目标在线密码猜测模型 基于指针生成器网络

杨丽、李勇、陈习安、石瑞新、冀中汉
中国科学院信息工程研究所
中国科学院大学网络安全学院
北京，中国
[狮子8119，韩中]@iie.ac.cn

摘要：现有的目标在线密码猜测模型是基于无概率上下文语法（PCFG），其固有的缺点是猜测结构对不同的用户总是相同的。这个问题会导致猜测效率低下。为了解决这一问题，我们提出了一个由指针生成器网络组成的目标在线密码猜测模型（PG-Pass）。它可以自动了解个人信息对密码的影响，并更准确地猜测目标用户的密码。通过大量的实验，我们得到了最优参数。结果表明，在只有个人识别信息（PII）的条件下，PG-Pass模型的一次猜测成功率达到19.49%，是TarGuess-I的10倍。当猜测100次时，猜测成功率为41.07%，证明了本文所提模型的有效性。

关键词-目标在线密码猜测，深度学习，指针生成器网络

Ⅰ.介绍

文本密码是目前最流行的身份验证技术之一。它具有操作方便、熟悉用户的优点，在可预见的未来[1]仍将使用。由于有太多的网站密码需要用户记住，用户总是选择的密码远离随机的[2] [3]。他们选择容易记住的字符串作为密码的一部分，比如个人信息，这给了攻击者一个机会。大多数网站执行严格的密码政策，并安排网站密码强度计来帮助用户建立安全的密码。然而，这些密码强度计被证明是特别的和不一致的[4]。此外，还提出了几种密码猜测模型来衡量密码强度。

根据攻击模式和所使用的个人信息，密码猜测模型可以分为目标在线猜测和拖网离线猜测。[5] [6] [7]最近进行了一些关于拖网捕鱼和离线猜测的研究。由于个人身份信息（PII）成为可用的[8]，有针对性的在线攻击引发了担忧。据我们所知，在有针对性的在线猜测中，Das等人。[9]研究了密码的重用问题，并首次提出了一种跨站点的密码猜测模型。然后，李等人。[10]分析了PII是如何影响密码的。通过将PII添加到概率上下文无关语法（PCFG）中，他们提出了个人-PCFG模型。之后，王等人。[8]系统地描述了典型的目标猜测场景，并创造性地提出了TarGuess-I模型。然而，这些模型都是基于PCFG的，由于生成密码的顺序固定，PCFG有限制
结构这与用户编写密码的不同习惯不一致。

本文主要针对于有针对性的在线密码猜测。我们提出了一种基于指针生成器网络[11]的目标在线密码猜测模型（PGPass），旨在更准确地猜测目标用户的密码。选择指针生成器网络是因为它是自动文本摘要中最实用的方法之一。基于复制机制，指针生成器网络增强了处理词汇表外（OOV）单词的能力，同时保持了生成新单词的能力。我们认为，生成一个基于密码的PII类似于从文本中生成一个摘要。实验结果表明，PG-Pass模型能够在较少的猜测时间下优于以往所有的目标在线密码猜测模型。

我们总结了我们的主要贡献如下：

- 提出了一种新的目标在线密码猜测模型（PG-Pass），该模型可以在PII的基础上很好地编写密码，产生高质量的猜测。据我们所知，这是指针生成器网络第一次应用于目标在线猜测。
- 我们设计了整体的PG-Pass模型框架，包括数据处理、模型训练和密码生成三个步骤。通过大量的实验，我们得到了最优参数。
- 实验结果表明，PG-Pass模型在目标在线密码猜测中取得了最先进的性能。PGPass模型的猜测成功率可达到19个。猜一次49%。

本文的组织结构如下。二、简要概述了相关工作。教派。III提出了模型框架。教派。四、我们进行了实验，并分析了我们的模型的效果。我们的结论是在最后一节中得出的。

Ⅱ.相关工作

目标在线密码猜测的研究时间比离线猜测要短。在过去的五年中，已经进行了一些初步的工作。

9781-6654-0527-0/22/$31.00©2022IEEE507

2022年第25届计算机支持设计合作工作国际会议（CSCWD）|978-1-6654-0527-0/22/$31.00©2022IEEE|DOI：10。1109/CSCWD54268.

