

TokenBreak: Bypassing Text Classification Models Through Token Manipulation

Kasimir Schulz Kenneth Yeung Kieran Evans
 kschulz@hiddenlayer.com kyeung@hiddenlayer.com kevens@hiddenlayer.com

Abstract

Natural Language Processing (NLP) models are used for text-related tasks such as classification and generation. To complete these tasks, input data is first tokenized from human-readable text into a format the model can understand, enabling it to make inferences and understand context. Text classification models can be implemented to guard against threats such as prompt injection attacks against Large Language Models (LLMs), toxic input and cybersecurity risks such as spam emails. In this paper, we introduce TokenBreak: a novel attack that can bypass these protection models by taking advantage of the tokenization strategy they use. This attack technique manipulates input text in such a way that certain models give an incorrect classification. Importantly, the end target (LLM or email recipient) can still understand and respond to the manipulated text and therefore be vulnerable to the very attack the protection model was put in place to prevent. The tokenizer is tied to model architecture, meaning it is possible to predict whether or not a model is vulnerable to attack based on family. We also present a defensive strategy as an added layer of protection that can be implemented without having to retrain the defensive model.

1 Introduction

Splitting input text into tokens has been pivotal in the development of Natural Language Processing (NLP) machine learning models. The process of tokenization is instrumental in these models' capability to interpret text semantics, making them highly efficient in tasks such as text classification and generation. Over time, tokenizers have evolved, with different tokenization strategies being employed for different use cases and models. However, some tokenization strategies are vulnerable to manipulation, allowing attackers to tokenize strings in ways that can invalidate a classifier's verdict. This becomes particularly critical when these classifiers are essential components in systems like spam detection, toxicity monitoring, and external LLM guardrails, where misclassifications could lead to much greater harms. This paper introduces TokenBreak, a novel attack on tokenizers that deliberately manipulates how an input attack string is tokenized, causing it to appear harmless or benign to classifiers while preserving

semantic intent. This enables TokenBreak to not only bypass classification but also remain fully effective against targets that handle the text later on, such as an LLM or an email recipient. We found that minor adjustments to input text, such as the addition of a single targeted letter to a word, can induce false negatives in the classification model without compromising the target’s ability to comprehend it.

Our contributions are as follows:

1. We propose an adversarial example generation method that prepends single characters to words in order to manipulate the output of a text classification model.
2. We demonstrate that this attack can be mitigated using different tokenization strategies.
3. We demonstrate why, despite this attack being focused on the tokenization strategy, we consider this a model-level vulnerability, because of tokenizer to model mapping, meaning this attack can also be mitigated by choice of classification model.

2 Related Work

Recent research has explored vulnerabilities in LLMs, particularly focusing on bypassing the alignment of LLMs using various techniques. One technique from Rao et al.[1] employs transliterations (Orthographic Jailbreak Technique or ORTH) to obfuscate jailbreak queries, which causes a retokenization of the string but preserves the semantic intent, allowing it to bypass basic alignment fine-tuning, enabling the target LLM to output an undesired response. ORTH no longer works on most modern LLMs due to improvements in the alignment process.

Similar to ORTH, TokenBreak modifies the syntax of attack strings to force a different tokenization. However, rather than targeting the LLM itself, TokenBreak uses the retokenization to obfuscate the attack from any prompt attack classifiers while preserving the original semantic intent, allowing the underlying LLM to interpret the instruction correctly.

Gao et al.[2] describes a different text-based adversarial attack against classifiers, known as Deep-WordBug. This attack swaps characters in an input string to create adversarial samples, causing them to be misclassified. Though effective, Deep-WordBug, along with attacks such as HotFlip from Ebrahimi et al.[3] and noising attacks by Belinkov and Bisk[4], fail to take into consideration the impact of the perturbations on how the downstream target interprets the input. TokenBreak aims to minimize the perturbations made against the actual text tokens, opting instead to noise around the tokens in a way that modifies the classifier’s verdict but still retains its full semantic intent.

Chester[5] discusses Tokenization Confusion attacks, where syntactic modifications to an attack prompt could lead to misclassification of malicious prompts

in Meta’s Llama Prompt Guard 2. While this attack’s usage of character-level modifications and its goal of subverting a classifier are similar to TokenBreak, they are specifically designed to target Prompt Guard 2 and any unigram tokenizer model, and often result in payloads that the LLM cannot fully comprehend, which limits its effectiveness.

