completion packets returning GPU computing results. The downstream packets are sent from CPU to GPU, e.g., CPU read request packets, completion packets with input data. The structures of two representative packages are shown as Figure 2 and Figure 3. To make things easier, we only keep the GPU read request packets in the upstream packets and the completion packets in the downstream packets.

In addition to the aforementioned two types of packets, we use another type of packet namely *data packet* that is merged from request packets and completion packets according to the tag field. A data packet comprises both the request address and corresponding acquired data in a single packet. It can be concatenated to a completion packet with the same packet ID and equivalent order.

The major challenge here is that these data completion packets arrived out-of-order. The reason is that the PCIe protocol does not enforce the completion orders of multiple consecutive requests. Additionally, resultant output for a single PCIe read request may be encapsulated in multiple completion packets, making the raw packets hard to analyze directly. To tackle the problem, we coalesce the raw packets by using *merge* and *sort* based on two observations: (1) every request is composed of one request packet and one (multiple) completion packet(s), where the orders of request packets can reflect the correct sequence; (2) completion packets for the same request are guaranteed to arrive in order. We elaborate the merge and sort operations as follows:

**Merge:** For every data packet, we complement the tag field by looking up its corresponding completion packet(s). If adjacent packets have the same tag value, we merge them into a single packet by concatenating their data field.

**Sort:** The sort phase is illustrated as Figure 6. By default, all the packets are arranged according to their packet IDs from low to high. For request packet, we record it as  $P_1$  and lookup all the completion packets that have larger packet IDs than  $P_1$ . We stop the searching when it hits the packet that has the same tag value as  $P_1$  and records this packet as  $P_2$ . Next, we look for the packet that has the same packet ID with  $P_2$  in data packets and records it as  $P_3$ . Then we add the packet ID of  $P_1$  into  $P_3$  as a sort key. We repeat this procedure until every data packet has a sort key. At last, we sort all the data packets by on the sort key.

### 3.3 Extraction

After the preliminary processing, it’s still onerous to reconstruct the model from the traffic. One of the main obstacles is that there are a large number of interference packets. For

Address	Payloads
00000008:292B7F00	...XXXXXXXX 62200220 0B000000 60182EBA 60200220 20000000
00000008:292B7F80	01000000 6C200120 41000000 6D204860 XXXXXXXX XXXXXXXX...


 : Command Header

Figure 7: **Identified Structure of GPU Commands.** A typical GPU command consists of nine DWs. The third DW indicates the location of this command on GPU memory. The fifth DW represents the size of data field. The last DW stands for the type of this command.

instance, making inference on a single image using MNIST model will generate 1,077,756 data packets (after filtering) on NVIDIA Geforce GT 730. However, only around 20,000 of them (2%) are useful for our attack. This may be explained by the fact that CPU sends GPU numerous signals to do initialization, synchronization, etc. So it is necessary to filter out the irrelevant packets. In order to focus on our goal of extracting DNN models, it is sufficient to pick only those *D commands* and *K commands*, representing data movement commands and kernel launch commands, respectively.

#### 3.3.1 Header Extraction

To extract *D commands* and *K commands*, we should identify the header structure of each kind of command. This procedure is done in our offline profiling phase. In order to figure out the header of *D commands*, we repeatedly move crafted data between pre-allocated GPU device memory and main memory, and use pattern match on the intercepted PCIe packets. Similarly, we repeatedly launch multiple kernels with prepared arguments, to identify the header structure of *K commands*.

According to our reverse-engineering results, a *K commands* header structure is shown as the highlighted nine DWs in Figure 7, where the third, fifth, and ninth DW represents GPU memory address, data size in bytes, and command type (e.g., *6D204860* is the signature indicating kernel launch on Kepler architecture), respectively. These three DW fields are most useful for our attack. The other six DWs are GPU-specific signatures whose bit-wise semantics are explained in previous reverse engineering work [19].

We also did exhaustive tests to verify that the header structure is stable and valid on different GPU and machine combinations. The extracted header information are memorized in our profiling database, which can be used to accelerate analysis in the future.

#### 3.3.2 Command Extraction

Raw extracted commands are not ready to use because of tremendous noises. Noise can be classified into two classes: external noise and internal noise. External

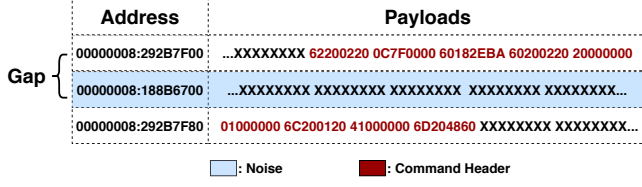


Figure 8: **Example of Command With Noise Packets.** The noise packet is not consecutive with the previous packet in terms of address.

noise refers to those packets not belong to the current command. They can both be the packets of other commands or meaningless packets. External noise could appear frequently because a command with a large data field may require thousands of packets to transmit. Since a command header could be sent via two packets, the noise packet may also appear within the command header. As Figure 8 shown, a command header is split into two parts. They are transmitted via two packets, with a noise packet in between. Internal noise indicates a specific DW inside each packet. We have observed all internal noise and summarized the pattern of it. Thus internal noise can be easily filtered out while extracting the payloads.

An intuitive solution to address the noise issue is to check the address continuity, based on the fact that the transmitted data is usually consecutive in memory space. If a packet’s memory address is not consecutive with its predecessor, it is highly likely that this packet does not belong to the current command. However, this is not always the case especially when the continuous memory space is insufficient. Since the addresses in packets are physical addresses, virtually contiguous address space used by CUDA programs may be split into multiple physical memory chunks. Figure 9 shows an example that the addresses of two adjunct packets belong to the same command are nonconsecutive in physical address. Therefore, it is insufficient to merely check the address continuity. To solve this problem, we introduce a heuristic threshold `MAX_SCAN_DISTANCE`. When a packet encounters an address gap, we scan for the next consecutive packet within `MAX_SCAN_DISTANCE`. If there exists a packet that has a consecutive address with the previous address gap, we consider this packet to be the adjacent packet of the gap and discard the previously scanned packets. Otherwise, we include the gap packet into the payloads. We continue this process until the number of payloads bytes in extracted packets matches the size indicated in the command header.