可以相信，有两个因素可能会影响所获得的猜测成功率。一种是如何描述密码中的PII，另一种是找到一个合适的模型来基于PII生成密码。据我们所知，之前的工作主要集中在描述密码中的PII上。

2016年，李等人。[10]探讨了用户的PII在密码中的存在程度。分析结果将PCFG扩展到语义丰富的模型，并提出了个性化PCFG模型。除了PCFG中的“L”、“D”和“S”符号外，Paporal-PCFG还增加了六种PII类型，包括生日、姓名、电子邮件地址、帐户名称、手机号码和身份证号码。该模型采用了一种基于长度的PII匹配方法。他们将整个密码与PII进行匹配，记录匹配的字符串的长度，并将其替换为一个PII符号。对于密码中不匹配的字符串，PporsonalPCFG将其替换为LDS符号。在生成阶段，Papiol-PCFG用基于排序结构的片段替换LDS和PII符号。

2016年，Wang等人。[8]系统地分析了典型的目标猜测场景，并提出了目标在线猜测框架TarGuess。他们发现了基于长度的PII匹配方法的弱点，这可能会低估或高估PII的使用。此外，基于长度的标记对它们的子类型不敏感。因此，他们提出了一种基于类型的PII匹配方法。对于基于类型的PII标记，它的下标数字代表一个PII的特定子类型，而不是长度。基于基于类型的PII标签和PCFG模型，他们为场景1提出了相应的TarGuess-I模型，并提高了猜测成功率。王等人。“工作[8]
已经导致了对NIST SP800-63-2的修订。

2020年，Xie [12] [13]发现一些有效的语义标签还没有被证实，并在TarGuessI模型中使用。在TarGuess-I中添加了三种类型的语义标签后，他们提出了
TarGuess-I^{+KPX}. “P”表示从类似于目标网站的数据集创建的流行密码列表；“K”表示在标准键盘上用物理位置序列识别密码片段；“X”表示用户生成的PII中的连续字符。他们进一步提高了治疗的效果
TarGuse-I模型。

他们研究的主要缺点是他们没有尝试尝试新的模型。所有这些工作基本上都是基于PCFG的。在密码生成阶段，PCFG通过实例化密码结构频率表来获得候选密码。不同用户的密码结构的猜测顺序是相同的，区别在于填充的字段。实际上，不同用户的密码结构并不是按照相同的顺序排列的。因此，肯定有改进的空间。然后，我们在后面的部分中介绍了本文提出的PG-Pass模型。

III .模型框架

在本节中，我们将详细讨论PG-Pass模型框架。如图所示。1、PG-Pass模型框架由三个步骤组成：数据处理、模型训练和密码生成。首先，数据处理的特征并标记PII，根据这些PII标签分割密码，并将这些数据组织成指针生成器网络支持的格式。其次，在训练阶段，指针生成器网络学习PII和密码之间的重要关系，并模拟密码分布。第三，利用波束搜索，指针生成网络根据目标用户的PII生成猜测密码。

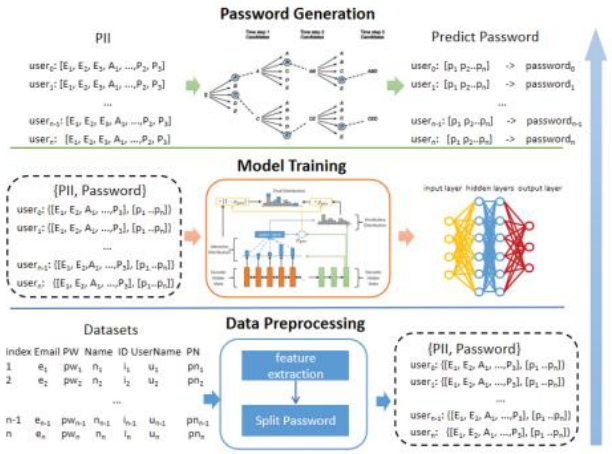

图1. PG-Pass模型的框架。

A. 数据预处理

密码可以看作是短写文本，但它们与自然语言有些不同。例如，密码不是由汉字组成的，而是由拼音字母或与中文文本相比的单个字符组成的。与英文文本相比，没有明显的空间分隔符。因此，自然语言处理模型不能直接用于密码文本中。

以12306（一个火车票务网站）数据集为例，原始的PII包括五个属性：姓名、电子邮件地址、手机号码、帐户名和身份证号码。这个名字是由汉字组成的。生日是隐藏在ID号中的。所以我们需要提取PII并用标签来描述它们。我们使用基于PII标签的字符串匹配方法来分割用户的密码来进行训练数据。然后，我们将不匹配的字符串分成密码中的单个字符。