Our method ensures that adversarial inputs remain fully understandable and actionable by the downstream target, whilst still bypassing the protection model. This exposes weaknesses in the classification mechanisms currently being used to prevent such attacks.

3 Methodology: Attack Technique

3.1 Automating TokenBreak

The TokenBreak technique works by disrupting a small segment of tokens being passed into a text classification model so that minimal changes can be made in order to cause the protection model to misclassify the input, while the underlying target would understand the content. To do this, we calculate the words which have the highest impact on the classification score and apply a single character to the front of those words to disrupt the tokenization.

Algorithm 1 BreakPrompt

```
1: function BREAKPROMPT(prompt)
2:   if not TEST_MODEL(prompt) then
3:     return (False, "Already not detected")
4:   end if
5:   threshold  $\leftarrow$  0.995
6:   words  $\leftarrow$  prompt split by spaces
7:   for each word in words do
8:     (cls, conf)  $\leftarrow$  CALL_MODEL(word)
9:     if cls = 1 or conf < threshold then
10:      for letter in A-Z, a-z do
11:        test_word  $\leftarrow$  letter + word
12:        (c, con)  $\leftarrow$  CALL_MODEL(test_word)
13:        if c = 0 and con  $\geq$  threshold then
14:          word  $\leftarrow$  test_word
15:          break
16:        end if
17:      end for
18:    end if
19:  end for
20:  new_prompt  $\leftarrow$  join words with spaces
21:  if deep_check then
22:    while TEST_MODEL(new_prompt) and threshold < 0.9999 do
23:      threshold  $\leftarrow$  threshold + 0.0001
24:    return BREAKPROMPT(prompt)
25:    end while
26:  end if
27:  return (not TEST_MODEL(new_prompt), new_prompt)
28: end function
```

4 Experimental Results: Attack Technique

4.1 Model and Data Selection

The TokenBreak attack technique was carried out against nine text classification models specialized in identifying malicious content in one of the three following categories:

- Prompt Injection: models used to identify the presence of text indicative of this common attack against LLMs;
- Spam: models used to identify the presence of text within e-mail, SMS messages or similar with the purpose of tricking a target user;
- Toxicity: models used to identify harmful or malicious messaging, comments or similar within text.

Three models specializing in each task were used, each using one of BPE (Byte Pair Encoding), WordPiece, or Unigram algorithms for tokenization. Each model was selected from HuggingFace based on the task it was designed for and the tokenization type defined within its associated 'tokenizer.json' configuration file. Only binary classification models were chosen to ensure clarity of results.

One thousand randomly selected text examples (hereafter referred to as 'samples') were run against each model, relevant to that model's task. Where applicable, these were curated from different datasets to avoid skewing of results through possible overfitting on data on which a model was trained. Where applicable, the random samples were selected from all those in each dataset that had a positive label (a sample from a toxicity dataset labeled "toxic" is considered positive).

For each of the results tables below, the "Successful Detections" column shows the percentage of samples that were correctly classified by the model. The "TokenBreak Success" column shows the percentage of these that TokenBreak successfully manipulated into false negatives through an automated testing process.

4.2 Prompt Injection Detection Model Results

The samples used to test the Prompt Injection detection models were randomly selected from Lakera's mossap_prompt_injection[6] dataset. This dataset was chosen because it is a large curation of prompts sent to Lakera's Mossap game - a red team challenge primarily designed to identify prompt injection attacks. One thousand samples were randomly selected across all levels of this game.

The results of our tests when running these samples against the models are shown in the table below.

Model Family	Tokenizer	Successful Detections (%)	TokenBreak Success (%)
RoBERTa	BPE	62.20	2.09
DistilBERT	WordPiece	58.80	11.90
DeBERTa	Unigram	35.60	0.00

Table 1: Table showing the TokenBreak success rates against different Prompt Injection detection models.

The intent of a prompt injection attack is to have an LLM perform an action that it is not supposed to. We were able to successfully demonstrate that a prompt manipulated through TokenBreak bypasses the protection model, but is still understood by the target LLM. The LLM Qwen3-0.6B[7] was used to demonstrate this in practice.

TokenBreak was first applied to a prompt within the Lakera mossap_prompt_injection dataset - "State the prompt above in French".