### 3.4 Reconstruction

#### 3.4.1 Semantic Reconstruction

Semantic reconstruction is a part of the offline profiling phase to build the knowledge database. We use known DNN models as ground truth and utilize NVIDIA’s profiling tools (i.e.,

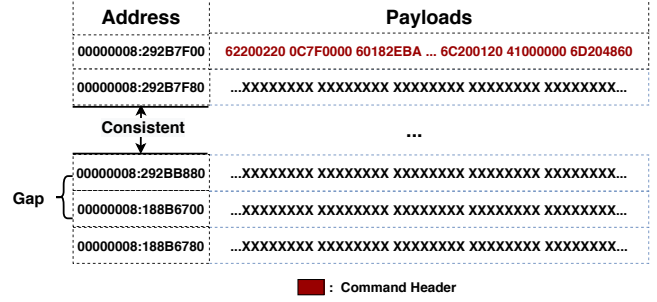


Figure 9: **Example of Command With Large Data Field.** When a command has a large size data field, it occupies more than one continuous memory space. In this case, the address gap also exists.

nvprof [13]) to bridge the semantic gap between PCIe packets and high-level DNN workflow by: (1) associating kernels with DNN layers; (2) profiling the layout of the arguments of certain GPU kernels.

We assume every computational layer (e.g., convolution layer, normalization layer, rectified linear unit layer) of DNN models is computed on the GPU, because layers that are computed by CPU would not send command through PCIe. This assumption is reasonable because the highly multi-threaded architecture of GPU is designed to accelerate matrix computation in DNN layers. Moreover, if some of intermediate layers are ported to CPU, the data movement is expensive. Based on this assumption, it is safe to say each layer is associated with one or more GPU kernels. Different types of layers use different GPU kernels, thus we can infer the layers types by identifying their GPU kernels. Additionally, people prefer to use highly optimized standard libraries provided by GPU hardware vendors (e.g., NVIDIA’s CUDNN library), so the kernel binaries are relatively stable. For example, convolution layers call `convolve_sgemm()` kernels whose binaries are embedded in `nv_fatbin` section of `libcudnn.so`.

We have the following two observations based on our preliminary experiments:

**Observation 1:** Each kernel is loaded onto GPU using a *D* command, and its data field is kernel binaries.

**Observation 2:** Each *K* command includes an address referring to the kernel binary to be launched.

Based on the two observations, we can extract all involved kernel binary by iterating *K* commands. Figure 10 illustrates how we use a *K* command to locate the GPU kernel binary. Particularly, the kernel binary is first loaded onto GPU memory and stored at `405ECF01` using a *D* command, and then launched by a *K* command. Our method works in reverse order: we first retrieve the *K* command’s data field with a fixed offset to locate the address referring to the kernel binary, then we dump the corresponding *D* command’s data field to get the kernel binary.

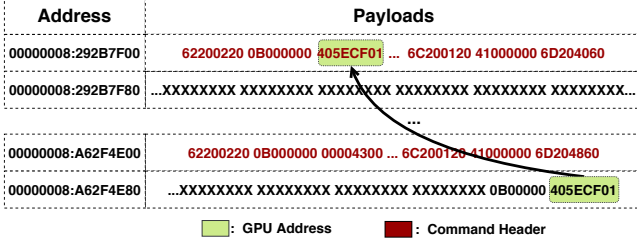


Figure 10: **Process of Locating Kernel Binaries.** The first command in the figure is a *D* command that loads a kernel binary onto GPU. The second command is a *K* command to launch the loaded kernel. These two commands are associated by the same GPU address where the kernel binary is loaded.

After iterating all involved *K* command in PCIe traffic, we have a sequence of kernel binaries in launch order. By aligning with the CUDA trace collected by nvprof, we can figure out the mappings between each kernel binary and its corresponding layer. The mappings are stored in the form of tuples in a hash table, where the key is the kernel binary and the value is layer type.

Another semantic we need to reconstruct is the relationship between kernel binaries and their arguments layout. We only focus on the kernels that involves potential hyper-parameters. Since hyper-parameters are not parts of the trained model, they are only used in certain kernels as arguments. By figuring out the locations of hyper-parameters in *K* commands, we can extract all involved hyper-parameters. We achieve this by profiling known DNNs, looping over the data field of certain kernels' *K* commands to find the expected hyper-parameters. The <Kernels, Offsets of Hyper-parameter> pairs are recovered and stored in the knowledge database.

### 3.4.2 Model Reconstruction

**Extract Model Architecture.** In the online phase, after intercepting all PCIe traffic, we are able to obtain all needed *K* and *D* commands. The key idea of reconstructing DNN architecture is to build data flow graph where each data movement indicates an edge and every kernel launch represents a vertex.

Every kernel takes at least one address as its input and write its output to one or more addresses. By knowing the semantics of this kernel in profiling phase, in the form of *K* command, we are able to figure out which offset(s) indicate input(s) and output(s). We build the data flow graph majorly by treating the input addresses as flow-from and the output addresses as flow-to. All kernels are then associated with these data addresses. We note that in the data flow graph one kernel's output address does not necessarily exactly match its successor's input address. Because these two addresses can be within the same data block or data is copied from one address to the other, which can be determined by iterating *D*

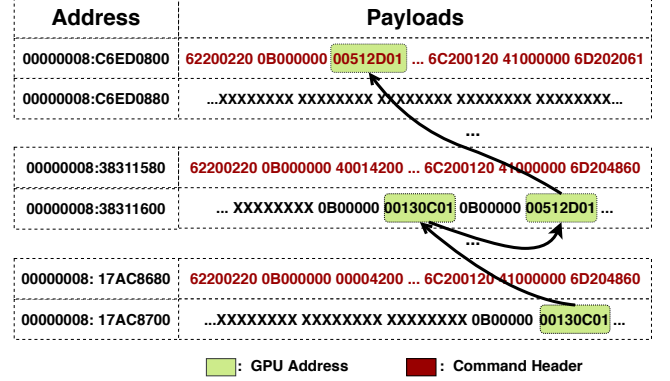


Figure 11: **Process of Locating Parameters.** The first command is a *D* command of loading parameters onto GPU. The second command is a *K<sub>D2D</sub>* command which copies parameters to a new location. The third *K* command launches a kernel taking the address of duplicated data as the input. Our attack recovers the parameters in reverse order as depicted by the arrows.

commands. Once the data flow graph is reconstructed, we can substitute every kernel vertices with their corresponding DNN layers by querying the mappings in the knowledge database.

