## Adversarial Machine Learning

Adversarial machine learning is a research field that lies at the intersection of machine learning and computer security. It aims to enable the safe adoption of machine learning techniques in adversarial settings like spam filtering, malware detection etc [ **cite** [**https://en.wikipedia.org/wiki/Adversarial\_machine\_learning**](https://en.wikipedia.org/wiki/Adversarial_machine_learning) ]. If the ML models are deployed online for model-as-a-service, attackers can easily launch model evasion attacks or trying to steal the model in cloud for profit. The goal of an adversary aiming model evasion attacks is to confusethe model into providing a false negative classification. Our study addresses the case when an attacker attempts to evade detection by modifying the submitted PDF files so that its malicious functionality remains intact but the probabilistic score return by model is decreased. In short, we focus on evasion attacks here but leave model stealing attacks as future work.

From an adversarial viewpoint, the more information about a learning-based system is available, the higher the chances become that the system can be successfully gamed. Such kind of attacks has been studied thoroughly assuming attackers have full knowledge about the deployed classifier. In practice, this assumption is rarely held, especially for the online system. The knowledge about the deployed classifier can be obtained from all kinds of sources. Still, it remains largely unclear what an attacker may learn about a learning-based method deployed “in the wild” and how this information can be exploited. We use a real, deployed Model 2 as a testing case, to verify the effectiveness of evasion attacks and later propose some effective model defense strategies.

We have built a framework for practical evasion strategies, and adapt several evasion algorithms for practical application scenarios. Our experiment results reveal that the detection accuracy of model 2 declines sharply even if it is exposed to the simplest attacks. The experiment results show that three potential techniques can strengthen the robustness of model against adversarial data manipulation. The rest of this session touches the following subtopics:

* Adversarial Examples Generation
* Case Study: Adversarial Example Generation
* Model Robustness & Effective Defense Strategies
* Performance Evaluation

### Adversarial Examples Generation

In this session, we are going to discuss adversarial ML in particular scenarios. To be specific, it is supposed that an attacker has obtained some information of a targeted model, such as the features extracted, the algorithm applied and the training set etc. It is generally believed that as attackers know more about the model, the adversarial examples generated can perform stronger model evasion attacks. In this session, we refer to the technique proposed by Nedim Smdic [4] in order to conduct evasion attack against the learning-based model. The general idea of our evasion technique is based on insertion of dummy content into PDF files which is ignored by PDF renderers but affected the computation of features used in Model 2. Once we can influence a subset of model’s features, we develop attack algorithms for adversarial examples generation.

To systematically explore the attacker’s options, we define an orthogonal set of evasion strategies reflecting various degrees of available knowledge. The letters F, T or C, corresponds to the classifier components feature set, training dataset and classifier alg, respectively and is present in the name of a scenario. We describe both high-level algorithms and low-level implementations for staging evasion attacks in following 4 attack scenarios:

1. Attack Scenario F

In scenario F, only the feature set is available to the adversary, to a varying extent. The adversary might be aware of some or all features, mistakenly consider obsolete features as being used, be capable of reading a subset or all features or be able to modify some or all features to a varying degree. Manipulation of a sufficient subset of features is, however, required in order to be able to modify samples and proceed with evasion.

1. Attack Scenario FT

This scenario enables the adversary to take advantage of the knowledge the target classifier’s training dataset, in addition to the known features. The dataset may be fully or partially leaked, enabling more accurate decisions in the process of generating a successful attack sample. Knowledge of training data enables the attacker to perform the entire attack offline before submitting the final result.

1. Attack Scenario FC

In Scenario FC, the adversary knows the feature set and some details about the classifier, such as its type, parameters or the specific implementation. An adversary with no information about the training dataset at all and without a surrogate dataset has little advantage of knowing the classifier. With a surrogate dataset they can train a surrogate classifier of the right type, yet the accuracy of this approximation depends on the quality of the gathered data. This attack can also be performed offline, similar to other attacks based on surrogate classifiers.

1. Attack Scenario FTC

The adversary has the best chance of evading the target classifier if he knows the details of all three classifier components. In that case, he can fully reproduce the online classifier in an offline setting, submitting the attack results only when a sufficiently good evading sample has been found. An offline mimicry attack or an offline classifier-specific attack that defeat the offline classifier have a strong probability of defeating the online one as well.