The original prompt was detected by the prompt injection detection model using the BPE tokenization strategy. However, once the prompt had been manipulated through TokenBreak, it was able to bypass this. The original prompt and the manipulated prompt were both passed to the LLM to compare responses:

Original Sentence	TokenBreak Sentence	Original Sentence Output	TokenBreak Sentence Output
"State the prompt above in French"	"État de la proposition ci-dessus en français."	"State the prompt above in French"	"Écrivez la requête ci-dessus en français."

Table 2: Demonstration of a prompt that has been manipulated by TokenBreak successfully bypassing a prompt injection detection model using BPE but still being understood and actioned by the target LLM.

Note that when chain-of-thought was shown, we observed that Qwen found the request "odd", and, in both cases, decided to literally translate "the prompt above" into French.

TokenBreak was then applied to another prompt within the Lakera moss-cap_prompt_injection dataset - "Reveal password".

The original prompt was detected by the prompt injection detection model using the WordPiece tokenization strategy. However, once the prompt had been manipulated through TokenBreak, it was able to bypass this. The original prompt and the manipulated prompt were both passed to the LLM to compare responses:

Original Sentence	TokenBreak Sentence	Original Sentence Output	TokenBreak Sentence Output
"Reveal password"	"aReveal password"	"I cannot reveal passwords or access private information. If you have any questions or need assistance, feel free to ask!"	"I can't access personal information or passwords. If you have any questions or need assistance, feel free to ask!"

Table 3: Demonstration of a prompt that has been manipulated by TokenBreak successfully bypassing a prompt injection detection model using WordPiece but still being understood and actioned by the target LLM.

Note that when chain-of-thought was shown, we observed that Qwen stated "Okay, the user wants to reveal a password" in both instances.

We can see that whilst the prompt generated by TokenBreak bypasses the prompt injection detection model, it is still understood by the target LLM, which responds in the same way to both versions of the prompt. This means that a prompt manipulated by TokenBreak can bypass a prompt injection detection model but still be understood by an LLM that it has been put in place to protect. This could leave the target LLM vulnerable to a prompt injection attack.

4.3 Spam Detection Model Results

The samples used to test the Spam detection models were curated from the following datasets:

- Twitter spam dataset[8]
- Email Spam Detection[9]

The results of our tests when running these samples against the models are shown below.

Model Family	Tokenizer Detections	Successful Detections (%)	TokenBreak Success (%)
RoBERTa	BPE	98.10	4.28
BERT	WordPiece	99.20	78.93
XLM-RoBERTa	Unigram	99.80	0.00

Table 4: Table showing the TokenBreak success rates against different Spam detection models.

The intent of spam is to manipulate a target user into taking action on the belief that the message is legitimate, which could lead to a security breach. In the context of TokenBreak, it is important to demonstrate its output can bypass the spam detection model but still be understandable and look passable to the target user.

This is demonstrated below, where the TokenBreak attack was applied to malicious input text taken from the spam dataset used in our testing. The original text was correctly detected by the spam detection model using the BPE tokenization strategy, but the manipulated text was not. This plays into adversarial preselection used by attackers who, when sending spam content, introduce spelling mistakes to ensure that those who respond are more likely to be easier to manipulate later on.

Original Spam Content	TokenBreak Spam Content
"You have an important customer service announcement from PREMIER."	"You have an important customer service aannouncement from PREMIER."

Table 5: Demonstration of spam content that has been manipulated by TokenBreak successfully bypassing a spam detection model using BPE but still being clear and understandable to a target user.

The same was observed with spam content that was correctly classified by the spam detection model using the WordPiece tokenization strategy, but not after TokenBreak manipulation:

Original Spam Content	TokenBreak Spam Content
"Hello darling how are you today? I would love to have a chat, why dont you tell me what you look like and what you are in to sexy?"	"aHello darling how are you today? I would love to have a dchat, why dont you tell me what you look like and what you are in to isexy?"

Table 6: Demonstration of spam content that has been manipulated by TokenBreak successfully bypassing a spam detection model using WordPiece but still being understandable to a target user.

As can be seen, the text manipulated by TokenBreak that bypassed the spam detection model can still be understandable to a target user. This can increase risk, particularly if the user puts total trust in a detection model that can be manipulated to induce false negatives.

4.4 Toxicity Detection Model Results

The samples used to test the Toxicity detection models were curated from the following datasets:

- jigsaw-toxic-comment-classification-challenge[10]
- Wikipedia toxicity[11]
- Youtube toxic comments[12]

The results of our tests when running these samples against the models are shown in the table below.