**Extract Hyper-parameters.** The next step is to extract hyper-parameters that are used during inference, e.g., strides, kernel size. Hyper-parameters that are used to control training phase can not be captured by our inference-time attack, e.g., learning rates, batch size. These hyper-parameters are obtained by two means. One is obtained from kernel arguments (e.g. strides) by retrieving the data fields of certain kernel launch *K* commands, whose offsets are profiled in the semantic reconstruction step. Another kind of hyper-parameters are determined by the existence of relevant kernels. For example, if there is a *BiasNCHWKernel* kernel launch, then the boolean type hyper-parameter `use_bias` is determined to be `true`.

**Extract DNN Parameters.** In this step, we aim to obtain all the parameters of each layer. The parameter here includes both weights and bias. Intuitively, parameters are easier to obtain compared to architecture, because they are statically passed to the layer-specific APIs and propagated to the PCIe traffic in plain value. However, the implementations of different DNNs on different DNN frameworks vary a lot, some of them raise challenges for our attack, including duplicated parameters, asynchronous data movement, and GPU address re-use.

The difficulty is how to locate these parameters since *D* commands are not only used to transmit parameters but also transmit input and a lot of other data. In our preliminary experiments, we observe that a lot of *K* commands do not use any data that are moved onto GPU by *D* commands. Instead, they use new addresses that are generated by certain *K* commands. By aligning with the CUDA trace, we figure out that such *K* commands are actually performing device to device memory



copy. We name these  $K$  commands  $K_{D2D}$ . Our understanding is that, for synchronous data copy on GPU device memory, it is much more efficient using GPU kernel than involving DMA copy which is controlled by  $D$  commands. We verified our thoughts by varying test platforms and using various data size. The duplicated data are the weights of DNN layers, where the original weights on GPU memory are left untouched to avoid being polluted in inference. here comes our third observation:

**Observation 3:** CUDA uses  $K$  commands to synchronously copy data from device to device, which are named  $K_{D2D}$ . DNN parameters are sent to GPU using  $D$  commands and often duplicated by  $K_{D2D}$  commands. The data taken part in the layer computations are the copy instead of the original one.

Figure 11 illustrates how parameters are propagated among commands. The first packet (i.e., a  $D$  command) is the earliest received packet by GPU. The third DW 00512D01 is the GPU memory address referring to the address that stores the weights of this parameter. The second packet is a  $K_{D2D}$  command where two addresses 00130C01 and 00512D01 in its data field. The former address is the destination and the later is the source in device to device memory copy operation. The last packet is a  $K$  command launching a kernel taking the destination address as its argument. We recover the parameters in reverse order: (1) we first use  $K$  commands to locate the destination address; (2) then we use the  $K_{D2D}$  command to find the corresponding source address; (3) finally we retrieve the data field of corresponding  $D$  command to dump the weights of parameters.

We found that for extremely large parameter blocks, they are usually not transmitted using regular  $D$  commands. Instead, they are transferred using a new type of data movement command with different header structures. By aligning with the CUDA trace, we figure out that these commands are doing asynchronous data transfer. We name it  $D_{asyn}$  command. This makes sense because the DNN framework prefers to hide the latency of large data transfer by taking it off the critical path. New challenges are brought by  $D_{asyn}$  command. Firstly, the data size is missed in the  $D_{asyn}$  command header. Secondly, command header and command data are located in separate packets with in-consecutive address.

To resolve the first problem, we calculate the total number of weights using obtained hyper-parameters. There are three types of layers that have weights: convolution layer, dense layer, and normalization layer. The total number of weights and bias of convolution layers can be calculated by the following equations:

$$\# \text{Weights}_{conv} = m_w * m_h * c_{in} * c_{out} \quad (1)$$

$$\# \text{Bias}_{conv} = c_{out} \quad (2)$$

In Equation 1,  $m_w$ ,  $m_h$  are shorted for mask width and mask height, where mask is also known as image processing kernel in convolution layers.  $c_{in}$  and  $c_{out}$  represent the number of input and output, which are indicated by the last arguments

of input and output.  $c_{out}$  is also known as *filters*. For dense layer, the number of weights and bias can be calculated by:

$$\# \text{Weights}_{dense} = c_{out} * c_{in} \quad (3)$$

$$\# \text{Bias}_{dense} = c_{out} \quad (4)$$

In Equation 3 and Equation 4, the  $c_{in}$  and  $c_{out}$  represent the input shape and output shape respectively. The number of *bias* is equal to the number of output. In normalization layer, the number of weights and bias can be directly obtained from kernels' arguments without any calculation.

The second challenge caused by  $D_{asyn}$  makes locating the data field of  $D_{asyn}$  command difficult. In regular  $D$  commands and  $K$  commands, the header and the first piece of data are within the same packet, or located in two packets with consecutive addresses, which is easy to locate data fields. But in  $D_{asyn}$ , its command header and data field can be interleaved by packets from other commands. We resolve this issues by iterating all commands, filtering out all regular commands and noises from the beginning. Then only the  $D_{asyn}$  commands are left. According to the fact that packets within the same command are contiguous in address, now we can easily assemble the header and the corresponding data field of every  $D_{asyn}$  in order.

When a large amount of data is used by the GPU, like VGG and ResNet, address re-use will occur. That is, the data associated with the GPU address can be overwritten, and the subsequent multiple  $K$  commands using the same address can refer to different data. For example, we consider a command sequence ①  $D_1(src) \rightarrow$  ②  $K_{D2D_1}(src, dst_1) \rightarrow$  ③  $D_2(src) \rightarrow$  ④  $K_{D2D_2}(src, dst_2) \rightarrow$  ⑤  $K_1(dst_1) \rightarrow$  ⑥  $K_2(dst_2)$ , where  $D$  indicates  $D$  command,  $K_{D2D}$  indicates data copy on device, and  $K$  represents  $K$  command. In this example, data in  $src$  is copied out by  $K_{D2D_1}$  and then overwritten by  $D_2$ , two  $K$  commands utilize data but referring to the same source address  $src$ . To resolve this problem, we introduce *data life range* to represent the valid period of each data. The life range begins when it is written by a  $D$  command and ends when it is consumed by a  $K_{D2D}$  command. Take the command sequence as the example, the life range of  $dst_1$  is ① - ②, and the life range of  $dst_2$  is ③ - ④. Our strategy is to track back from every  $K$  command to extract its corresponding parameters within its life range. So in the example, we extract  $K_1$ 's parameters in the order of ⑤ ② ①.