B. 模型培训

输入数据集D包含训练阶段的PII和密码两部分，可以表示如下。例如，U_1表示第一个用户的PII，P_1表示第一个用户的密码。与此同时，U_1= [u11, .,u1k和P1= [p11, .,p1l]中分别包含几个值
他们，u11表示第一个用户的PII的第一个PII标签，p11表示第一个用户的密码的第一段。

$$D = \{[U_1,P_1], [U_2,P_2], \ldots, [U_n,P_n]\}$$

这个问题类似于在PII的指导下生成密码。本文利用了指针生成器网络。指针生成器网络的框架

如图2所示。在这里，我们将PII作为原始文章，并将密码片段作为文本摘要。

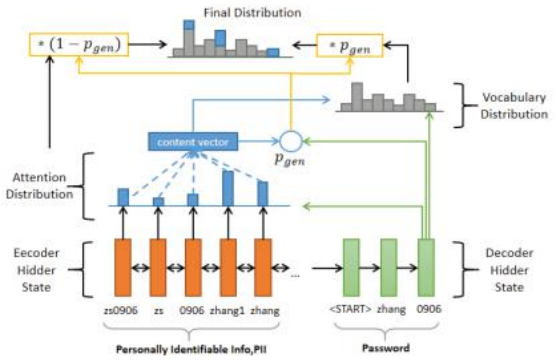

图2. 指针生成器网络的构建框架。

1)Seq2Seq：指针生成器网络基于序列到序列（Seq2Seq）。PII被编码到中间层的隐藏状态，然后解码成另一种表示。在编码过程中，该模型使用单层双向长短期记忆（LSTM）网络来计算PII的隐藏状态h和隐藏状态hi在PII中的第t个标签。在解码过程中，该模型增加了一个注意机制，并使用了一个单层的单向LSTM。在训练阶段，每一步t模型输入PII的标签，以获得解码状态st.使用hi和st来获得注意力的重量 a^t此时此刻，在PII中的标签。

$$e_i^t = v^T tanh(W_h h_i + W_s s_t + b_{attn})$$

$$a^t = softmax(e^t)$$

接下来，注意力的权重是a^t和隐藏状态hi计算一个上下文向量h_t^*.

$$h_t^* = \sum_i a_i^t h_i$$

上下文向量h_t^*是否与解码器的状态相连接t并通过两个线性层来生成词汇表分布Pvocab. Pvocab是词汇表中所有单词的概率分布。

Pvocab=软最大值（V\(V [st$_t^*$,h]+ b)+ b\)

*2)指针发生器网络：指针发生器网络引入了一个权重p*成根.根据上下文向量h_t^*，解码器的状态为st，以及解码器输入xt在seq2seq模型中，计算生成概率p成根步骤t。

p成根= σ (w*)h_{ht}^{T*}+ w s_s^Tt+ wx_x^Tt+ bptr

p成根∈[0,1]是一个软开关，它决定是在词汇表中生成一个单词，还是通过注意力分布从输入的PII中复制一个单词。每个输入PII都有一个OOV扩展词汇表，它在给定的词汇表中存储所有未注册的单词。在引入了OOV词汇表后，得到了概率的计算公式

表i
中所使用的密码数据集的基本信息
这篇论文

数据集	Web服务	总密码	泄露时间	与PII
中国程序员大本营	程序员电子商务火车票务	6,428,632	2011	
“网站简称		16,283,140	2011	
dodonew		130,347	2014	
12306				

在解码时间步t处生成目标字w为作为fol

$$P_{OOV} = \sum_{i:w_i=w} a_i^t$$

$$P(w) = p_{gen} P_{vocab}(w) + (1 - p_{gen}) P_{OOV}(w)$$

C. 密码生成

PG-Pass模型输入基于类型的PII标记的内容，以按顺序生成密码段。在训练阶段，密码段数是固定的。对于不满足长度要求的密码，我们使用空格或超出固定长度的截断部分。因此，由模型生成的密码片段的数量也是固定的。生成后，我们删除终止符之前的空格，并连接密码段，形成最终猜测的密码。当模型预测下一个密码段时，我们使用参数设置为K的波束搜索方法。在每一步预测下一个密码段时，我们按照预测概率的顺序取前K个密码段。最后，我们得到了k-预测的密码。

增值实验与评价

A. 实验设置

1)数据集：我们使用了三个公共的真实世界的数据集，即，
表一中的CSDN，Dodonew和12306。由于本文中使用的比较实验结果取自[8]，为了保证比较的公平性，我们所使用的数据集和处理方法尽可能与[8]相同。然而，我们最终的数据集中的密码数量仍然略有不同。三个数据集之间密码号的最大差异率为0.8%。比较
使用TarGuess-I模型和我们基于数据集12306的模型PG-Pass的结果见本节。IV-D1.