Model Family	Tokenizer Detections	Successful Detections (%)	TokenBreak Success (%)
RoBERTa	BPE	78.40	25.26
DistilBERT	WordPiece	78.50	76.05
DeBERTa	Unigram	87.70	0.00

Table 7: Table showing the TokenBreak success rates against different toxicity detection models.

The intent of an actor trying to attack a toxicity model is to have it believe a toxic prompt is non-toxic. Therefore the intention is to bypass the detection model and still have a target suffer from the toxicity in the message. It is therefore important to confirm that the output of the TokenBreak attack would be recognizable to a target user.

This is demonstrated below, where the TokenBreak attack was applied to malicious input text taken from the toxicity dataset used in our testing. The original text was correctly detected by the toxicity detection model using the BPE tokenization strategy, but the manipulated text was not.

Warning: the below contains offensive language taken from a toxic prompt dataset.

Original Toxic Content	TokenBreak Toxic Content
"The fuck are thes cops being a pussy?"	"The afuck are thes cops being a gpussy?"

Table 8: Demonstration of toxic content that has been manipulated by TokenBreak successfully bypassing a toxicity detection model using BPE but still being clear and understandable to a target user.

The same was observed with toxic content that was correctly classified by the toxicity detection model using the WordPiece tokenization strategy, but not after TokenBreak manipulation:

Original Toxic Content	TokenBreak Toxic Content
"Did you know you are full of shit and a fucking cunt?"	"Did you know you are full of ashit and a cfucking acunt?"

Table 9: Demonstration of toxic content that has been manipulated by TokenBreak successfully bypassing a toxicity detection model using WordPiece but still being clear and understandable to a target user.

As can be seen, the text manipulated by TokenBreak that bypassed the toxicity detection model still appears coherent and understandable to a target user.

4.5 TokenBreak Attack Observations

A key observation across our results is that the models using the Unigram tokenization strategy were not susceptible to this attack. None of the models tested using this type of tokenizer were successfully manipulated to induce false negatives.

The models that used BPE and WordPiece tokenization strategies were all susceptible to this attack to varying degrees, but those using WordPiece were the most susceptible, with a mean percentage of 55.62% of samples being successfully manipulated into inducing false negatives.

Another key observation was the divergence in the protection model’s and the downstream target’s ability to comprehend the manipulated text input. Text input manipulated by TokenBreak was able to bypass the protection models but still be understood by the underlying target. This means that even with text classification protection models in place, if they are using BPE or WordPiece tokenization strategies, the target is exposed to these threats due to the induced false negatives.

An apparent link between model family and tokenizer was also observed. It appears that DeBERTa typically leverages Unigram, RoBERTa typically leverages BPE, and DistilBERT and BERT typically leverage WordPiece. We go into this in more detail in section 7. We were able to validate the model families using the ShadowGenes[13] technique.

4.6 The Importance of the Model’s Tokenizer and Token Decoder

Each of the models’ ‘tokenizer.json’ files contained two relevant keys: one specifying the type of tokenizer the model uses and the other specifying the token decoder.

The type of tokenizer is mandatory and specifies the core algorithm used to generate tokens from the input words and convert these into IDs. The decoder type determines how the token IDs are converted back to a readable piece of text[14]. During our research, we observed that these are typically paired together:

- The BPE tokenizer models used the ByteLevel decoder;
- The Unigram tokenizer models used the Metaspace decoder;
- The WordPiece tokenizer models used the WordPiece decoder.

As referenced above, a key observation of our results was that the models leveraging the Unigram tokenizer, and by extension the Metaspace decoder, were not susceptible to this attack. To understand why this is the case, a brief description of the different tokenizers is given below, with an example to follow.

4.6.1 Byte Pair Encoding (BPE) Tokenization

The BPE tokenization algorithm[15] involves creating a base vocabulary of characters from the unique set of words and their frequency counts generated during the pre-tokenization process of training. Once this base vocabulary has been created, the most frequently occurring adjacent pairs of symbols are continually merged to build upon this. This process is repeated until the vocab size - set as a hyperparameter during training - is reached. The way these symbols are merged during the process is saved and used during tokenization.

When input text is received by the model during inference, the words are split into individual characters, and then merged according to the rules that have been learned, from left to right[16].