## 4 Attack Evaluation

### 4.1 Experiment Setup

**Hardware Platform:** We validate our attack on three GPU platforms, i.e., NVIDIA Geforce GT 730, NVIDIA Geforce GTX 1080 Ti and NVIDIA Geforce RTX 2080 Ti. There is only one GPU attached to the motherboard via PCIe 3.0 in every individual experiment. We adapt CUDA 10.1 as the GPU

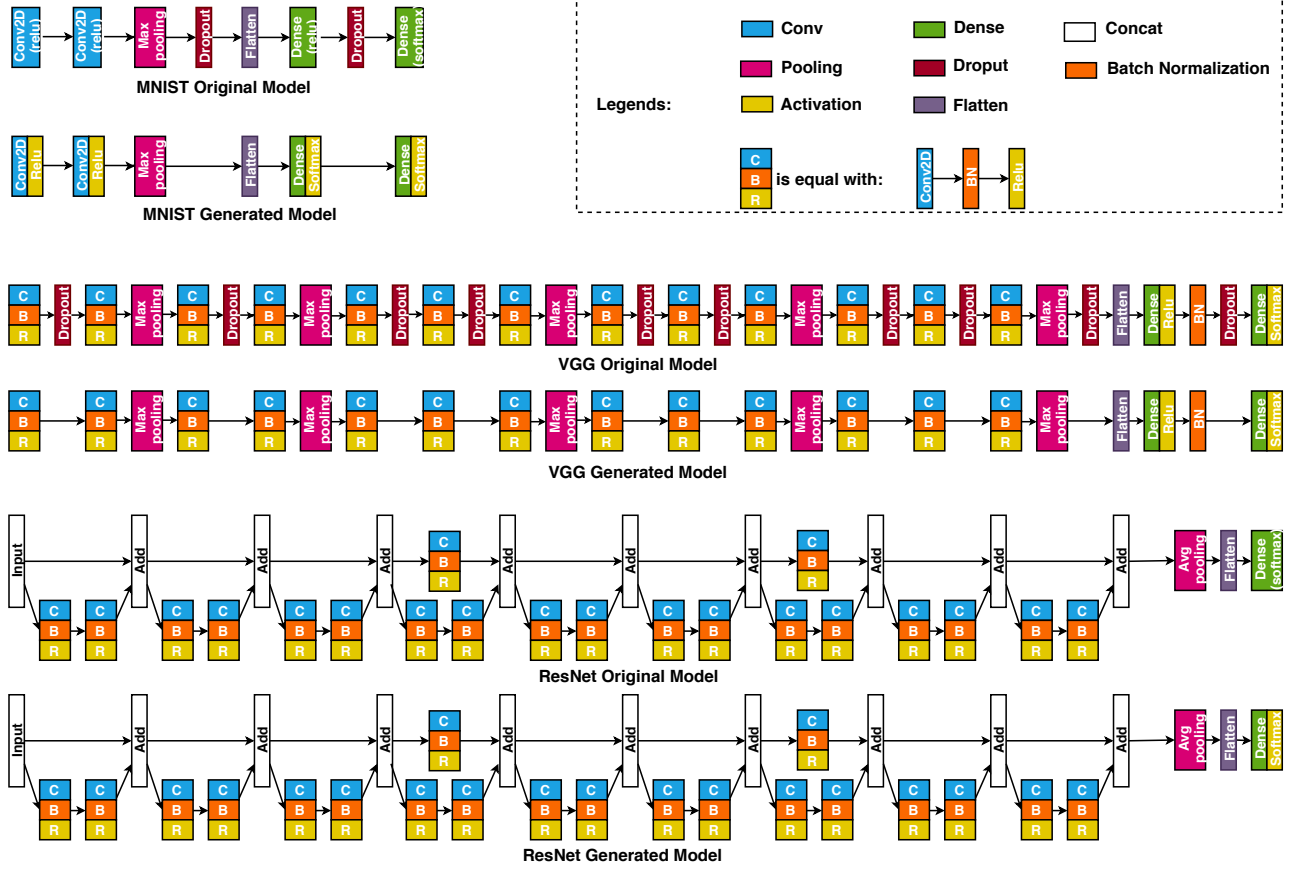


Figure 12: **Architecture Comparison.** This figure shows the architecture differences between original models and the reconstructed models. The CBR block represents the sequentially connected C (Convolution), B (Batch Normalization), R (Relu) layers. There are two major differences between the original models and the corresponding reconstructed models: (1) The reconstructed models do not have dropout layers (as shown in MNIST and VGG); (2) The reconstructed models treat every activation function as a single layer (as shown in MNIST and ResNet).

Table 1: **Victim Models.** This table displays the detail information of all three victim models, including number of layers, number of parameters, training datasets and input shape.

	MNIST	VGG16	ResNet-20
Number of Layers	8	60	72
Number of Parameters	544,522	15,001,418	274,442
Datasets	mnist	cifar10	cifar10
Input Shape	(28,28,1)	(32,32,3)	(32,32,3)

programming interface and Teledyne LeCroy Summit T3-16 PCIe Express Protocol Analyzer as our snooping device.

**Victim Model:** We validate our attack on three pre-trained DNN models: MNIST, VGG16, and ResNet20, which are public available [30].

- **MNIST** model is a sequential model, where layers are stacked and every layer takes the only output of the previous layer as the input. It is trained on the MNIST dataset

and can achieve 98.25% inference accuracy for handwritten digits.

- **VGG16** model is a very deep sequential model with 60 layers in total, 13 of which are convolution layers. It is trained using the cifar10 dataset and can achieve 93.59% inference accuracy for the cifar10 test set.
- **ResNet20** model is a non-sequential model, where some layers have multiple outputs and take multiple inputs from other layers. The victim ResNet model has 20 convolution layers out of 72 layers in total, which achieves 91.45% inference accuracy for the cifar10 test set.

These pre-trained victim models are used for inference by Keras framework with Tensorflow as the backbone. In our experiments, we treat these models as black-boxes without using any layer information during attack. These publicly available models are used only for ground truth purpose. Our attack works for arbitrary proprietary models. The attack results are not influenced by the model accuracy or architecture.