我们将两个数据集CSDN和Dodonew作为测试集来模拟实验部分中真实的在线攻击。IV-D2.PII-CSDN和PII-Dodonew是通过使用电子邮件地址匹配CSDN和Dodonew和12306来获得的。匹配数据集PII-CSDN和PII-Dodonew中的密码号
如表二所示。与[8]相比，两个数据集密码号的最大差异率为1.76%，为应收账款。

2)指针发生器网络参数：本节介绍了一些参数的设置。seq2seq模型中的隐藏状态维度设置为256。单词的嵌入维数被设置为128。指针生成网络只使用指针网络，而不使用覆盖机制。

表二
密码对的基本信息设置通过匹配
使用12306

数据集	总密码	与PII
PII-Dodonew	49,567	^
PII-CSDN	12,412	^

在训练阶段，我们使用Adagarad。15.在培训和测试期间，批量大小被设置为8。我们将PII截断或填充为400个令牌，并将密码段限制为15个令牌。

3)猜测号码：每个网站对密码都有特定的限制，以抵御攻击。根据美国的说法。S.国家身份认证指南NIST sp800-63-2，对于1级或2级系统，每个帐户允许的假登录数在30天内不应超过100个，[8]。所以在本文中，我们将猜测数的上限设为100。也就是说，我们对每个用户帐户只猜测100次。

B.数据预处理

在实验中使用了几种不同的方法来描述密码中的PII。

方法1：此方法处于字符级别。我们提取
电子邮件前缀、用户名、姓名（拼音格式）、生日和手机号码，将它们划分为单个字符。同样地，密码也会被分成多个字符。 方法2：我们采用在[8]中定义的29个基于类型的PII标签。29个基于类型的PII标签包括N1，...，N7、B1，...，B10、A1、A2、A3、E1、E2、E3、P1、P2、I1、I2、I3，其中： (1) N表示名称用法，N1表示全名用法，N2表示abbr。全名，N3表示姓，N4表示名，N5表示+姓，N6表示姓氏+名的第一个字母，N7表示姓，第一个字母大写；(2) B表示生日用法，B1表示YMD格式，B1表示完整生日，B2表示MDY表示完整生日，B2已经指定，B3表示DMY表示完整生日，B4表示生日日期，B5表示在生日，B6+月，B7月+年，B8最后两个数字+日期MD格式，日期B9MD格式+最后两个数字，B10日期在DM格式+最后两位数字；(3)代表
账户名称使用情况，A1代表完整账户名称，A2代表账户名称（第一）字母段，A3代表账户名称（第一）数字段；(4) E代表电子邮件前缀用法，E1代表完整电子邮件前缀，E2代表电子邮件前缀的第一个字母段，E3代表账户名的第一个数字段；(5) P代表手机号码用法，P1代表前3位，P2代表最后4位；(6) I代表中文名义识别号，I1代表后4位，I2代表前3位，I3代表前6位。我们使用基于类型的匹配方法切割密码，密码中不匹配的字符串被分割成单个字符。

方法3：该方法与方法2相似，但29个基于类型的PII标签中有一些是不同的，包括电子邮件前缀，

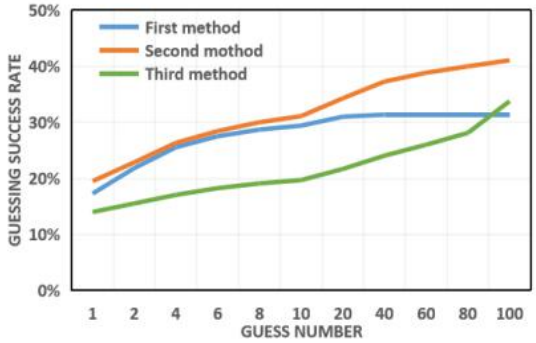

图3. 不同PII标签下的结果表征方法。

表三
三种不同的基于类型的PII标签顺序

索引	标签顺序
1	E1-E3, A1-A3, N1-N7, B1-B10, I1-I3, P1
2	-P3 N1-N7, B1-B10, A1-A3, E1-E3, P1-
3	P3, I1-I3 I1-I3, P1-P3, A1-A3, N1-N7, B1-B10, E1-E3