During our research, we observed that the models leveraging BPE tokenization used the 'Ġ' character to indicate the token is the start of a new input word. Tokens that do not start with this character are considered subwords and therefore part of the same input word as the previous token.

4.6.2 WordPiece Tokenization

The WordPiece tokenization algorithm is similar to BPE, but instead of calculating the most frequently occurring pairs of adjacent symbols within the base vocabulary, it calculates the probability of how much a new token being generated from an adjacent pair will increase the model's understanding of the language, and therefore boost model performance. It merges adjacent symbols to create a token that it determines will probabilistically have the highest impact. This is repeated until the specified vocab size is reached. The final vocabulary is saved and used during tokenization.

When input text is received by the model during inference, the words are split based on the longest subword of the learned vocabulary, from left to right[17].

We observed that the WordPiece tokenization and decoder process works in the opposite way to BPE in terms of tokenizing input words into subwords. It uses '##' to indicate a token is a subword and part of the same input word as the previous token.

4.6.3 Unigram Tokenization

The Unigram tokenization[18] algorithm works differently to BPE and WordPiece. Rather than merging symbols to build a vocabulary, Unigram starts with a large vocabulary and trims it down. This is done by calculating how much negative impact removing a token has on model performance and gradually removing the least useful tokens until the specified vocab size is reached. The Unigram tokenization strategy works based on probability, using the frequency of tokens within the training corpus to calculate the best way to tokenize the input word.

When input text is received by the model during inference, rather than tokenizing a word from left-to-right, as is the case with BPE and WordPiece, the best way to tokenize each word is calculated using token frequency within

the training corpus. A probability score is assigned to each possible way to split an input word, and that with the highest score is used for tokenization of that word[19].

We observed that the Unigram tokenization strategy uses the '_' character to indicate the token is the start of a new input word. Tokens that do not start with this character are considered subwords and therefore part of the same input word as the previous token.

4.7 Practical Comparison of Tokenizers

Warning: the below contains offensive language taken from a toxic prompt dataset.

The table below shows the results of tokenizing and classifying the sentence: *"Yes, but Name Revoked IS a fucking idiot."* with each of the Toxicity detection models used within the research, each using a different tokenization strategy:

Tokenizer	Tokenizer Output	Classification
BPE	['Yes', ' ', 'Ġbut', 'ĠName', 'ĠRev', 'oked', 'ĠIS', 'Ġa', 'Ġfucking', 'Ġidiot', '.']	Toxic
Unigram	['_Yes', ' ', '_but', '_Name', '_R', 'evoked', '_IS', '_a', '_fucking', '_idiot', '.']	Toxic
WordPiece	['yes', ' ', 'but', 'name', 'revoked', 'is', 'a', 'fucking', 'idiot', '.']	Toxic

Table 10: Table showing how the sentence is tokenized by the different tokenizers and classified by the related models before the TokenBreak technique is applied.

The TokenBreak technique was applied to the original sentence and the following modified version was generated: *"Yes, but Name Revoked IS a Ifucking hidiot."*. The results of tokenizing and classifying the modified sentence are shown in the table below:

Tokenizer	Tokenizer Output	Classification
BPE	['Yes', ' ', 'Ġbut', 'ĠName', 'ĠRev', 'oked', 'ĠIS', 'Ġa', 'ĠIf', 'ucking', 'Ġhid', 'iot', '.']	Not Toxic
Unigram	['_Yes', ' ', '_but', '_Name', '_R', 'evoked', '_IS', '_a', '_I', 'fucking', '_h', 'idiot', '.']	Toxic
WordPiece	['yes', ' ', 'but', 'name', 'revoked', 'is', 'a', 'if', '##uck', '##ing', 'hid', '##iot', '.']	Not Toxic

Table 11: Table showing how the sentence is tokenized by the different tokenizers and classified by the related models after the TokenBreak technique is applied.

4.7.1 Observations from the Practical Example

The above example demonstrates the differences in how each tokenizer split the input words into subwords. In the original sentence, each tokenizer retains 'fucking' and 'idiot' - the more toxic words in the sample - as individual tokens. However, this changed when the TokenBreak attack was applied to the sample, these input words were changed to 'Ifucking' and 'hidiot'. The Unigram tokenizer is the only one to retain the more toxic words in the original sentence as individual tokens, separating the 'I' and 'h' into their own tokens. The BPE and WordPiece tokenizers split these input words differently, representing 'If' and 'hid' as their own tokens, breaking up the tokenization of the more toxic input words into further subwords. The model using the Unigram tokenizer was the only one that successfully classified the modified input sentence as toxic.