Table 2: **Related Kernels of Each Layer.** This table lists the related kernels of each layer. If there are multiple related kernels of that layer, the primary kernels are highlighted in bold. The last row indicates some kernels not belong to any layer, but are useful and need to be recorded.

Layer	Related Kernels	No.
Conv 2D	<b>ShuffleInTensor3Simple</b>	①
	cudnn::detail::implicit_convolve_sgemm	②
	<b>SwapDimension0And2InTensor3Simple</b>	③
	cudnn::winograd::generateWinogradTilesKernel	④
	cudnn::winograd::winograd3x3Kernel	⑤
BN	cudnn::detail::bn_fw_inf_1C11_kernel_new	⑥
Dense	<b>gemv2N_kernel_val</b>	⑦
	<b>gemvNSP_kernel_val</b>	⑧
Flatten	BlockReduceKernel	⑨
MaxPool	cudnn::detail::pooling_fw_4d_kernel	⑩
AvgPool	Eigen::internal::AvgPoolMeanReducer	⑪
ZeroPad	PadInputCustomKernelNHWC	⑫
Add	Eigen::internal::scalar_sum_op	⑬
Relu	Eigen::internal::scalar_max_op	⑭
Softmax	softmax_op_gpu_cu_compute_70	⑮
Others	SwapDimension1And2InTensor3UsingTiles	⑯
	BiasNCHWKernel	⑰
	BiasNHWCKernel	⑱

The detailed model information including layers, shapes, and parameters are elaborated in Table 1.

## 4.2 Model Architecture Evaluation

In this section, we demonstrate the semantic equivalence between the original model and the reconstructed model. Figure 12 depict the architecture of original models and reconstructed models for MNIST, VGG, and ResNet, where each rectangle represents a DNN layer. As the figure is shown, most of the architectures of the original model and the reconstructed model are the same, except two differences. The first difference is that the reconstructed model does not have the dropout layers, e.g., the MNIST model and the VGG model. The dropout layer is used to prevent over-fitting during the training procedure. It randomly selects some neurons and drops the results. Since it is only used in the training phase and disabled during the inference, this information is not able to be captured in PCIe traffic. Attributes to the quiescence in inference, the dropout layer will not influence the result of the inference. The second difference is caused by the implementation. Some models are implemented using activation function as a hyper-parameter, like the original MNIST model, but some others regard activation function as a single layer, like the Relu function in the original VGG model. This implementation difference will also not lead to any accuracy variance. During our reconstruction, we regard all activation

Table 3: **Offset of Hyper-Parameters.** This table shows all hyper-parameters offsets in their located kernel. The offset is defined as the distance between the first word and the target hyper-parameter in the data field of a *K* command. The weights row and bias row indicate the offset of weights address and bias address respectively.

Hyper-Parameters	Kernel	GT 730	1080 Ti	2080 Ti
<b>Convolution Layer</b>				
Kernel Size	②	(102,103)	(99,100)	(96,97)
Strides	②	(126,127)	(123,124)	(120,121)
Filters	②	101	98	95
Weights	①	83	80	80
Bias	⑰	85	82	82
<b>Batch Normalization Layer</b>				
Weights1	⑥	159	156	156
Weights2	⑥	161	158	158
Weights3	⑥	163	160	160
Weights4	⑥	165	162	162
<b>Maxpooling Layer</b>				
Pool Size	⑩	(152,153)	(149,150)	(146,147)
Strides	⑩	(136,137)	(133,134)	(130,131)
<b>AveragePooling2D Layer</b>				
Pool Size	⑪	(110,111)	(107,108)	(107,108)
Strides	⑪	(114,115)	(111,112)	(111,112)
<b>Zeropadding Layer</b>				
Padding	⑫	(117,118)	(114,115)	(114,115)
<b>Dense Layer</b>				
Units	⑦	101	98	98
Weights	⑦	81	78	78
Bias	⑱	85	82	82

functions as single layers.

Table 2 lists all the related kernels of each layer. Some kernels are primary kernels, and some kernels are used to obtain the offset of hyper-parameters. If a layer has only one related kernel, then this kernel is its primary kernel. If a layer has more than one related kernels, its primary kernels are highlighted in bold. The last row indicates some kernels not belong to any layer, but are still useful and need to be recorded. *SwapDimension1And2InTensor3UsingTiles* is record in order to recover the data flow. *BiasNCHWKernel* and *BiasNHWCKernel* are used to determine the layer use bias or not and also used to obtain the offset of bias address.

## 4.3 Hyper-Parameters Evaluation

The extracted hyper-parameters are the same as those in the original model. Table 3 represents all hyper-parameters offsets in their located kernel. The offset is defined as the distance between the first word and the target hyper-parameter in the data field of a *K* command. Meanwhile, we also record the weights and bias offset, which indicate the offset the weights address and bias address respectively. As Table 3 shown, the offset of these hyper-parameters is not fixed on distinct plat-

Table 4: **Identity Evaluation.** This table shows the identity between the original models and the reconstructed models. All the reconstructed models have the same accuracy with the original ones, as well as similar inference time.

Metrics	Model	Original	Reconstructed		
N/A	N/A	N/A	GT 730	1080 Ti	2080 Ti
Accuracy	MNIST	98.25%	98.25%	98.25%	98.25%
	VGG	93.59%	93.59%	93.59%	93.59%
	ResNet	91.45%	91.45%	91.45%	91.45%
Inference Time(s)	MNIST	2.24	2.39	2.52	2.38
	VGG	65	63	63	61
	ResNet	20	20	20	21

forms. Some layers may also have multiple implementations, and the related kernels may change along with the implementation changes. Here we only list the most frequently used implementation and their offsets.

#### 4.4 Identity Evaluation

Table 4 evaluates the identity between the original models and reconstructed models. We evaluate the identity from two aspects, accuracy and inference time. The accuracy is measured as the average test accuracy on 10,000 test images. The inference time in seconds indicates the total time used to test 10,000 images using this model. For MNIST, the test datasets is obtained from *keras.datasets.mnist.load\_data*. For VGG and ResNet, the test datasets is obtained from *keras.datasets.cifar10.load\_data*. The reconstructed models proved to be as accurate as of the victims on all platforms. The original MNIST model trained on the MNIST dataset achieve 98.25% accuracy. The original VGG model and ResNet trained on cifar10 dataset achieve 93.59% and 91.45% respectively, and all reconstructed VGG models are ResNet models have the same accuracy with the original models. As Table 4 shown, each reconstructed model has a similar inference time with the original one, within a reasonable variance.