One of the most important components in our framework are attack algorithms. The main goal is to generate PDF files whose feature vectors are likely to receive low classification scores.

We randomly select 2,000 highly scored malicious samples as the original seeds to generate adversarial examples. After the generation process is done, we then use these examples to be against Model 2. The experiments presented in this section assess the effectiveness of evasion techniques presented so far. In our evaluation protocol, we take on the role of an attacker and combine all available means to defeat an up-to-date version of Model 2. As shown in Table 4, this attack causes a great damage to model 2. In the scenario of FC, the detection accuracy of model 2 is only 2.92%, meaning more than 97% of malicious documents are able to evade classifier after variation.

Although robust against data noise, Model 2 is not was not designed for resilience against adversarial noise. That’s why we construct Model 3. Model 3 is constructed by modifying feature and training set, with an increased training data of 200,000 samples. This model contains around **100** independent trained decision trees and ??? randomly selected features selected for each tree. This updated training set includes some new variants, such as some variants generated by Mimicry Attack and Reverse Mimicry Attack methodology. As shown in Table 4, when model 3 is attacked by the tactics used in the above four scenarios, its detection accuracy is higher than Model 2 in a large margin, demonstrating the robustness of our re-trained model.

From the operational perspective, it is crucial to understand which features contribute most to the success of the reported attacks. In general, interpretation of models created by learning techniques is always difficult. Random Forest classifiers provide a ranking of features according to their informativeness, which has been crucial for the design of the attack.

Table 4: Different Attack Scenarios and Model Accuracy (TODO: Fix this)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attack Scenarios | # of original seeds | # of Adversarial Examples |  | Local ML Model (inside mimicus) | Model 2 (rf) Accuracy | Defense Technique 1 | DT 2 | DT 3 | Model 3 Accuracy |
| F | 2000 | 2157 |  | SVM | 71.18% | 96.71% |  |  |  |
| FC | 2000 | 240 |  | RF | 2.92% | 12.50% |  |  |  |
| FT | 2000 | 4196 |  | SVM | 84.25% | 96.76% |  |  |  |
| FTC | 2000 | 600 |  | RF | 15.83% | 18.71% |  |  |  |

还需新增一列，在各种攻击环境下所使用的 对抗样本生成算法，参看原论文，Table1。

* 观点：不要让攻击者知道模型的算法以及具体参数，建议算法最好不要公开，增加算法的差异度。

### Case Study: Adversarial Example Generation

A practical way to interpret attacks is to observe concrete changes in feature values produced by the attacks. Although it does not scale to cases with many features and files, this kind of investigation provides deep insight into the example at hand.

This session presents a concrete example for adversarial example generation. We select a file with CVE ID ‘CVE-2013-0641’ as an example. This file has the vulnerability that hackers can execute any code remotely. We apply the methodologies in the above four scenarios to vary selected samples and then check against the VirusTotal anti-virus service. The original sample is scanned by around 60 detection engines, within which 33 engines predict the sample as malicious. While only around 22 engines are able to predict the sample variants as malicious, this demonstrates strong model evasion ability of adversarial examples.

Table 5 Detection Accuracy for VirusTotal anti-virus service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File Hash | Origin | F | FC | FT | FTC |
| 00ba5c43b1cec186c634c24ac21982d3 | 33/60 | 22/60 | 23/60 | 22/60 | 22/60 |

Since most PDF detection engines are based on structure and content, once we modify the structure and content, such as adding some objects from benign samples or modifying the file size, the malicious file will have a higher chance to evade the classifiers. We compare the feature space of the file before and after variation. As shown in Table 6, this “benignization” is evident in the provided example. By comparing the BEFORE and AFTER columns, we see that the variation for this file includes adding an author (author\* features), set the creation (createdate\_ts) and modification (moddate\_ts) data into recent past etc. All changes towards the benign class. After variation, the sample remains the malicious behavior while 10 more models have been successfully evaded.

The mimicry attack is well-known in the security literature. Its idea is to transform a malicious sample in such a way that it mimics a chosen benign sample as much as possible, making the resulting mimicry sample harder to detect. This attack alg. is simple to implement, can be applied to any classification algorithm, and does not necessarily depend on a particular learned classifier model. Therefore, it is suitable for evaluation in every evasion scenario. The results for the whole dataset reveal that even with the smallest amount of available information, i.e., an ability to freely modify two thirds of the feature values in feature space, our attacks reduce the accuracy of the model from 99% to the most 2.92% (the FC Scenario).