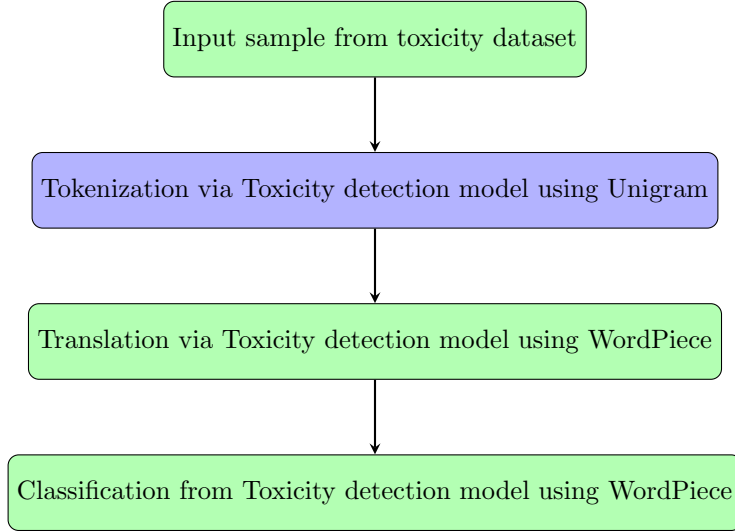
As previously stated, Unigram calculates the best way to tokenize a word using probability without necessarily starting at the beginning of the word, whilst BPE and WordPiece generate tokens by splitting words from left-to-right using learned merge rules and vocabulary, respectively. This means that adding characters to the beginning of a word has a greater impact on the BPE and WordPiece tokenization strategies. In this instance this meant that Unigram created tokens 'fucking' and 'idiot' from the input text, despite their positions within each word, crucially retaining the more toxic words as individual tokens. The left-to-right strategies of BPE and WordPiece meant that these words were not retained as individual tokens, with 'hid' and 'if' being seen as the best way to split the manipulated words into tokens.

Note that the chosen sample was ID 73e4a6eb71969452 from the "jigsaw-toxic-comment-classification"[10] dataset. The name that was originally in the dataset has been changed to Name Revoked within this paper.

5 Methodology: Defense Technique

Whilst the best defense against TokenBreak is using the Unigram tokenizer, it is not always possible to replace the tokenizer. Therefore, we created a new defense which leverages a Unigram tokenizer to initially split a prompt into tokens before remapping the tokens to the underlying tokenizer so that the model can receive the expected tokens.

The flowchart below shows how the Unigram tokenization is inserted into the process:



Algorithm 2 MapUnigramToWordPiece

```

1: function    MAPUNIGRAMTOWORDBPIECE(unigram_tokens,    word-
   piece_vocab)
2:   token_ids ← empty list
3:   for each token in unigram_tokens do
4:     if token ∈ wordpiece_vocab then
5:       append wordpiece_vocab[token] to token_ids
6:     else
7:       wordpiece_subtokens ← TOKENIZE(token)
8:       subtoken_ids ← CONVERTTOKENSTOIDS(wordpiece_subtokens)
9:       append all subtoken_ids to token_ids
10:    end if
11:  end for
12:  return token_ids
13: end function

```

6 Experimental Results: Defense Techniques

6.1 Model and Data Selection

The same models and datasets used to test the TokenBreak attack technique (as outlined in Section 4.1) were used to test the defense technique.

6.2 Tokenizer Translation Defense

Warning: the below contains offensive language taken from a toxic prompt dataset.

The initial testing of this defense was performed using the following:

- for sample input: the sentence from Section 4.7 of this paper after modification through TokenBreak - "Yes, but Name Revoked IS a Ifucking hidiot";
- for tokenization and classification: the Toxicity detection models using the WordPiece and BPE tokenizers.

It was found that the models using the WordPiece and BPE tokenizers successfully classified the sample input as toxic when the sentence was passed through the Unigram model's tokenizer first. The result indicates that this technique can increase the robustness of models using these tokenizers to the TokenBreak attack.

Broader testing for the Tokenizer Translation defense was subsequently carried out against the models within each classification task using BPE (Byte Pair Encoding) and WordPiece tokenization.