帐户名称、姓名和生日。我们根据电子邮件前缀和帐户名称分别分成字符类型。我们使用拼音和缩音缩写字母。对应于每个汉字分别作为一个单独的段在名称中，和姓氏及其首字母大写。我们采用年份
格式为YYYY和YY格式，月格式为MM格式，生日的日期格式为DD格式。

实验结果如图所示，方法2的性能最好。.3.我们的实验也证实了基于类型的PII标签具有高度的适应性。

C.参数优化

本节将分析基于类型的PII标记顺序的影响，并确定词汇表大小的值。

1) PII顺序：句子中单词的顺序对于自然语言的处理很重要。我们测试了PII顺序是否影响实验结果，遵循三个不同的PII顺序。在本节中介绍的结构的表示法。IV-B.从图4 (A)中，我们注意到PII的顺序几乎不影响猜测的成功率。

2)词汇量大小：我们使用不同的词汇量大小来计算猜测的成功率。.4在图(B)中，结果显示，当词汇量在30000到80000之间时，猜测的成功率是相似的。在本文中，我们设置词汇量大小为50000。

D.实验结果

1)在数据集12306上的比较结果：在最优模型参数下，我们比较了PG-Pass与TarGuess-I、Papiont-PCFG的猜测成功率
基于12306数据集的PCFG模型。猜出成功率
是密码猜测中的一个标准指示器。它越高，模型的工作效果就越好。.5.我们在图中报告了比较结果。为了公平起见，我们在实验中使用了与[8]相同的设置。使用了数据集12306中50%的数据

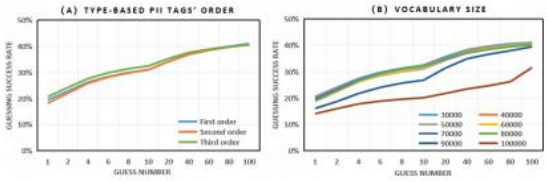

图4. 不同基于类型的PII标签顺序和词汇量大小下的猜测成功率。

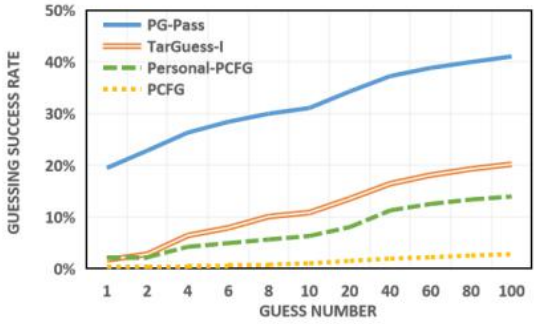

图5. 基于12306个数据集的PG-Pass和TarGuess-I、个人-PCFG、PCFG的比较。

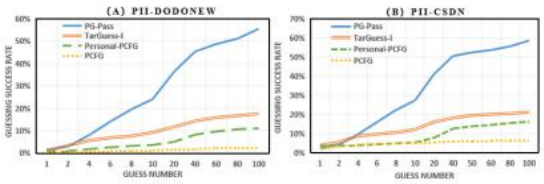

图6. 基于Dodonew和CSDN数据集的PG-Pass和TarGuess-I、个人-PCFG、PCFG的比较。

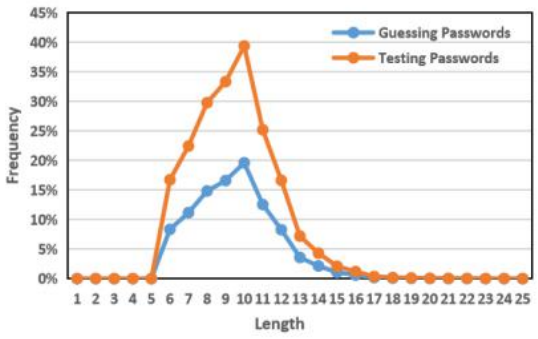

图7. 基于12306个数据集的猜测密码和真实密码的长度分布。

用于培训，其余的50%用于测试。TarGuess-I、Papol-PCFG和PCFG的猜测成功率来自[8]。如图5所示，PG-Pass模型的猜测成功率比TarGuess-I高100%~1000%。PG-Pass模型仅在猜测一次时就达到了19.49%，大约是TarGuess-I的10倍。此外，PG-Pass模型在猜测100次时，猜测成功率达到41.07%，约为TarGuess-I的两倍。