Table 6 Changes of feature values for a subset of features in an attack. The BEFORE column shows the feature values extracted from a malicious candidate file, the adversarial example generation alg. transformed these values in feature space into a new data point (AFTER).

|  |  |  |
| --- | --- | --- |
| Feature | Before | After |
| author\_lc | 0 | 6 |
| author\_len | 0 | 14 |
| author\_uc | 0 | 6 |
| count\_javascript | 1 | 6 |
| createdate\_ts | -1 | 650616173 |
| createdate\_tz | -1 | 10020 |
| moddate\_ts | -1 | 482083775 |
| keywords\_lc | 0 | 4 |
| keywords\_len | 0 | 7 |
| producer\_lc | 0 | 8 |
| producer\_len | 0 | 19 |
| version | 4 | 7 |

### Model Robustness & Effective Defense Strategies

In our last experiment, we have investigated the robustness of defensive mechanisms to our evasion technique. We propose to use **3** kinds of techniques to increase the robustness of ML model. The first one is simple and straightforward: Increase the number, the diversity and the timeliness of the training dataset; The second one is also simple: Adjust the feature set and delete the features been exposed; The third one is to apply adversarial training.

If the feature sets have been exploited by attackers, we can modify the weight of features or delete the related features and retrain the ML models. As shown in Figure 2, the top 30 features are sorted by importance for Model 3 in ascending order. It is not surprising features such as count\_font, count\_javascript, size, count\_obj and count\_endobj account for most of the weights. In a white box setting of the adversary environment, we assume the adversary knows the 5 most important features. As a proactive defense strategy, we suggest removing those exploited features and retrain the model immediately.

Figure 2 Top 30 features of Model 3



Table 7 shows the detection accuracy of the retrained Model 3 after removing 5 features from above. As shown, when the classifier is trained using all features above, the accuracy rate of model is around 99.82%. If we delete up to top five features, the accuracy is almost stable. That concludes our model can confront grey box attacks even using the rest of not so important features for training. The top 5 related features here are (note: with the format to be (index numer, feature name)): (1, count\_font), (2, count\_javascript), (3, size), (4, count\_obj) and (5, count\_endobj)

Table 7 Accuracy of Model after deleting top 5 related features

|  |  |
| --- | --- |
| Features Deleted | Accuracy |
| [] | 99.82% |
| [1] | 99.52% |
| [1,2] | 99.52% |
| [1,2,3] | 99.64% |
| [1,2,3,4] | 99.64% |
| [1,2,3,4,5] | 99.64% |

More, we assess the model robustness by the effectiveness of features. First, we sequence the features by their importance, and then delete the most important features one by one to create new feature sets which are used for model retraining. As shown in Figure 3, the curve represents the accuracy of model when features are deleted one by one. When the features are decreased to 100, the accuracy of the retrained model still maintains at around 90%. This demonstrates:

* Despite the high weights of individual features, if they are deleted, the accuracy of model only declines a small margin;
* The interaction of ‘Medium Weight’ features can make the model robust, and reduce the effect caused by the deletion of individual important features significantly;
* “Medium Weight” features can help to effectively prevent the Model Evasion attacks;

Figure 3 Detection Accuracy as features are deleted



### Performance Evaluation

In order to assess the prediction performance of model, we randomly divide dataset into two classes with 90% training and 10% testing, and 10-fold cross validation has been applied. As shown in Figure 4, the area below the ROC curve is around 1, which indicates good prediction performance of Model 3.

Figure 4 ROC Curve



In this section, we have presented the empirical security evaluation of a deployed learning-based system. Our study assumed that an attacker has no specific insider information about the system. It demonstrated, however, that enough in- formation can be gathered from various sources and extended with approximations and automatic inference algorithms in order to stage a successful evasion attack. In our experiments carried out on an established system for detection of PDF malware, Model 2, the significant drop in detection rates has been observed.

The findings of our study suggest that careful attention should be paid to the design of features and algorithms used in data-driven security techniques. The main message of our experiments is that an attacker can significantly decrease the accuracy of a learning-based system if he has sufficient knowledge of its features and techniques. The main factor that contributes to this insecurity is the knowledge of features. Such an impact suggests that even a small amount of knowledge about the features can be exploited for staging evasion attacks.