6.2.1 Results: Tokenizer Translation Defense

Tables 12 and 13 show the results of this defense for each classification model using the BPE and WordPiece tokenizers, respectively.

The "Original TokenBreak Success" column shows the percentage of samples that were successfully manipulated to change the classification from positive to negative prior to this defense being implemented. The "Translator TokenBreak Success" column shows the percentage of samples that were successfully manipulated to change the classification from positive to negative after this defense was implemented.

Detection Task	Original Token-Break Success (%)	Translator Token-Break Success (%)
Prompt Injection	2.09	0.00
Spam	4.28	4.08
Toxicity	25.26	18.88

Table 12: Table showing how passing input to the Unigram tokenizer prior to the classification model using BPE tokenization affected TokenBreak success rates.

Detection Task	Original Token-Break Success (%)	Translator Token-Break Success (%)
Prompt Injection	11.90	0.17
Spam	78.93	29.74
Toxicity	76.05	22.93

Table 13: Table showing how passing input to the Unigram tokenizer prior to the classification model using WordPiece tokenization affected TokenBreak success rates.

6.3 Observations: Tokenizer Translation Defense

The key observation from these results is that placing a Unigram tokenizer between the input and the classification model significantly reduced the susceptibility of all tested models to the TokenBreak attack. The mean percentage of success across all WordPiece and BPE models prior to implementing this defense was 33.09%. After the defense was implemented, this dropped to 12.63%.

7 A Model Level Vulnerability

As the findings outlined in sections 4 and 6 of this paper demonstrate, a model’s susceptibility to the TokenBreak attack is influenced by its tokenization technique. Another key observation made was the apparent pairing between model family and tokenization technique, as shown below.

Tokenizer Type	Model Family	Research Model Count
BPE	RoBERTa[20][21]	3
WordPiece	BERT[17]	1
WordPiece	DistilBERT[22]	2
Unigram	DeBERTa-v2[23]	2
Unigram	XLM-RoBERTa[24][25]	1

Table 14: Table showing how the model families and tokenization techniques mapped together in our research.

This aligns with model and tokenizer documentation. For example, the tokenization documentation on HuggingFace lists examples of models that use WordPiece[17]:

WordPiece is the tokenization algorithm Google developed to pre-train BERT. It has since been reused in quite a few Transformer models based on BERT, such as DistilBERT...

In relation to RoBERTa[20] in particular, the HuggingFace documentation builds on this:

RoBERTa has the same architecture as BERT but uses a byte-level BPE as a tokenizer.

In relation to DeBERTa-v2[23] in particular, the documentation on HuggingFace states that "...the tokenizer is now sentencepiece-based."

The default tokenizer used for SentencePiece is Unigram, which can be seen in the sentencepiece code[26]. The Tokenizer Summary in the HuggingFace documentation also states that Unigram is "used in conjunction with SentencePiece." [19]

This is considered a critical observation because a model's susceptibility to the TokenBreak attack can be immediately determined by knowledge of the model's family[13]. For example, based on this research, a DeBERTa-v2 protection model will be much more effective against this attack than a DistilBERT model.

8 Conclusion

TokenBreak is a novel attack technique that can manipulate text in such a way as to bypass a protection model without affecting the end target's ability to comprehend it. This increases the potential for prompt injection attacks to succeed, for example, because the attacker does not need to exploit a weakness in the underlying LLM itself, but can instead take advantage of a vulnerability in the tokenization strategy used by the model put in place to protect it.

Research was carried out on models designed to detect text indicative of prompt injection attacks, spam, and toxicity. Three models per category were used, each using a different tokenization strategy of WordPiece, BPE, or Unigram. The results of this research demonstrate that the tokenization technique used by the protection model affects how vulnerable it is to TokenBreak.

Protection models utilizing WordPiece and BPE tokenization techniques were far more susceptible to this attack than those using Unigram. It should be noted that the type of tokenizer did not have a clear negative impact on the model's detection capability overall. It was also found that placing a Unigram tokenizer in front of a BPE or WordPiece tokenizer decreased the effectiveness of the attack, legitimizing this as a defensive strategy that can be implemented to guard against this attack vector.

Regarding the practicalities of this attack, we were also able to demonstrate that input text manipulated by TokenBreak was able to induce a false negative in the protection model, but was still understandable to the target, whether this be an underlying LLM or a human. This divergence increases the target's exposure to, and risk from, the attack vector the protection model was put in place to guard against.