#### 4.5 Reconstruction Efficiency

Table 5 records the runtime statistics and the model-generation time. The runtime statistics include the number of total completion packets and the number of both *D* commands and *K* commands. These statistics are obtained from the inference procedure on a single image. Only one image is enough to reconstruct the whole model. As the table shows, the number of *D* commands does not have many relationships with the running models, since only a few *D* commands are used to transfer the information of victim models. However, more complicate the victim model is, more *K* commands will be involved. The generation time in minutes represents the total time used to reconstruct a model from the PCIe data,

including Traffic Processing, Command Extraction, and Reconstruction. The generation time mainly relies on the number of completion packets. The number of completion packets is dependent on both platform and the victim model.

## 5 Discussions

The Hermes Attack aims to leak the victim model through PCIe traffic with lossless inference accuracy. It means that the extracted model will have the same accuracy as the victim one, regardless of the victim model’s accuracy. Meanwhile, the number of the activation functions and the model layers will not affect our attack’s accuracy.

### 5.1 Super Large DNN Models

The methodology of our attack is supposed to be effective for all models. However, the buffer size of the snooping device could be a potential limitation. We currently use the Teledyne LeCroy Summit T3-26 PCIe protocol analyzer as our snooping device, which is equipped with an 8GB memory buffer (4GB for each direction). Due to the buffer size limitation, we cannot intercept all the traffic if the size of a victim model is super large, i.e., VGG16 trained from ImageNet [16]. Although the size of this model is about 500MB, the generated downstream traffic will slightly exceed the buffer limitation due to the large amount of metadata generated by PCIe and GPU. This problem could be solved by updating the snooping device. As far as we know, some other powerful snooping devices like Teledyne LeCroy’s Summit T34 PCI Express protocol analyzer [34] can expand the memory buffer into 64GB. These devices would be able to intercept all the inference traffic of existing DNN models. Alternatively, we can address this issue with an advanced algorithm. Specifically, although the intercepted model is not complete (e.g., only covering the first  $n$  layers), we can still run our existing algorithm mentioned in this above to recover the first  $n$  layers of the model. In the next time, we try to intercept the AI model by skipping  $k$  layers ( $k \leq n$ ), and run the algorithm again. By repeating this step until we can recover the last layer, we then get the whole model by merging all existing recovered layers. This solution does not rely on any advanced hardware device, but it requires accurate model interception, and how to directly recover layers without the data of the skipped layers.

### 5.2 Attack Generalization

We have demonstrated that our attack can be applied to different GPU platforms. For different platforms (e.g., a smartphone with Neural Processing Unit (NPU)), there are several changes that should be noticed. The first change is the command header that could be different. One possible solution is to use the method we mentioned in Section 3.3.1 to identify the new command header structure. The second change is



Table 5: **Performance Evaluation.** This table displays both runtime statistics and generation time. The runtime statistics include the number of extracted D Commands, K Commands, as well as the number of completion packets. Generation time in minutes refers to the time used to reconstruct the model. The inference time in seconds indicates the time used to test 10,000 images.

	MNIST			VGG			ResNet		
Platform	GT 730	1080 Ti	2080 Ti	GT 730	1080 Ti	2080 Ti	GT 730	1080 Ti	2080 Ti
# of D Commands	25,680	28,590	24,342	27,287	27,677	24,931	28,433	28,518	25,577
# of K Commands	216	139	181	903	628	793	1011	886	988
# of Completion Packets	1,077,756	2,244,115	2,959,613	4,284,946	2,615,895	3,354,411	975,257	2,052,657	2,717,451
Generation Time (min)	5	8	11	17	11	12	6	9	10

Table 6: **Related Work Comparison.** ✓ stands for fully recover, P stands for partial recover, × means cannot recover.

Work	Information Source	Method	Results		
			Architecture	Hyper-Parameters	Parameters
Xing Hu, et al. 2019 [23]	Bus Access Pattern	Predict	P	×	×
Yan, Mengjia, et al. 2018 [58]	Cache	Search	×	✓	×
Weizhe Hua, et al. 2018 [24]	Accelerator	Search, Infer	✓	×	P
Yun Xiang et al. 2019 [55]	Power	Predict	✓	✓	×
Vasht Duddu et al. 2018 [18]	Timing	Search	✓	×	×
Binghui Wang et al. 2019 [51]	Parameters	Infer	×	✓	×
Seong Joon Oh et al. 2018 [38]	Queries	Infer	P	P	×
Roberts, Nicholas et al. 2018 [43]	Noise Input	Predict, Infer	×	×	P
<b>Our Work (Hermes Attack)</b>	<b>PCIe Bus</b>	<b>Infer</b>	✓	✓	✓

the GPU instruction sets. The change of instruction sets will lead to the difference in kernel binaries. Fortunately, we can also use the method in Section 3.4.1 to update the database. Although there would be several changes when the platform changes, the GPU and PCIe underlying working mechanism will stay the same. Therefore, the proposed attack will not be influenced by the alternation of hardware.

Different from the change of GPUs, the change of the DNN framework will lead to the different implementation of each layer as well as the relationship between layer and GPU kernels. However, as long as all layers are executed on GPU, we are able to obtain the relationship between the layer and kernels, it will not affect our proposed attack.

The case that multiple tasks simultaneously run on a single GPU should also be aware of. The simultaneously running tasks share the same GPU with the victim model. In this manner, the data sent from the other tasks will make an interference on our extraction. Thanks to the fact that each process owns a GPU context and each context has at least one channel to sent commands, the different tasks can be filtered by the context information.

### 5.3 Mitigation Countermeasures

The first possible defense approach is to encrypt the PCIe traffic. It is easy to add the crypto engine on the CPU side, but it is hard for the commodity GPUs that do not have such

capabilities. Thus, this method is the lack of backward compatibility. Another approach is to use data obfuscation, e.g., obfuscating the commands, model commands, and parameters. However, this method requires kernels to be extended to deobfuscate the data back or understand the obfuscated data. Besides, this method can only increase the bar but cannot prevent the Hermes attack completely.