PG-Pass模型的上述结果表明，该模型可以很好地学习：(I)PII如何影响密码的生成；（二）如何构造密码。

2)现实世界的实践：通常，在实际应用中，数据源的培训数据和目标用户不同于不同的网站。为了获得更好的验证效果，我们模拟了在线攻击。我们分别在数据集12306上进行训练，并在匹配的数据集PII-CSDN和PII-Dodonew上进行测试。在无花果。6，我们的模型PG-Pass在Dodonew数据集上的猜测成功率比TarGuess-I模型高42%~216%，比~高11%~179%
在CSDN数据集上的TarGuess-I模型。这个
猜测Dodonew和CSDN数据集的成功率可以达到55个。当猜了100次时，分别为59%和58.73%。实验结果表明，PG-Pass模型具有良好的适应性和适用性。

E. 结果分析

在本节中，我们将从长度和结构分布中分析成功猜测的密码。

1)长度分析：我们计算猜测密码的长度分布和密码的长度分布
分别基于12306个数据集的测试集，如图7所示。我们发现猜测密码长度分布与实际密码相似。10个字符长度的密码占最突出的部分，其次是9个字符和8个字符。这也反映了PG-Pass模型可以很好地学习密码的组成，并生成一定比例的密码。

2)结构分析：首先分析了12306数据集猜测成功的密码结构。.8图中显示了在不同猜测时间下产生的结构数的明显趋势。当猜测一次时，PG-Pass模型为所有用户帐户尝试了22个密码结构。当猜测100次时，PG-Pass模型尝试了364个密码结构。生成的结构的多样性可能是PG-Pass模型性能良好的原因之一。此外，我们还比较了猜测成功密码与真实密码的高频结构。基于12306数据集，测试集中猜测100次时的前10个密码结构和测试集中的前10个密码结构如表IV所示。在本节中介绍的结构的表示法。IV-B.在前四种结构中，它们是完全相同的。在前十个结构中，只有两个结构的顺序是不同的。证明了PG-Pass模型可以很好地学习密码的结构特征。

最后，我们对不同的数据集进行了更仔细的分析。图9显示了12306、PII-Dodonew、PIICSDN测试集中10个最常见的结构的比例，以及每个结构在100次猜测时猜测正确密码的比例。与PII-Dodonew和PII-CSDN数据集相比，该模型在前10名中均取得了相对较高的猜测成功率

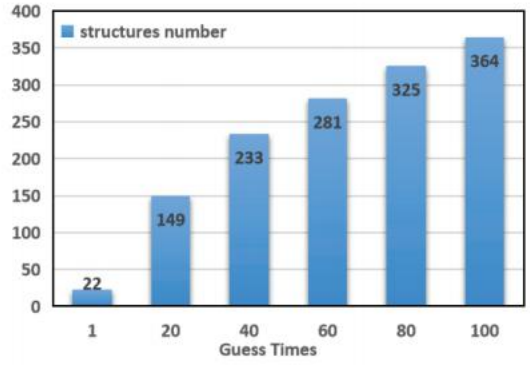

图8.猜测密码在不同猜测时间下的结构数。

表iv

十大密码结构比较

索引	猜100次	测试集
1	E1	E1
2	A2+E1	A2+E1
3	″qq″+E1	″qq″+E1
4	N1	N1
5	“a”+E1	N2+E1
6	N2+E1	“a”+E1
7	A2+A3	A2+A3
8	E2	E2
9	“q”+E1	“q”+E1
10	N2+A1	N2+A1

12306个数据集的结构。然而，由于12306个数据集的结构分布相对分散，因此PIIDodonew和PII-CSDN数据集的结构分布更多
集中的，和模型生成的结构的数量
由于难度有限，基于12306数据集的100次猜测成功率低于PII-Dodonew和PII-CSDN。12306、PII-Dodonew和PII-CSDN数据集的猜测成功率分别为41.07%，55.59%和58。73%.