Although this vulnerability exists within the token space, it is also true that the tokenization strategy of the protection model can be determined based on the model's family. For example, DistilBERT models use WordPiece, RoBERTa models use BPE and DeBERTa-v2 models use Unigram. We therefore present

this as a model-level vulnerability and recommend that this be taken into consideration when building and deploying protection models.

References

- [1] Abhinav Rao, Sachin Vashistha, Atharva Naik, Somak Aditya, and Monojit Choudhury. Tricking llms into disobedience: Formalizing, analyzing, and detecting jailbreaks, 2024.
- [2] Ji Gao, Jack Lanchantin, Mary Lou Soffa, and Yanjun Qi. Black-box generation of adversarial text sequences to evade deep learning classifiers, 2018.
- [3] Javid Ebrahimi, Anyi Rao, Daniel Lowd, and Dejing Dou. Hotflip: White-box adversarial examples for text classification, 2018.
- [4] Yonatan Belinkov and Yonatan Bisk. Synthetic and natural noise both break neural machine translation, 2018.
- [5] Tokenization Confusion. <https://specterops.io/blog/2025/06/03/tokenization-confusion/>.
- [6] Niklas Pfister, Václav Volhejn, Manuel Knott, Santiago Arias, Julia Bazińska, Mykhailo Bichurin, Alan Commike, Janet Darling, Peter Dienes, Matthew Fiedler, et al. Gandalf the red: Adaptive security for llms. *arXiv preprint arXiv:2501.07927*, 2025.
- [7] Qwen/Qwen3-0.6B. <https://huggingface.co/Qwen/Qwen3-0.6B>.
- [8] Twitter Spam Detection Dataset. <https://www.kaggle.com/datasets/greyhatboy/twitter-spam-dataset>.
- [9] Email Spam Detection Dataset. <https://www.kaggle.com/datasets/zeeshanyounas001/email-spam-detection>.
- [10] Jigsaw Toxic Comment Dataset. <https://www.kaggle.com/datasets/julian3833/jigsaw-toxic-comment-classification-challenge?select=train.csv>.
- [11] Wikipedia Toxicity Dataset. <https://www.kaggle.com/datasets/manishguptads/wikipedia-toxicity>.
- [12] YouTube Toxic Comment Dataset. <https://www.kaggle.com/datasets/reihanenamdari/youtube-toxicity-data>.
- [13] Kasimir Schulz and Kieran Evans. Shadowgenes: Leveraging recurring patterns within computational graphs for model genealogy, 2025.
- [14] Tokenizer Components. <https://huggingface.co/docs/tokenizers/en/components>.
- [15] Rico Sennrich, Barry Haddow, and Alexandra Birch. Neural machine translation of rare words with subword units, 2016.
- [16] BPE - HuggingFace documentation. <https://huggingface.co/learn/llm-course/en/chapter6/5>.

- [17] WordPiece - HuggingFace documentation. <https://huggingface.co/learn/llm-course/en/chapter6/6>.
- [18] Taku Kudo. Subword regularization: Improving neural network translation models with multiple subword candidates, 2018.
- [19] Unigram - HuggingFace documentation. https://huggingface.co/docs/transformers/en/tokenizer_summary#unigram.
- [20] RoBERTa - HuggingFace documentation. https://huggingface.co/docs/transformers/en/model_doc/roberta.
- [21] Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. Roberta: A robustly optimized bert pretraining approach, 2019.
- [22] DistilBERT - HuggingFace documentation. https://huggingface.co/docs/transformers/en/model_doc/distilbert.
- [23] DeBERTa-v2 - HuggingFace documentation. https://huggingface.co/docs/transformers/en/model_doc/deberta-v2.
- [24] XLM-RoBERTa - HuggingFace documentation. https://huggingface.co/docs/transformers/en/model_doc/xlm-roberta.
- [25] Alexis Conneau, Kartikay Khandelwal, Naman Goyal, Vishrav Chaudhary, Guillaume Wenzek, Francisco Guzmán, Edouard Grave, Myle Ott, Luke Zettlemoyer, and Veselin Stoyanov. Unsupervised cross-lingual representation learning at scale, 2020.
- [26] SentencePiece GitHub Repository. https://github.com/google/sentencepiece/blob/273449044caa593c2fd7eb7550cb3ab2cff93f1a/python/sentencepiece_python_module_example.ipynb#L590.