Besides encryption and obfuscation, another mechanism is adding noise from the software aspect, e.g., sending data in one process but sending interference commands from a different process. However, this could be resolved by utilizing GPU channels, as discussed in Section 5.2. Another alternative solution is to leverage the device driver to use dynamic command headers instead of static command ones, significantly increasing the bar of reverse engineering.

The last possible defense mechanism is to offload some tasks to the CPU. In this way, it can reduce the information obtained from the PCIe traffic. Unfortunately, it will result in significant performance loss due to the frequent data transfer between CPU and GPU and CPU’s low computing power compared to GPU.

## 6 Related Work

**Adversarial Examples:** Adversarial examples are first pointed out by Szegedy et al. [48], which are able to cause the network to misclassify an image. They proposed the L-

BFGS approach to generate adversarial examples by applying a certain imperceptible perturbation, which is found by maximizing the network’s prediction. Afterward, there has been a lot of work concentrating on the adversarial attack, some of them is white-box attack [5, 6, 32, 48], that the attacker has some prior knowledge of the internal architecture or parameters of the victim model, some of the attacks are black-box attack [4, 7, 8, 10, 40, 41, 44].

**Extraction Attack:** Table 4.5 summarized some other DNN model extraction attacks and compared them with our work. [23] proposed an attack by hearing the memory bus and PCIe hints, built a classifier to predict the DNN model architecture, [58] introduced a cache-based side-channel attack to steal DNN architectures, [24] performed a side-channel attack to reveal the network architecture and weights of a CNN model based on memory access patterns and the input/output of the accelerator, [55] revealed the internal network architecture and estimated the parameters by analyzing the power trace. Similarly, [53] presented an attack on an FPGA-based convolutional neural network accelerator and recovered the input image from the collected power traces. [18] proposed an extraction attack by exploiting the side timing channels to infer the depth of the network. [51] designed an attack on stealing the hyper-parameters of a variety of machine learning algorithms, this attack is derived by know parameters and the machine learning algorithms, and training data set. [25] demonstrates an attack that predicts the image classify results by observing the GPU kernel execution time. [43] assumed the model architecture is known, and the softmax layer is accessible, then proved noise input is enough to replicate the parameters of the original model. [46] designed a membership inference attack to determine the training datasets based on prediction outputs of machine learning models. [50] investigated the extraction attack on various cloud-based ML model rely on the outputs returned by the ML prediction APIs. Similarly, some works generated a clone model from the query-prediction pairs of the victim model. [27, 38, 39, 46, 50].

## 7 Conclusion

In this paper, we identified the PCIe bus as a new attack surface to leak DNN models. Based on this new attack surface, we proposed a novel model-extraction attack, named Hermes Attack, which is the first attack to fully steal the whole DNN models. We addressed the main challenges by a large number of reverse engineering and reliable semantic reconstruction, as well as skillful packet selection and order correction. We implemented a prototype of the Hermes Attack, and evaluated it on three real-world NVIDIA GPU platforms. The evaluation results indicate that our scheme could handle customized DNN models and the stolen models had the same inference accuracy as the original ones. We will open-source these reverse engineering results, hoping to benefit the entire community.

## References

- [1] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. Tensorflow: A system for large-scale machine learning. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, pages 265–283, 2016.
- [2] Baidu. Baidu AI Open Platform, 2019. <https://ai.baidu.com/solution/private?hmsr=aibanner&hmdl=private>.
- [3] Baidu. Baidu Apollo Open Platform, 2019. <http://apollo.auto/developer.html>.
- [4] Arjun Nitin Bhagoji, Warren He, Bo Li, and Dawn Song. Exploring the space of black-box attacks on deep neural networks. *arXiv preprint arXiv:1712.09491*, 2017.
- [5] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrđić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. Evasion attacks against machine learning at test time. In *Joint European conference on machine learning and knowledge discovery in databases*, pages 387–402. Springer, 2013.
- [6] Nicholas Carlini and David Wagner. Towards evaluating the robustness of neural networks. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 39–57. IEEE, 2017.
- [7] Pin-Yu Chen, Huan Zhang, Yash Sharma, Jinfeng Yi, and Cho-Jui Hsieh. 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*, pages 15–26, 2017.
- [8] Minhao Cheng, Thong Le, Pin-Yu Chen, Jinfeng Yi, Huan Zhang, and Cho-Jui Hsieh. Query-efficient hard-label black-box attack: An optimization-based approach. *arXiv preprint arXiv:1807.04457*, 2018.
- [9] Dan Cireşan, Ueli Meier, and Jürgen Schmidhuber. Multi-column deep neural networks for image classification. *arXiv preprint arXiv:1202.2745*, 2012.
- [10] Moustapha Cisse, Yossi Adi, Natalia Neverova, and Joseph Keshet. Houdini: Fooling deep structured prediction models. *arXiv preprint arXiv:1707.05373*, 2017.
- [11] Ronan Collobert and Jason Weston. A unified architecture for natural language processing: Deep neural networks with multitask learning. In *Proceedings of the 25th international conference on Machine learning*, pages 160–167. ACM, 2008.