V.结论

本文提出了一种针对在线的PG-Pass模型
首次采用了基于指针生成器网络的密码猜测模型PG-Pass算法。这也是将指针生成器网络应用于目标在线密码猜测中的首次研究。我们设计了模型框架，并通过详细的实验得到了最优参数。结果表明，PG-Pass模型能够优于以往的目标在线密码猜测模型。猜测密码在长度分布和结构组成上都接近于实际的密码。通过对实际在线攻击的仿真，证明了该模型的有效性。提醒用户要更加重视，网站密码设置要更加复杂。

参考文献

[1] C.赫利和P。“一项研究议程承认
密码的持久性，“IEEE安全与隐私，卷。10，没有。1，pp.
28－36，2011.

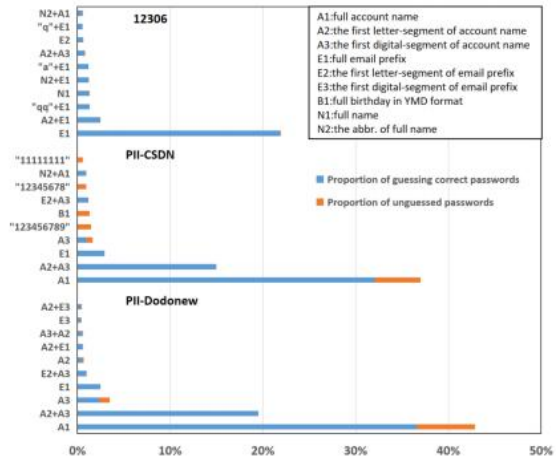

图9.在12306、PII-Dodonew、PII-CSDN测试集中，10个最经常出现的结构的比例，以及每个结构在100次猜测时间中猜测正确的比例。

[2] J.“猜测的科学：分析一个包含7000万个密码的匿名语料库”，2012年IEEE安全与隐私研讨会。IEEE，2012，页。538－552.
[3] D.王，P。王，D。他和Y。田，《生日，姓名和双重安全：了解中国网民的密码》，第28期
USENIX安全研讨会（USENIX安全19），2019，pp。1537－ 1555.
[4] X.卡纳瓦莱特和M。曼南，“从非常弱到非常强：分析密码强度计”，在网络和
分布式系统安全研讨会（NDSS 2014）。互联网协会，2014年。
[5] M.Weir，S。AggarwalB。De Medeiros和B。Glodek，“使用概率上下文无关语法的密码破解”，2009年第30届IEEE安全与隐私研讨会。IEEE，2009，页。391－405.
[6] W.梅利切尔，B。Ur，S.M.Segreti。Komanduri，L.鲍尔，N。克里斯汀和L。F.克兰纳，“快速、精益、准确：使用神经网络建模密码的可猜测性”，第25届{USENIX}安全研讨会（{USENIX}安全16），2016年，页。175－ 191.
[7] B.Hitaj，P.Gasti，G。阿特尼斯和F。*佩雷斯-克鲁兹，“帕斯根：密码猜测的深度学习方法”，在应用密码学和网络安全国际会议上*。施普林格，2019，页。
217－237.
[8] D.王，Z。张，P。王，J。Yan和X。黄，“针对在线密码猜测：一个被低估的威胁”，2016年ACM SIGSAC计算机与通信安全会议论文集，2016年，页。1242－ 1254.
[9] A.达斯，J。博诺，M。凯撒，N。博里索夫和X。王说，“密码重用的纠结之网。”在NDSS中，第1卷。14日，没有。2014，2014，pp.23－26.
[10] Y.李，H。王和K。*孙先生，“对人类选择密码中的个人信息及其安全影响的研究”，发表在IEEE信息通信2016-第35届IEEE国际计算机通信年度会议上*。IEEE，2016，页。1－9.
[11] A.见，P。J.刘和C。D.*曼宁，“到达要点：用指针生成器网络进行总结”，arXiv预印本arXiv：1704.04368，*
2017.
[12] Z.谢，M。张，Y。郭，Z。李和H。*王，“基于我的密码猜测方法”，无线通信与移动计算，卷*。2020，pp.1－22，2020.
[13] Z.谢，M。张，A。Yin和Z。*李，“一个新的目标密码猜测模式”，在澳大利亚信息安全与隐私会议上*。施普林格，2020年，页。350－368.
[14] A.Vaswani，N.Shazeer，N.帕尔马，J。Uszkoreit，L.琼斯。N.戈麦斯，Ł。凯泽和我。*《注意力就是你所需要的》，《神经信息处理系统的进展》，2017年，页*。5998－6008.