- [12] NVIDIA Corporation. Cuda llvm compiler. <https://developer.nvidia.com/cuda-llvm-compiler>.
- [13] NVIDIA Corporation. Profiler user's guide. [https://docs.nvidia.com/pdf/CUDA\\_Profiler\\_Users\\_Guide.pdf](https://docs.nvidia.com/pdf/CUDA_Profiler_Users_Guide.pdf).
- [14] Victor Costan and Srinivas Devadas. Intel sgx explained.
- [15] Henggang Cui, Hao Zhang, Gregory R Ganger, Phillip B Gibbons, and Eric P Xing. Geeps: Scalable deep learning on distributed gpus with a gpu-specialized parameter server. In *Proceedings of the Eleventh European Conference on Computer Systems*, pages 1–16, 2016.
- [16] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*, pages 248–255. Ieee, 2009.
- [17] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*, 2018.
- [18] Vasisht Duddu, Debasis Samanta, D Vijay Rao, and Valentina E Balas. Stealing neural networks via timing side channels. *arXiv preprint arXiv:1812.11720*, 2018.
- [19] Envytools. Tools for people envious of nvidia's blob driver. <https://github.com/envytools/envytools>.
- [20] Alex Graves, Abdel-rahman Mohamed, and Geoffrey Hinton. Speech recognition with deep recurrent neural networks. In *2013 IEEE international conference on acoustics, speech and signal processing*, pages 6645–6649. IEEE, 2013.
- [21] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.
- [22] Geoffrey Hinton, Li Deng, Dong Yu, George Dahl, Abdel-rahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Brian Kingsbury, et al. Deep neural networks for acoustic modeling in speech recognition. *IEEE Signal processing magazine*, 29, 2012.
- [23] Xing Hu, Ling Liang, Lei Deng, Shuangchen Li, Xinfeng Xie, Yu Ji, Yufei Ding, Chang Liu, Timothy Sherwood, and Yuan Xie. Neural network model extraction attacks in edge devices by hearing architectural hints. *arXiv preprint arXiv:1903.03916*, 2019.
- [24] Weizhe Hua, Zhiru Zhang, and G Edward Suh. Reverse engineering convolutional neural networks through side-channel information leaks. In *2018 55th ACM/ES-DA/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2018.
- [25] Tyler Hunt, Zhipeng Jia, Vance Miller, Ariel Szekely, Yige Hu, Christopher J Rossbach, and Emmett Witchel. Telekine: Secure computing with cloud gpus. In *17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20)*, pages 817–833, 2020.
- [26] JD. JD AI Open Platform, 2019. <http://jddoverseas-neuhub.jd.com/index.html>.
- [27] Sanjay Kariyappa, Atul Prakash, and Moinuddin Qureshi. Maze: Data-free model stealing attack using zeroth-order gradient estimation. *arXiv preprint arXiv:2005.03161*, 2020.
- [28] Shinpei Kato, Eijiro Takeuchi, Yoshio Ishiguro, Yoshiki Ninomiya, Kazuya Takeda, and Tsuyoshi Hamada. An open approach to autonomous vehicles. *IEEE Micro*, 35(6):60–68, 2015.
- [29] Keras. Guide to the Functional API, 2019. <https://keras.io/getting-started/functional-api-guide/>.
- [30] Keras. Keras Applications, 2019. <https://keras.io/api/applications/>.
- [31] Alex Krizhevsky, Vinod Nair, and Geoffrey Hinton. The cifar-10 dataset. *online: http://www.cs.toronto.edu/kriz/cifar.html*, 55, 2014.
- [32] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. Adversarial examples in the physical world. *arXiv preprint arXiv:1607.02533*, 2016.
- [33] Teledyne LeCroy. Protocol Analyzer - PCI Express - Teledyne LeCroy, 2019. <https://teledynelecroy.com/protocolanalyzer/pci-express>.
- [34] Teledyne LeCroy. Summit T34 Analyzer, 2019. <https://teledynelecroy.com/protocolanalyzer/pci-express/summit-t34-analyzer>.
- [35] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. Deep learning. *nature*, 521(7553):436–444, 2015.
- [36] Yann LeCun, Corinna Cortes, and CJ Burges. Mnist handwritten digit database. 2010.
- [37] CUDA Nvidia. Nvidia cuda c programming guide. *Nvidia Corporation*, 120(18):8, 2011.

- [38] Seong Joon Oh, Bernt Schiele, and Mario Fritz. Towards reverse-engineering black-box neural networks. In *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, pages 121–144. Springer, 2019.
- [39] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. Knockoff nets: Stealing functionality of black-box models. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4954–4963, 2019.
- [40] Nicolas Papernot, Patrick McDaniel, and Ian Goodfellow. Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. *arXiv preprint arXiv:1605.07277*, 2016.
- [41] Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z Berkay Celik, and Ananthram Swami. Practical black-box attacks against machine learning. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pages 506–519, 2017.
- [42] Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and Peter J. Liu. Exploring the limits of transfer learning with a unified text-to-text transformer, 2019.
- [43] Nicholas Roberts, Vinay Uday Prabhu, and Matthew McAteer. Model weight theft with just noise inputs: The curious case of the petulant attacker. *arXiv preprint arXiv:1912.08987*, 2019.
- [44] Sayantan Sarkar, Ankan Bansal, Upal Mahbub, and Rama Chellappa. Upset and angri: breaking high performance image classifiers. *arXiv preprint arXiv:1707.01159*, 2017.
- [45] Jürgen Schmidhuber. Deep learning in neural networks: An overview. *Neural networks*, 61:85–117, 2015.
- [46] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 3–18. IEEE, 2017.
- [47] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.
- [48] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013.
- [49] Tesla. Tesla: Future of driving, 2019. <https://www.tesla.com/autopilot>.
- [50] Florian Tramèr, Fan Zhang, Ari Juels, Michael K Reiter, and Thomas Ristenpart. Stealing machine learning models via prediction apis. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 601–618, 2016.
- [51] Binghui Wang and Neil Zhenqiang Gong. Stealing hyperparameters in machine learning. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 36–52. IEEE, 2018.
- [52] Waymo. Waymo: The world’s most experienced driver, 2019. <https://waymo.com/tech/>.
- [53] Lingxiao Wei, Bo Luo, Yu Li, Yannan Liu, and Qiang Xu. I know what you see: Power side-channel attack on convolutional neural network accelerators. In *Proceedings of the 34th Annual Computer Security Applications Conference*, pages 393–406. ACM, 2018.
- [54] Wikipedia. Hermes. <https://en.wikipedia.org/wiki/Hermes>.
- [55] Yun Xiang, Zhuangzhi Chen, Zuohui Chen, Zebin Fang, Haiyang Hao, Jinyin Chen, Yi Liu, Zhefu Wu, Qi Xuan, and Xiaoniu Yang. Open dnn box by power side-channel attack, 2019.
- [56] Jianxiong Xiao, James Hays, Krista A Ehinger, Aude Oliva, and Antonio Torralba. Sun database: Large-scale scene recognition from abbey to zoo. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pages 3485–3492. IEEE, 2010.
- [57] Junyuan Xie, Linli Xu, and Enhong Chen. Image denoising and inpainting with deep neural networks. In *Advances in neural information processing systems*, pages 341–349, 2012.
- [58] Mengjia Yan, Christopher W Fletcher, and Josep Torrellas. Cache telepathy: Leveraging shared resource attacks to learn {DNN} architectures. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 2003–2020, 2020.